International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Authentication by Equalizing the Graphical Bars

Salim Istyaq

Computer Engineering, University Polytechnic, Faculty of Engineering & Technology,
Aligarh Muslim University, Aligarh-202002-UP-India

Abstract: ***Today, user authentication is one of the important topics in computer era. Powerful text-based password schemes could provide with certain degree of security. However, the fact that strong passwords are difficult to remember sometimes leads their own users to write them down on papers or even save them in a computer file. Graphical User Authentication (GUA) 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 recent years, many networks, computer systems and Internet based environments try used graphical authentication technique for their customer's logged in. All of graphical passwords have two different aspects which are usability and security. Different techniques for graphical systems have been proposed in literature over the past few years such as-Recognition Based Technique [2], Recall Based Technique [2]. This paper presents a survey of comparative study between different techniques of GUA.***

Keywords: Matrix authentication, encoded format, shoulder surfing, authentication, graphical bars.

1. Introduction

A graphical authentication system which is very user friendly and reliable for their users as compared to other techniques. The concept of using long password is also good but there are many problems i.e. they are not easy to remember due to their complexity. Study shows that the user tends to choose their password which is short and friendly to remember [1]. So we move on to the new concepts i.e. graphical passwords and biometrics. But these techniques are also have their own barriers e.g. in biometric like iris scan, retina scan, finger print etc. The cost of establishment is too much high compare to the others security modules and authentication process is too much slow. Huge numbers of techniques are launching day by day. In last decade most of them are suffer from vulnerabilities like shoulder surfing. There are graphical passwords scheme that have been proposed which are resistant to shoulder surfing. There are graphical password scheme that have been proposed which are resistant to shoulder surfing but have their own disadvantages like usability issue or taking more time for login or having tolerance level, PDA are used to store user password and confidential information. We have introduced the system in which the user can convert their passkey in any other reference. Only the user knows in which format the passkey is formatted. These passwords provide a great security against many brute force attacks as passwords changes every session of time.

2. Related Work

1. Dhamija and Perrig [1] proposed a graphical authentication system based on the hash visualization technique. In this authentication system the user has to select the images from the set of random images. To authenticate in this system he or she asked to select the pre-selected image as already selected in the registration. The weakness of the system is that the server needs to store the seeds of the selected image of each and every user in the simple or plain text.

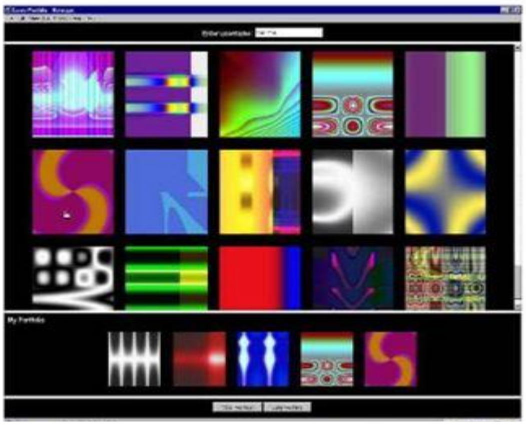


Figure 1: Random images used by Dhamija and Perrig

2. Passface [2] it is supported by the fact that the human brain can quickly recognize the face. It is a technique in which a user has to select the faces from the grid. The user is asked to select the images for a given period of time.

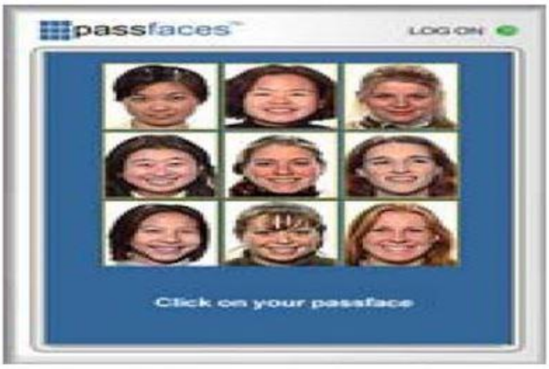
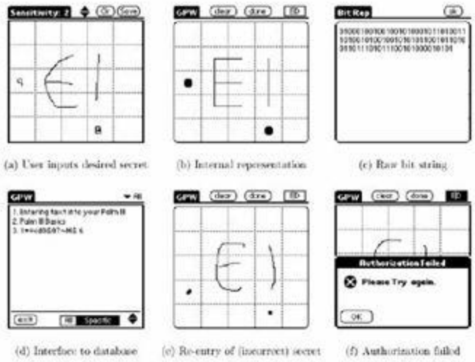


Figure 2: Passfaces

3. Jermyn, et al. [3] proposed a new technique on which user has to draw a secret i.e. DAS on a given 2D grid. If the drawing matches on the same grid in same sequence then the users are authenticate on the basis of their selection.



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Figure 3: DAS technique by Jermyn

4. Syukri [4] proposed a system in which the user has to draw the signature using the mouse. It includes two phase registration phase and verification phase. At the time of registration the user draw a signature on area through which it has to be saved on the database and at the time of verification this signature is extracted from the database and further normalization takes place with the input signature of the user, in order to match. This technique also has disadvantage i.e. the user is not friendly with signature done by mouse and forgery also may take place.

Figure 4: Signature technique by Syukri

5. Blonde [5] proposed a system in which the user must check the approximate area of predefined location. Passlogix [6] encoded this scheme by giving some permission to user to check as many objects to prove their authentication.

6. Haichang et al. [7] proposed a new shoulder surfing resistant scheme as shown in Fig. 5 where the user is required to draw a curve. This graphical scheme is the combination of DAS and story scheme that provide the user great authenticity.

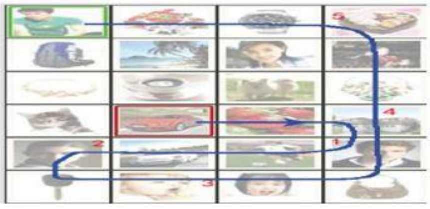


Figure 5: Haichang's shoulder-surfing technique

7. Wiedenback et al. [8] proposed a system which is resistant to shoulder surfing on some extent. In this method the user has to click the convex hull formed among the different objects in the search of passwords. The password length depends on area of solution it acts as indistinguishable or hard to guess if the number of pictures should be more.

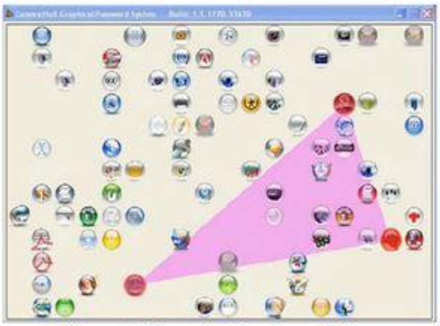


Figure 6: Example of a convex hull

Jensen [9], [10] proposed a graphical password scheme for mobile devices. During password creation, a user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. As the numbers of images are limited to 30, the password space of this scheme is not large.

7. Weinshall and Kirkpatrick [11] proposed several authentication schemes such as picture recognition, object recognition, pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes.

8. Goldberg [12] designed a technique known as "passdoodle". This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen.

To overcome the shoulder-surfing problem, many techniques are proposed. Zhao and Li [13] proposed a shoulder-surfing resistant scheme "S3PAS". The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security. Man, et al [14] proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code. In the authentication stage, the user must type the unique codes of the passobjects variants in the scenes provided by the system. Although the scheme shows perfect results in resisting hidden camera, it requires the user to remember code with the pass-object variants. More graphical password schemes have been summarized in a recent survey paper [15]. Zheng et al [16] designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text.

4. Proposed Work

There are three stages in authentication system:

4.1 Registration Phase

Users enter his username and password in registration phase and also make their password on the given bars.

4.2 Login Phase

During login phase, the user has to enter his username and password and make the same selection at the time of registration.

4.3 Verification Phase

The given username with password are matched and after that the bars are matched with registration time value.

5. Hybrid Authentication Scheme

There are following phases:

5.1 Registration Phase

In registration phase the user is first asked to enter their username, the system is checked the username is exist or not, if username is new then the system is go further in forward process but if it already present the user is asked to change their username. The name composed of alphanumeric value also after the registration of unique username, user have to submit their textual password which also contain numbers and symbols etc. After giving the password the system shows some display in the format of bars, here the users have to select their graphical password [18] which should be anything but in numeric value and after the increment and decrement of bars the user now save their registration phase setting as shown in Fig. 7.

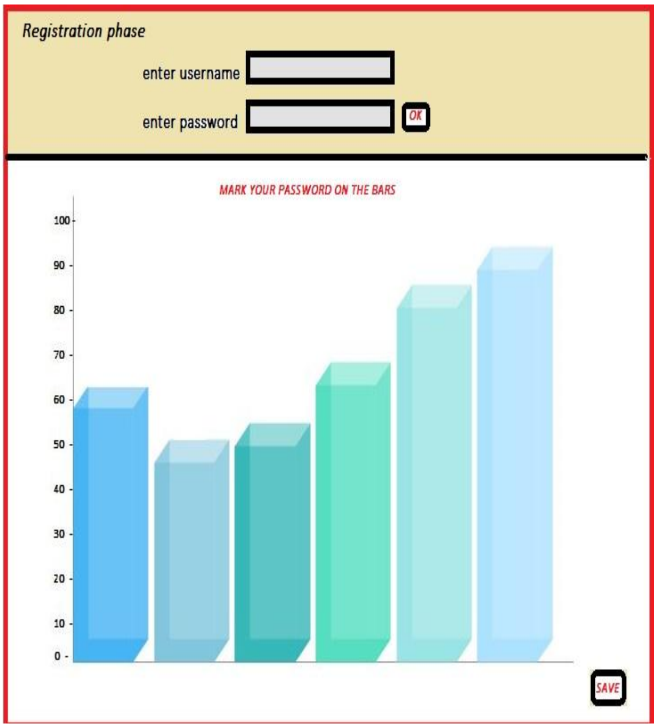


Figure 7: Registration phase

5.2 Login Phase

At the time of login the user first enter their username and password if these two parameters are right then the user are further recommended for next stage, the next stage contain the randomly organized bars with some addendum parameters. Here the user has to enter their selection by increasing or decreasing the bars in order to set the bars same as in register phase in Fig. 8.

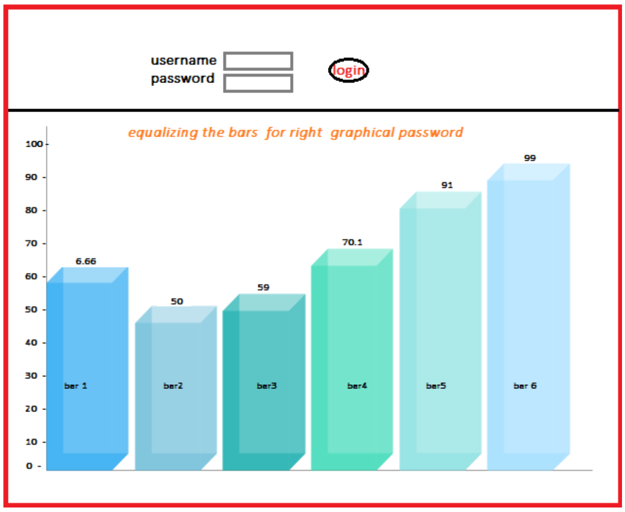


Figure 8: Login phase

5.3 Verification Phase

Now the database is fetched and users details is now further match with the given details in the registration phase. This technique of authentication is very strong in order to protect the content from many attacks like dictionary attack, brute force attack etc. This authentication system provides an interactive way of recognizing the passwords from graphical bars, this approach of graphical authentication are harder to guess the passwords or crack the system.

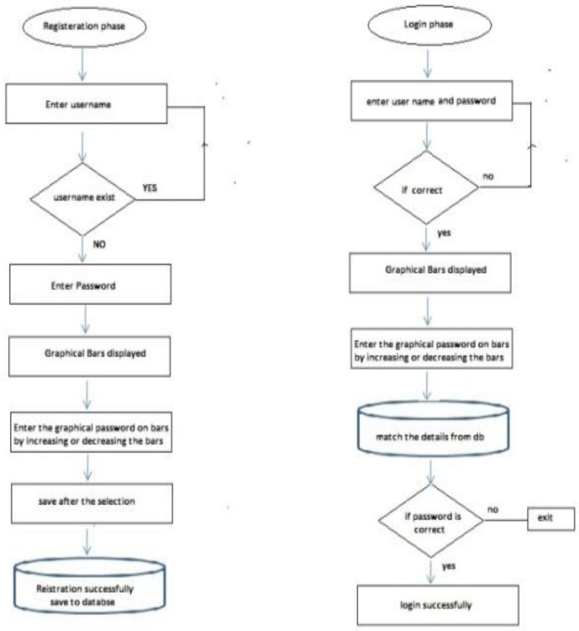

Registeration phase
Enter username
username exist
YES
NO
Enter Password
Graphical Bars displayed
Enter the graphical password on bars by increasing or decreasing the bars
save after the selection
Reistration successfully save to databse
Login phase
enter user name and password
if correct
no
yes
Graphical Bars displayed
Enter the graphical password on bars by increasing or decreasing the bars
match the details from db
if password is correct
no
exit
yes
login successfully

Figure 9: Flow chart

Suppose a user wants to register his/her id through our system then he/she first provides the username and textual password and give their initial passwords on the bars like they can give their mobile no i.e. 90271... or 6665059 etc these digits can be give in any way like with decimal part (6.66) or integral part (50 or 59).these are all for resemble in user mind the user also give their D.O.B or family members

D.O.B etc. they can give in any way but at the time of login they can put the same digits with same integral or decimal part as registered.

6. Security and Usability

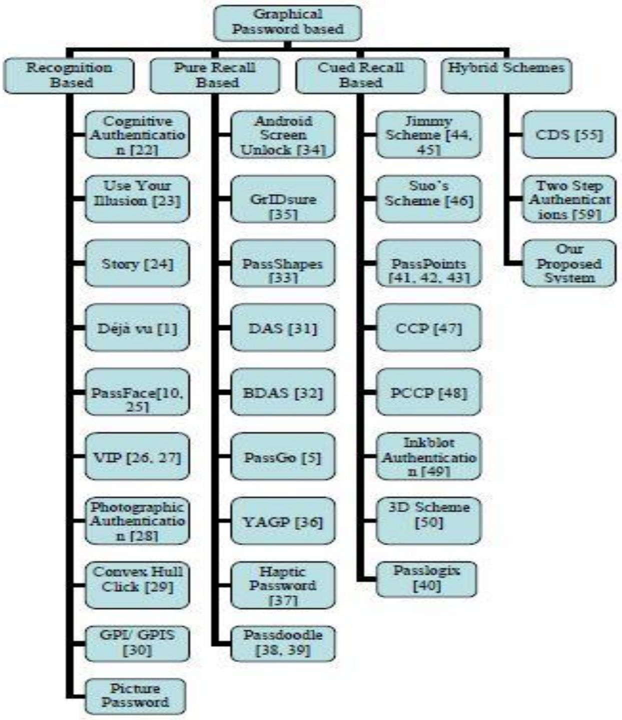
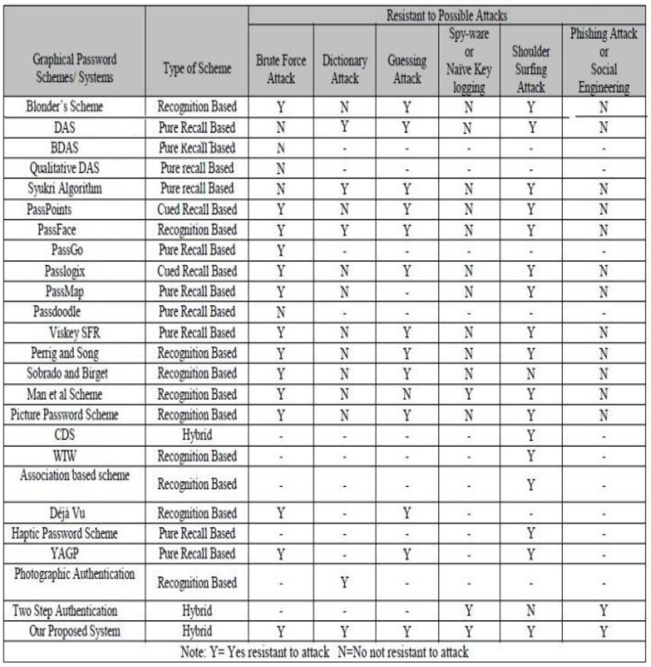


Figure 10: Different types of system

The proposed system is hybrid and too much secure as you compare with the other authentication technique. Here, it is too complex to the faulty user in order to pass through the different phases of system i.e. equalizing the bar graph for accessing OTP [19]. In this system the display is very interactive for the graphical remembrance on the users mind. Our proposed system is too much secure as compared with others as shown in Fig. 11.



Graphical Password Schemes/ Systems	Type of Scheme	Resistant to Possible Attacks					
		Brute Force Attack	Dictionary Attack	Guessing Attack	Spy-ware or Naïve Key logging	Shoulder Surfing Attack	Phishing Attack or Social Engineering
Blonder's Scheme	Recognition Based	Y	N	Y	N	Y	N
DAS	Pure Recall Based	N	Y	Y	N	Y	N
BDAS	Pure Recall Based	N	-	-	-	-	-
Qualitative DAS	Pure recall Based	N	-	-	-	-	-
Syukri Algorithm	Pure recall Based	N	Y	Y	N	Y	N
PassPoints	Cued Recall Based	Y	N	Y	N	Y	N
PassFace	Recognition Based	Y	Y	Y	N	Y	N
PassGo	Pure Recall Based	Y	-	-	-	-	-
Passlogix	Cued Recall Based	Y	N	Y	N	Y	N
PassMap	Pure Recall Based	Y	N	-	N	Y	N
Passdoodle	Pure Recall Based	N	-	-	-	-	-
Viskey SFR	Pure Recall Based	Y	N	Y	N	Y	N
Perrig and Song	Recognition Based	Y	N	Y	N	Y	N
Sobrado and Birget	Recognition Based	Y	N	Y	N	N	N
Man et al Scheme	Recognition Based	Y	N	N	Y	Y	N
Picture Password Scheme	Recognition Based	Y	N	Y	N	Y	N
CDS	Hybrid	-	-	-	-	Y	-
WIW	Recognition Based	-	-	-	-	Y	-
Association based scheme	Recognition Based	-	-	-	-	Y	-
Déjà Vu	Recognition Based	Y	-	Y	-	-	-
Haptic Password Scheme	Pure Recall Based	-	-	-	-	Y	-
YAGP	Pure Recall Based	Y	-	Y	-	Y	-
Photographic Authentication	Recognition Based	-	Y	-	-	-	-
Two Step Authentication	Hybrid	-	-	-	Y	N	Y
Our Proposed System	Hybrid	Y	Y	Y	Y	Y	Y
Note: Y= Yes resistant to attack N=No not resistant to attack							

Figure 11: Comparisons of our system

The possibilities of passwords generate in this system is too many because the users can change the set of values on each bars starting from integers, fractional no, and end to infinity.
The combination of passwords form in the above example is:
No. of bars=6
Set of values =0 to 100 including decimal numbers at two places i.e. 6^(100+99).
Finally, a onetime password is to be sent on the user's phone.

7. Conclusion

In this paper, we have proposed a new system of authentication here the user used the textual password with the new advancement of authentication with graphical bar interface. These methods are very effective in order to make an impact over the proposed system, in the coming days we also proposed many of these hybrid graphical schemes that are resistant to all the major attack.

References

[1] R. Dhamija, and A. Perrig "Déjà Vu: A User Study Using Images for Authentication" in 9th USENIX Security Symposium, 2000.

[2] Real User Corporation: Passfaces, www.passfaces.com

[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.

[6] Passlogix, site http://www.passlogix.com.

[7] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing.

[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.

[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.

[10] W. Jansen, "Authenticating Users on Handheld Devices" in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[11] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.

[12] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[13] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and*

Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.

[14] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme" in *Proceedings of International conference on security and management*, Las Vegas, NV, 2003.

[15] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey" in Proceedings of ACSAC'05.

[16] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, no.5 May 2010.

[17] Pair & Hybrid Based Authentication Technique using PBKDF2 Priyanka Kedar, Vrunda Bhusari.

[18] Salim Istyaq, "A New approach of Graphical Password with Integration of Audio Signature Combination of Recall and recognition" i*n International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 6, Issue 4, Aug 2016, 45-50.*

[19] Salim Istyaq and Lovish agrawal "A New Technique For User authentication Using Numeric One Time Password Scheme" in *International Journal Of Computer Sciences and Engineering (IJCSE)*, Volume-4, Issue-5, E-ISSN: 2347-2693 on 31st May-2016, pp. 163-165.

Author Profile

Salim Istyaq (M 2016) became Member of **WASET** in May 2016. The Author has B.Sc. Engineering in Computer, M.Tech. in Communication & Information Systems. Currently pursuing Ph.d. in Computer Engineering from Aligarh Muslim University, Aligarh, U.P. India. Presently, working as an Assistant Professor in Computer Engineering, University Polytechnic, Faculty of Engineering & Technology, A.M.U., Aligarh-202002, U.P.-India since 2004 to till date. Earlier, worked as Guest Faculty in ECE Department, Jamia Millia Islamia, New Delhi-110025. Also worked in Computer Engineering, Al-Mergheb University, Alkhoms, Libya. So far published 05 Papers in International Journals (one paper in **WASET**) and 02 in IEEE Conferences. Review Committee Member in Editorial Board of various International Journals (**WASET**, OMICS, ARSEAM, IJETAE).