An Investigation on Jawi CAPTCHA Based Security for Login Authentication and Authorization: Is It an Alternative Solution?

Sakinah Ali Pitchay, Nur Nabihah Mohd Suhaimi, Madihah Mohd Saudi,
Farida Ridzuan, Nurlida Basir and N.F.Nabila

***Abstract*—Authentication plays a significant role in computer security to validate human users. CAPTCHA is one of human interaction proof test to verify whether user is a human or a computer program. It has become a very popular security mechanism used to prevent any automated abuse of online services which is intended for human user. The test usually is provided in the authentication phase where the user will be directed to the next page if they are authorized. From the login site, an attacker creates a program exploiting the username and password to get into a website. Recently, there are a lot of different types of CAPTCHA available on the internet. However, most of them have been successfully attacked by automated programs. Thus, this paper investigates existing related works on CAPTCHA which focus on login authentication and authorization by proposes a different approach using Jawi script. Based on investigations of the systematic review and preliminary findings, it shows that this is the first work that proposed using a different script and possible future directions for producing more reliable human/computer distinguishers. Future works will develop an alternative and stronger CAPTCHA to prevent breaking cyber-attack such as dictionary attack while maintaining ease of implementation on website and ease of use for human by reducing the difficulties on reading the CAPTCHA.**

***Index Terms*— Jawi CAPTCHA, Authentication, Authorization, cyber-attack**

I. Introduction

CAPTCHA is a short form of Completely Automated Public Turning Test to tell Computers and Humans Apart. Login services are major phase that exist in most application of website on the internet. As the usage of web services is increasing, the higher the chances of malicious programs attack on it. CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) test can solve the probability of being attacked as it prevents various websites from bots program that are created to attack any network resources. Bots are short form from 'robot' which is also a type of malware takes control over an affected computer.

According to [11], a good quality CAPTCHA test should have the following characteristics: (i) Content of CAPTCHA can be easily understood by human, (ii) Quick and consume less time, (iii) Suitable for all types of bots abuse. CAPTCHA must be highly secure and easy to use [11]. The previous works on CAPTCHA discuss that many versions of CAPTCHA have been proposed, developed and should not be only difficult to solve by computer programs, but should also friendly [19]. Many companies provide free services, however in the meantime, they suffered from attacks such as dictionary attack, password attack and brute force attack. Therefore, to solve this problem, CAPTCHA can be applied as it will ensure only human obtains an account and CAPTCHA is used to protect all the services on the websites [15]. The following section will identify the problems related to CAPTCHA and are summarised as follows:

A. Difficulties on reading the text-based CAPTCHA

The previous text-based CAPTCHA tried to make the test easier for human user and difficult enough for computer programs and bot [19]. However, the efforts including created a strong and complex CAPTCHA of many schemes that have background, lead to confusions, blurring, and tilting of text which may make it hard enough for human user to pass the test. Addition of background confusion and twisting of test may cause recognition and usability problem for human user to read the CAPTCHA.

B. Requires a large database for video and audio captcha

All CAPTCHA apart from text-based CAPTCHA provides a greater security. However, it is lack in terms of space availability which consumes large size of space to upload those types of CAPTCHA on the website [13]. The usage of video and audio based CAPTCHA tests need larger database and may face usability problem as user need to download or view and listen to it first before the user can solve the test. Thus, the scheme should be simple and at the same

Manuscript received July 23, 2017; revised Aug 10, 2017. This work was supported in part by the Ministry of Higher Education (MOHE) Malaysia under incentive journal and research grant [FRGS/1/2017/ICT04/USIM/02/1]. The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) and MOHE for the support and facilities provided.

Sakinah Ali Pitchay is with the Universiti Sains Islam Malaysia (USIM), Malaysia. Currently she is a senior lecturer in Faculty of Science and Technology (FST) and also Associate Fellow with Institute Science Islam. (corresponding author: sakinah.ali@usim.edu.my) *Member, IAENG*.

Nur Nabihah Mohd Suhaimi is a Bachelor of Computer Science in Information Security and Assurance student in FST, USIM.

Madihah Mohd Saudi is the Associate Professor, Farida Ridzuan, Nurlida Basir and N.F.Nabila are senior lecturer in FST, USIM.

time, it is secured enough to avoid abuses from bots.

C. Existing English text-based CAPTCHA had been commonly attacked

For the text-based CAPTCHA, researchers keep developing another language of CAPTCHA such as in Arabic, Persian and Latin as English text-based CAPTCHA have been attacked by dictionary attack [16]. Therefore, there is a need to develop another script of CAPTCHA that never been implemented yet.

Based on the identified problems, this paper proposes a new text-based CAPTCHA using Jawi script for login authentication and authorization. It is hoped that this work can increase the security of login services and can solve the hardness user faced while solving the CAPTCHA. Jawi Script has special characteristics which differs from another script. It looks almost similar to Arabic Script except 6 letters. Jawi script contains 35 letters and they are written from right to left like Arabic. Jawi script is used limited by certain country such as in Malaysia, Indonesia and Brunei. Hence, Jawi script as text-based CAPTCHA is more secured as it is a new method in this security field.

The remainder of the paper is organised as follow. In Section II, we discuss the login mechanism for security purposes. Section III summarizes the types of CAPTCHA and section IV highlights the related works. Alternative approach is proposed in Section V and followed by preliminary findings in Section VI. Finally, conclusions and future work are discussed in Section VII.

II. LOGIN MECHANISM

There are two types of login mechanism. Method in [11] used template matching and polynomial fitting algorithm to estimate the baseline.

A. Authentication

Authentication is the act in security where it is the process of determining the identity of a user [18]. There are many reasons why authentication is needed for any services. The main purpose of authentication is to verify the status of the user is a human or a machine which attempts to interact with the system getting the permission to login. Secondly, authentication is used to gather information regarding the way of user is accessing the system. Some of strategies that are usually used to identify a user are:

- Username and password: The typical one and the simplest. It is one of the approaches to identify someone because it is fully software-based.
- Physical security device: A physical device that is used to identify a person. In this case, a password or personal identification number (PIN) is also required to ensure that it is the right person.
- Biometric identification: Biometrics is the process of identifying someone using physical characteristics on user body such as voice recognition and thumbprints. It is assumed as strongest third-party authentication.
- User Based authentication: This common form of authentication whereby user use his login id and password that one registered and stored in system database which are validated under credentials.
- Smart Card based authentication: It is known as a second factor authentication which store cryptographic data inside the card.
- Grid Based authentication: It is a second factor authentication which is provided by entrust identity guard.
- Knowledge Based Authentication (KBA): This facility provides additional confidence in user's identity to challenge attacker that is unbreakable. This scheme can ask the user to answer at least one 'secret' question to confirm information about user that already known through registration process like cross verification. KBA is frequently used as an element in multifactor authentication and for self-service password.
- One Time Password (OTP): It is a dynamically generated password which is valid for once only. Thus, when the hacker hacks this password he cannot used it for the second time.

B. Authorization

Authorization is the process of determining the privilege for the user whether they are permitted to access the system or not. Similarly, authorization verifies what the user is authorized to do.

III. ISSUES IN CAPTCHA

Table 1 summarizes on comparison types of CAPTCHA [4-5]. The types of attack usually exist in the authentication and authorization phase are as follows. There are two common types of attack which are brute-force attack and dictionary attack. The brute-force attack involves the activity of trial and illegal method used by application programs to decode encrypted data such as password or Data Encryption Standard (DES) keys [13]. This attack usually focuses on breaking of password. In dictionary attack, one of the basic attacks to break into password-protected computer or server by systematically enters every word in a dictionary as a password. It is also can be used to find the necessary keys to decrypt an encrypted message or document.

IV. RELATED EXISTING WORKS

From Table 2, it shown that another type of CAPTCHA is more secured than text-based CAPTCHA. However, in terms of usability text-based CAPTCHA is the most easily implemented and low-cost program compared to others. Language apart from English, is more secured as there is no evidence or research that showing Arabic CAPTCHA is vulnerable to attack. Jawi script and Arabic script is very similar to each other, only a few letters exist in Jawi but absent in Arabic script. For the text-based CAPTCHA, words other than English letter are more secured. Therefore, this paper proposes the text-based CAPTCHA in Jawi text since the English CAPTCHA has been attacked by the dictionary attack.

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE I
COMPARISON ON THE STRENGTHS AND WEAKNESSES FOR EACH TYPE OF CAPTCHA

Types of CAPTCHA	Strength	Weaknesses
Text based CAPTCHA	1) Easy to be implemented on website. 2) Battle Text-based CAPTCHA able to defeat dictionary attacks. 3) Re-CAPTCHA Text-based CAPTCHA always uses new dictionary words and unable to be break by optical character recognition.	1) Some user having a problem to insert the right input. Causes of confusion are as follows: • Use of multiple lines. • Generation of multiple shapes. • Using various fonts. • Font size unstable. • Strong blurred letters. 2) Text-based CAPTCHAs easily can be broken by OCR techniques (e.g: Content based image retrieval). 3) User with low level of visibility can hardly pass the test.
Images based CAPTCHA	1) Simple click based system. Does not require user to type the words. 2) Image-based CAPTCHA pattern recognition of image is using tough artificial intelligence (AI) program.	1) Users with low vision or because of blurring in the images face a problem of image identification.
Audio based CAPTCHA	1) Employed for user who have impaired vision involving audio clip. 2) User-friendly.	1) Available only in English. User needs to have a comprehensive English vocabulary. 2) Possibility of character having similar sound. 3) Not effective for dumb user or user with low level of listening.
Video based CAPTCHA	1) Hard to break using Optical Character Recognition (OCR). 2) In certain cases, it provides greater security than other type of CAPTCHA.	1) Large size of file, may cause user having a problem of downloading the video to answer the test. 2) Need to replay if unable to catch up with the speed of video.
Puzzle based CAPTCHA	1) Similar to a game. 2) Able to help user train their minds. 3) User can communicate more with this CAPTCHA system as it is like a game.	1) Consumes more times to solve the test. 2) User cannot organize the puzzle within a short time.

TABLE II
DIFFERENTIATION OF JAWI ALPHABET AND ARABIC ALPHABET COMPARISON OF RELATED EXISTING WORKS ON CAPTCHA

Work	Feature	Strength	Drawback
2015 [7]	Password is based on the image selection which requires the user to choose the colour of the image selected and in what sequence for the authentication during the registration.	Security is more ensured. Only the legal user knows what kind of colour image selected and in what sequence they chose for the authentication during registration.	If the user forgot the sequence, they made as there is no backup password is provided.
2015 [19]	CAPTCHA is designed in ASP.net under Visual Studio platform with C# which is easy to be implemented on the computer.	Can be solved easily as they do not have to type the whole word but only need to provide word according to the associated query.	A problem might raise if there are user who cannot read or understand the query description. (e.g: Type the third word)
2015 [15]	Use text-based CAPTCHA that includes both digit and letter.	Combination of two text based captcha increased the hardness of program bot to break into the system	The CAPTCHA might be hard to recognized since the type of the letter is very complex
2015 [25]	CaRP is a combination of Captcha and graphical password scheme.	Graphical password is resistant to attacks such as relay attack and shoulder-surfing with dual view technologies.	Consumed a lot of database and computer program.
2014 [21]	Three group of images involved in this graphical password are famous places, famous people, and reputed company name. User clicks on the selected images during the registration phase to be used as a password.	Uses text password as well as graphical password to provide protection against different attack such as shoulder surfing attack, dictionary attack, brute force attack	Future work is based on the pattern as it is smaller in term of memory space.

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

	Also used text password.		
2017 [1]	-Graphical scheme: Recognition Based, pure-called based and cued recall based. -Graphical authentication combining pattern and a background image.	Improves the usability and the security during the authentication	Prototype produced was not suitable in mobile version.
2016 [12]	Use the technique of Pair Based authentication scheme onto CAPTCHA Creates a matrix to arrange the characters, numbers, and images.	Password is more secured as the CAPTCHA having common element in selecting row and column	User can be confused to choose the letter of CAPTCHA in the form of row and column
2016 [10]	Login method that includes a voice recognition system The voice will be stored in the password database	Reduce the degree of attack on the password break.	Problem could happen if the user computer does not have a microphone to record the voice recognition.
2015 [2]	CaRP stand for CAPTCHA as Graphical Password It uses the images to provide authentication. Image password will appear in the first place before the CAPTCHA image	Graphical password consists of pixels embedded in the picture Hard for the program bot to define the pixels and break the CAPTCHA.	Need to consume a lot of space since it combines the two type of password which is image and CAPTCHA text-based
2014 [17]	Consist of BarCAPTCHA, TransparentCAPTCHA and ThreadCAPTCHA	Difficult for BOT program to distinguish on which bars represent text and noise. Pixels used to represent text and another object in the CAPTCHA image hardly can be found by the computer program.	Consumes a lot of computer memory to run this program.
2014 [22]	Focus on click-based graphical password scheme called Cued Click Points (CCP) A password consists of sequence of images in which user can select one click-point per image. User is also required to select a sound signature correlated to each click point as the sound signature is used to help the user in recalling the click point on an image.	Sound signature is used to help user to recall the forgotten graphical password It is proved to have good performance in terms of speed, accuracy, and ease of use.	Lots of database are required to store and process the audio file.
2013 [16]	The CAPTCHA image is distorted by adding various types of noises in the background whether in the form of dots, lines, and arcs	Proposed to prevent automated-bots and help the user during the authentication process Number of characters, font types, font sizes make it hard for OCR to read.	Dots background may cause confusion to read the word.
2011 [24]	Uses algorithm to find key-points of input images against database images using Robust Scale-invariant feature transform (SIFT)	Secure and very hard to be cracked because the CAPTCHA requires the user to follow the hand gesture displayed which is impossible for the bot program to do	Low resolution of the image produced
2011 [26]	Involves setting of technique in the obfuscator module to produce DevaCAPTCHA robustness.	Exploit the difference in the reading effectiveness between humans and computer programs. Increase the security of Indian language based applications	Limited to certain people that interacting in the Deva script.
2008 [9]	Convert a textual CAPTCHA into a clickable CAPTCHA. Combines multiple CAPTCHA text in a grid which consists of English and some other languages. Need to click on the English text CAPTCHA.	Improving usability of text-based CAPTCHA	Can cause a confusion for some human user to key in the input required by the CAPTCHA system
2010	Algorithm is based on Chellapillas algorithm which consist of five phases:	CAPTCHA image can be quickly segmented into many small component	Too much cluttering line and character warping could cause the user much

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[14]	Preprocessing, Image Opening, Labeling, Component Splitting and Character Extracting The CAPTCHA implemented with the cluttering line and character wrapping		effort to read the CAPTCHA.
2010 [6]	CAPTCHA solver (breaking) uses modules like Pre-processing, segmentation, and character recognition. Use Pattern Matching technique gives high accuracy where it used 8 neighbours segmentation algorithms in which characters are not connected.	Increase of robustness and build secured CAPTCHA to provides secured online authentication.	Lot of process need to be performed and the usage of EZ Gimpy CAPTCHA has already being attacked.
2006 [23]	The usage of Persian or Arabic word as text-based CAPTCHA	User able to recognize the words easily but not computer programs.	Similarity of the background colour with the text colour causes the user cannot easily recognized the word displayed. The existence of random lines which made the recognition of dots in the word is impossible in some cases.
2004 [8]	Consist of image CAPTCHA that required the user to key in the input on the image displayed (e.g: ball, bus)	Bot program can hardly detect the image displayed and cannot do the dictionary attack.	Mislabeling problems that lead human to falsely insert the input for the CAPTCHA. Less image is presented in CAPTCHA per round causing the deflate of the computer performance.
2003 [20]	Algorithm A is used to find words in the image works from the bottom up starting with visual cues and incorporates lexical information. Algorithm B created to find entire words at once instead of looking for letters.	Affordable space is needed for creating this technique. User-friendly. Reduces the set of words into the manageable size using pruning technique.	Gimpy and EZ Gimpy CAPTCHA are already exposed to the dictionary attack. The cost to fix the problem is quite costly.

V. ALTERNATIVE APPROACH: JAWI SCRIPT

In the previous years, Jawi script became the first script used among the Malay, Indonesian as well as Bruneian. Nowadays, Jawi script are still included in educational module specifically in Asean countries such in Malaysia, Indonesia and Brunei. It is said to be almost similar with the Arabic letters excepts for a few words. Recent work in [3] employs Arabic word and claim as the first to generate Arabic handwritten CAPTCHAs. However, the pronunciation between Arabic and Jawi script are different where Jawi script could be written as in Malay medium language and with the additional of six characters in Jawi alphabet. The list of Arabic script and Jawi script are presented in Table 2. Thus, this paper proposes an alternative solution by providing another text-based CAPTCHA using Jawi script. The user can choose on the language based on familiarity either English or Jawi script text based CAPTCHA.

TABLE III
DIFFERENTIATION OF JAWI ALPHABET AND ARABIC ALPHABET

Twenty-nine characters of the Jawi alphabet similar to Arabic alphabet:
ا (a), ب (b), ت (t), ث (tha), ج (j), ح (Ê), خ (kh), د (d), ذ (dh), ر (r), ز (z), س (s), ش (sh), ص (î), ط (¼), ض (ð), ظ (§), ع (‘), غ (’), ف (f), ق (q), ك (k), ل(l),م(m), ن (n), و (u), هـ (h), ء (’), ي (y).
The added six characters only in Jawi Alphabet:
ڤ (v), چ (c), ڠ (ng), ڽ (p), گ (g), dan پ (ny).

VI. PRELIMINARY FINDINGS

To identify the requirements needed for the system, two methods for information gathering are investigated. The review of previous works and the second technique is by conducting an online survey on Jawi-text CAPTCHA. 4 close-ended and 1 open-ended questions have been answered by 146 respondents from random background area in Malaysia. The significant findings are summarised in Figure 1 - 5.

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

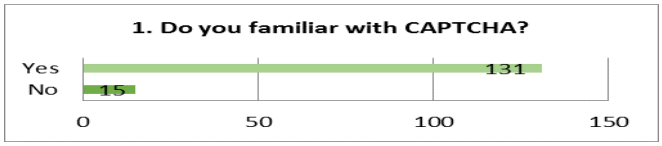

Fig. 1. 90% are familiar and 10% are not familiar with CAPTCHA to measure the familiarity.

The first question concludes majority of the user are familiar with the CAPTCHA.

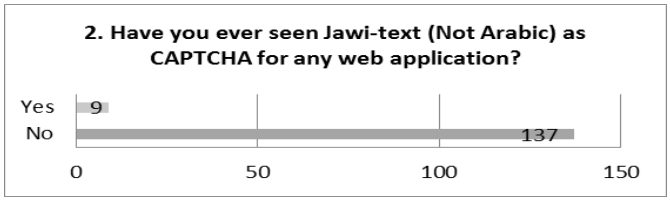

Fig. 2. 6% have seen and 94% have never seen Jawi-text CAPTCHA

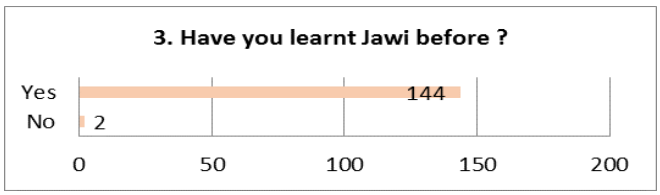

Fig. 3. 6% have seen and 94% have never see Jawi-text CAPTCHA

Fig. 4. 99% can read and write in Jawi-text and 1% could not.

Second question is a survey on existence of Jawi-text based CAPTCHA over the internet. User that answered "Yes" are required to identify the website that used Jawi-text. Unfortunately, none of them answered the question. This shows that the respondents unable to recall where the Jawi-text based CAPTCHA is being implemented and not widely used on the website or probably confused with the Arabic CAPTCHA. Third question is to analyse the knowledge of Jawi within respondents. It concludes that most of the user prefers Jawi-text based and able to recognize the displayed text.

5. Which of the following category that you prefer to write in Jawi-text as CAPTCHA? Please choose only two (2) category that you find the easiest as for Jawi text-based CAPTCHA.

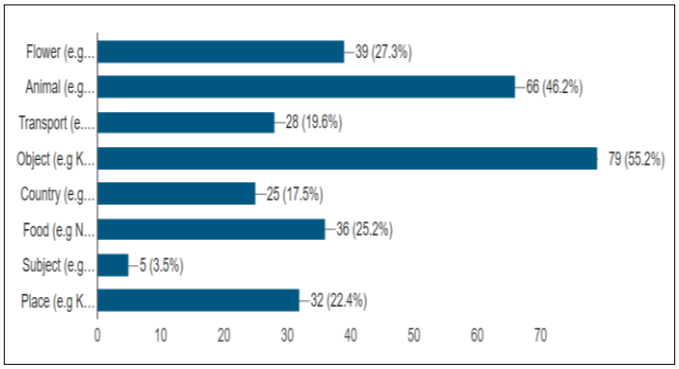

Fig. 5. Object (i.e: chair, table) received the highest number of votes as the easiest Jawi-text based CAPTCHA to be implemented. The second highest is animal and the most less voted is subject (i.e: Mathematics, Science).

Fourth question measures the total number of user who can read and write in Jawi-text. Hence, in terms of usability, Jawi-text based CAPTCHA is not a big issue for country that utilizes Jawi as one of the reading material. The final question is to identify the most suitable types to be implemented for the login authorization. Based on the preliminary findings, Jawi-text based CAPTCHA is proposed as the alternative secured solution and object was chosen as the category of word to be written digitally in Jawi character.

VII. CONCLUSION AND FUTURE WORK

This paper investigates different kinds of CAPTCHA that have been developed till recent. A systematic review has been investigated, login mechanism, types of CAPTCHA and identify the strength and drawbacks on related existing works. In future, focus will be on text-based CAPTCHA using Jawi script that provides high quality of security that preventing the system from bot abuse. Though the proposed work is limited to countries that utilizes Jawi script, but it is recommended to have an alternative approach for English text-based CAPTCHA due to increasing of cyber-attacks such as dictionary attack, password attack and brute force attack.

REFERENCES

[1] Affandi Radhi R.: ChoCD: Usable and Secure Graphical Password Authentica-tion Scheme. Universiti Sains Islam Malaysia. 2017.
[2] Anto Kumar, R., Sivakumar, R., & Aalin Grace, S. A New Implementation of Graphical Password Scheme for Captcha Based Security System. Middle-East Journal of Scientific Research, 23(7), 1353-1357. 2015.
[3] A.Alsuhibany, S., & Tanvir Parvez, M. Secure Arabic Handwritten CAPTCHA Generation Using OCR Operations. Proceedings of International Conference on Frontiers In Handwriting Recognition, ICFHR, 126-131. 2016.
[4] Bursztein, E., Bethard, S., Fabry, C., C. Mitchell, J., & Jurafsky, D. How good are humans at solving {CAPTCHA}? A large scale evaluation. Proc. Of The 2010 IEEE Symposium on Security and Privacy, 399-413. 2010.
[5] Bursztein, E., Martin, M., & C. Mitchell, J. Text-based CAPTCHA strengths and weaknesses. Proceedings of The 18Th ACM Conference On Computer And Communications Security, 125-138. 2011.
[6] Chandavale, A., & Sapkal, A. Algorithm for secured online authentication using CAPTCHA. Proceedings - 3Rd International Conference on Emerging Trends In Engineering And Technology, ICETET 2010, 292-297. 2010.
[7] Chaudari, P., Hajare, S., & Bhusare, P. Image Based Password Authentica-tion. International Journal of Advanced Research In Computer Science And Software Engineering, 5(2), 154-156. 2015.
[8] Chew, M., Tygar, J., & Berkeley, U. Image Recognition CAPTCHAs. Proceedings of The 7Th International Information Security Conference, (September), 268-279. (2004.
[9] Chow, R., Golle, P., Jakobsson, M., Wang, L., & Wang, X. Making CAPTCHAs clickable. Proceedings of The 9Th ACM Workshop On Mobile Computing Sys-tems And Applications, 91-94. 2008.
[10] Dehigaspege, L., Hamy, U., Shehan, H., Dissanayake, S., Dangalla, H., Wijewan-tha, W., & Dhammearatchi, D. Secure Authentication: Defending Social Net-works from Cyber Attacks Using Voice Recognition. International Journal of Scientific and Research Publications, 6(10), 120-126. 2016.
[11] Kaur, K. and Behal, S. Captcha and Its Techniques: A Review. International Journal of Computer Science and Information Technologies, Vol. 5 (5), 6341-6344. 2014.
[12] Ganjudde, M. Design Pair Based Algorithm for Selection of CAPTCHA as A Password to Get Better Security against Hard AI. International Journal on Re-cent And Innovation Trends In Computing And Communication, 4(1), 143-146. 2016.
[13] Ghorpade, J., Mukane, S., Patil, D., Poal, D., & Prasad, R. Novel Method for Graphical Passwords using CAPTCHA. International

Journal of Soft Computing and Engineering, 4(5), 2231-2307. 2014.
[14] Huang, S., Lee, Y., Bell, G., & Ou, Z. An efficient segmentation algorithm for CAPTCHAs with line cluttering and character warping. Multimedia Tools and Applications, 48(2), 267-289. 2010.
[15] Kaur, K., & Behal, S. Designing a Secure Text-based CAPTCHA. Procedia Com-puter Science, 57, 122-125. 2015.
[16] Khan, B., Alghathbar, K., Khan, M., Alkelabi, A., & Alajaji, A. Cyber security us-ing Arabic CAPTCHA scheme. International Arab Journal of Information Tech-nology, 10(1), 76-84. 2013.
[17] Kumar Choudhary, N., & Patil, R. CAPTCHAs based on the Principle- Hard to Separate Text from Background. International Journal of Computer Science and Information Technologies (IJCSIT), 5(6), 7501-7503. (2014).
[18] Mahajan, N., & Patil, D. Study of Authentication and Authorization in Cloud Computing. International Journal on Recent and Innovations Trends In Compu-ting And Communication, 4(7), 178-180. 2016.
[19] Mahato, S., Rani Pati, P., Tiwari, P., & Gaurav Mishra, R. Implementation of Advanced Captcha based Security System. International Journal of Technolo-gy Innovations and Research, 15(May), 1-7. 2015.
[20] Mori, G., & Malik, J. Recognizing objects in adversarial clutter: breaking a visual CAPTCHA. 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings., 1, 1-8. 2003.
[21] Patel, M., & Modi, N. Authentication Using Graphical Password. International Journal of Computational Engineering Research, 4(11), 2250-3005. 2014.
[22] Singh, S., & Agarwal, G. Integration of Sound Signature and Graphical Password Authentication System. International Journal of Computer Applications, 2(1), 1-3. 2013.
[23] Shirali-Shahreza, M., & Shirali-Shahreza, M. Persian/Arabic Baffletext CAPTCHA. Journal of Universal Computer Science, 12(12), 1783-1796. 2006.
[24] Srinivas, B., Kalyan Raju, G., & Venkata Rao, K. Advanced CAPTCHA tech-nique using Hand Gesture based on SIFT. International Journal of Computer Applications, 31(11), 16-22. 2011.
[25] Vamsi Priya, M., Nallamali, S., Bhanu Prakash, D., & Ramya Sri, K. Authentica-tion Using CAPTCHA as Graphical Password. International Journal of Ad-vanced Research in Computer and Software Engineering, 5(5), 1429-1436. 2015.
[26] Yalamanchili, S., & Rao, K. A Framework For Devanagari Script-Based CAPTCHA. International Journal of Advanced Information Technology (IJAIT), 1(4). 2011.

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)