Gamification of Internet Security by Next Generation CAPTCHAs

Mr. S. Ashok Kumar
Department of Information Technology
Sri Shakthi Institute of Engineering and Technology
Coimbatore, India
sashokkumarit@gmail.com

Mr. N. Ram Kumar
Department of Information Technology
Sri Shakthi Institute of Engineering and Technology
Coimbatore, India
ramkumarit@siet.ac.in

Dr. S. Prakash
Department of Information Technology
Sri Shakthi Institute of Engineering and Technology
Coimbatore, India
prakashdharsan@gmail.com

Mrs. K Sangeetha
Department of Computer Science and Engineering
SNS College of Technology
Coimbatore, India
sangithaprakash@gmail.com

Abstract—**CAPTCHA is a type of challenge-response test to ensure that the response is only generated by humans and not by computerized robots. CAPTCHA are getting harder as because usage of latest advanced pattern recognition and machine learning algorithms are capable of solving simpler CAPTCHA. However, some enhancement procedures make the CAPTCHAs too difficult to be recognized by the human. This paper resolves the problem by next generation human-friendly mini game-CAPTCHA for quantifying the usability of CAPTCHAs.**

Keywords- bots; captcha; gamification; internet security; attacks; Turing tests, pattern recognition, machine learning algorithms.

I. INTRODUCTION

CAPTCHA is abbreviated as Completely Automated Public Turing test to tell Computers and Humans Apart[3]. It was developed in the year 2000 at Carnegie Mellon University by John Langford, Nicholas J. Hooper and Luis Von Ahn[2]. CAPTCHA is used to differentiate between the humans and the computers. It also prevents the system when people try to spread the viruses or vulnerable attacks. CAPTCHA is the verification test that can be found at the end of the sign-up page form in Gmail or Yahoo account. CAPTCHAs are mostly used in websites that provide services like surveys, polls, and registration forms. CAPTCHA should be easy enough and user-friendly to the user, sometimes the user needs to try for many times by an assumption in order to login and access the system.

CAPTCHAs are a type of Artificial Intelligence. It cannot be solved by a computer system or by automated software; it is solvable only by a human being. The challenging task is to teach the computer about the human behavior and also to make the computer how the people think. The Artificial Intelligence has many algorithms, and it needs to be designed in such way that the computer behaves like a human, in order to explain the concept of CAPTCHA [4].

Applications of CAPTCHAs are Preventing Comment Spam in Blogs, Protecting Website Registration, protecting Email Addresses from Scrapers, Online Polls, Preventing Dictionary Attacks, Search Engine Bots, Worms and Spam [5].

II. BACKGROUND AND RELATED WORK

A. *CAPTCHAs based on text*

Text-based CAPTCHAs are the most common type of CAPTCHA where the text is usually presented in a distorted fashion. Sometimes, the text is twirled, twisted in various possible directions thereby making it difficult for automated chat bots to decipher the text. The text displayed in the CAPTCHA box is stricken out and scrambled. Humans find it easy and trivial to read the text.

Text-based CAPTCHAs is a very simple to implement. It is very efficient and requires a large question bank. In Text-based CAPTCHA the Number of classes of characters and digits are tiny small, so the problem occurs for a user to identify the correct characters and numbers. The text-based CAPTCHA is possible to determine the character and digit through Optical character recognition (OCR) technique. In Text-based CAPTCHAs simple asked questions like as based on arithmetic equation some example are given in Figure 1 [1].

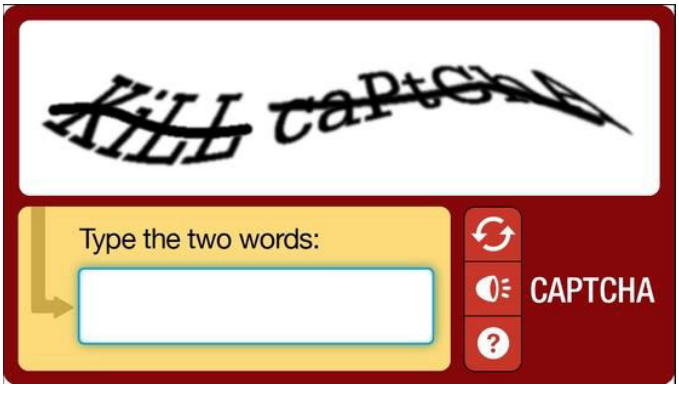

Figure 1. Text-based CAPTCHA

978-1-4673-8855-9/17/$31.00 ©2017 IEEE

B. CAPTCHAs based on image

In Image-based CAPTCHAs, several pictures are juxtaposed and simple actions such as Click all the images of animals or Click all the images of cats are to be performed by the user. The fact that automated chat bots find it increasingly difficult to distinguish one kind of image from another kind works in favor of Image-based CAPTCHAs. Sometimes, Image-based CAPTCHAs are tough nuts to crack as questions such as Click all the images of cats will be asked where apart from normal sized domestic cats, big sized feline images will also be displayed. To assist humans in such cases, a few hints such as – identification of cats requires not more than seven clicks etc. are provided [6].

In image-based CAPTCHAs user is required to identity image. The advantage of image-based CAPTCHA is that pattern recognition is hard AI problem and therefore it is difficult to break this test using pattern recognition technique. Example of images based CAPTCHA is given in Figure 2. [1]

Figure 2. Image-based CAPTCHA

C. CAPTCHAs based on Audio

In Figure 3: Audio based CAPTCHA's were developed with the thought of visually impaired users, and it relies on the user listening to the spoken word and then typing it into a box to pass the test [7].

Figure 3. Audio based CAPTCHA

D. Mathematical Captcha

Mathematical CAPTCHAs are simple numerical calculations such as 1+3, 4-1 etc. It is also associated with twisted text and an audio option. If the user fails to decipher the text, they can count on 'audio' option or request for another one [10]. An example of Mathematical CAPTCHA is given in Figure 4.

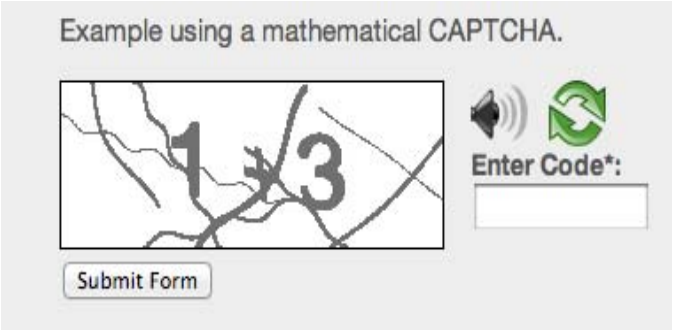

Figure 4. Mathematical CAPTCHA

E. Logic-based Captchas

Logic-based CAPTCHAs have become the latest fad. Humans need to use their intelligence and of course, their common sense to answer the CAPTCHAs correctly. Though the questions may seem trivial, automated chat bots find it extremely difficult to crack Logic-based CAPTCHAs [10]. An example of Logic based CAPTCHA is given in Figure 5.

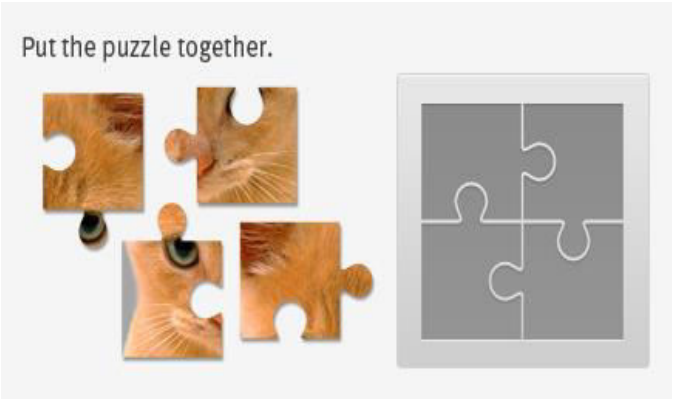

Figure 5. Logic based CAPTCHA

III. NEXT GENERATION GAME-CAPTCHAS

The next generation CAPTCHAs are based on simple and light weighted mini games which are used for differentiating human being from automated bots. These games are design generated randomly for each users using HTML5 with JavaScritp and transmitted to the client browser in encrypted form. There is no additional plug-ins or special software's required to implement these game CAPTCHA in both client and server side.

The following four different types of game-CAPTCHAs have experimented in this paper:

- Bird Shooting
- Connecting Dots
- Duck Hunt
- Drag-and-Drop

A. Bird Shooting

The bird shooting is an exciting game to click the flying birds to shoot and complete the task by shooting given the number of counts to determine the user is human. If robots are involved in this activity, it is easy to identify and prevent unauthorized activity to ensure the security of the website. In this below figure, there are different colors of birds are flying around, the rule given is to click the yellow bird, the user needs to click all the yellow birds in order to authenticate the correct user. The sample of bird shooting game CAPTCHA is shown in Figure 6.

Figure 6. Bird Shooting CAPTCHA

B. Connecting Dots

In Connecting Dots game the task may be given like connecting two red dots. The user needs to identify any two red dots in the CAPTCHA by clicking one dot and drag and drop to another red dot. This game is easy to play and confirm "I'm not a robot". It indicates the human recognition. Figure 7 shows the sample of Connecting Dots.

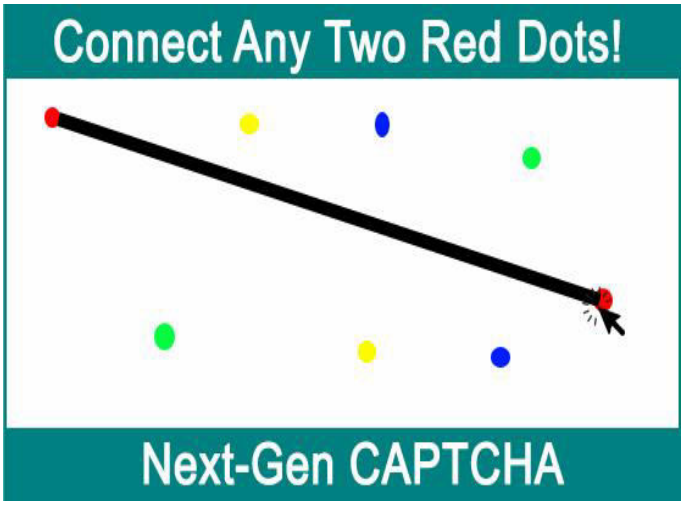

Figure 7. Connecting Dots CAPTCHA

C. Duck Hunt

In figure 8, the Dunt hunt technique was followed, the user will see the ducks passing around, and the rule is, as given in the figure the user need to shoot three ducks, once the user shoots the ducks the CAPTCHA is verified, and the user was authenticated.

Figure 8. Duck Hunt CAPTCHA

D. Drag-and-Drop

In Drag-and-Drop task is given, the user can drag and drop the object from one place to another place to complete the task. In the figure 9, there are three different shapes and there is also an empty space. To recognize a human, the user needs to fill the empty space by dragging the appropriate shape to the empty shapes. Once the user fills the shape, it will be authenticated; this is an another technique.

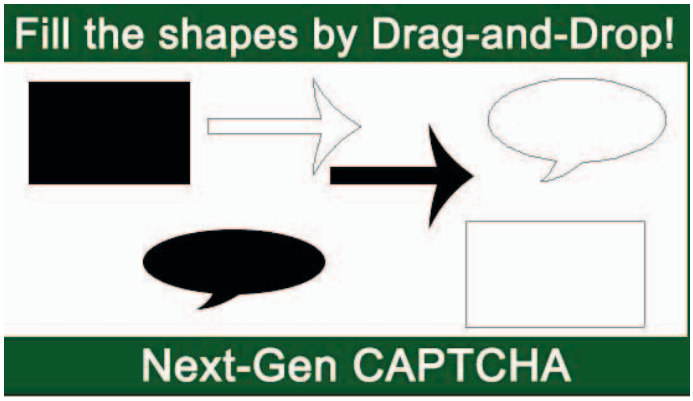

Figure 9. Drag-and-Drop CAPTCHA

IV. SECURITY ANALYSIS

The game based CAPTCHAs are purely developed and implemented using HTML5 and JavaScript. It will transmit to the client browser in the encrypted form, and intruders cannot able to decrypt the CAPTCHA code or hack the same.

A. Random Guessing Attack

Here the CAPTCHAs a based on the mini-game, so the users need not provided any input to solve the same. There is no possibility of random guessing attack in next generation mini game CAPTCHAs. Random Guessing Attack is otherwise called as Brute force attack. Brute force attack is like trying with various combinations of letters, numbers, and symbols. As the combinations are correct, it works fine and the user can login and access resources

B. Dictionary Attack

It is an authentication mechanism. The encrypted values are decrypted. The decrypted values are collected as a list. With the list of values, the user tries to guess a valid user's login and password. Once the user is valid, the system will allow accessing the resources.

CAPTCHA is a technique to differentiate between human and the script. To test, whether the user is a human or a nonhuman that particular test is called as Reverse Turing Test.

C. CAPTCHA in AI

The earlier CAPTCHAs has text as an image, and the user needs to type the letter inside the space in order to login to the system Sometimes it is very hard to recognize the test. Google came up and it overcomes the earlier version of CAPTCHAs into a new artificial intelligence system. Scientists were working on this by using various machine learning algorithm by converting the text into an image.

D. Deniel-of-a-service attack in CAPTCHA:

Deniel of service attack is an attack in which the user with proper login credentials can login access the resources. Otherwise, the access s denied to the user.DOS is performed with the help of bots; bots is an automated software. Bots send the huge fake information as a request to the server in which the server buffer becomes full and this leads to DOS attack. CAPTCHA is a very useful technique in the DOS attack. In the captcha, the user types the text that is given in the text box and likewise it is verified as a human or not.

V. USABILITY

The usability study involved 30 participants from various backgrounds in testing the next generation CAPTCHA in terms of understanding, the level of complexity, time taken, and user experience. The first test is time taken to understand the mini game compared with text-based or any other times of CAPTCHAs; the result shows its almost 20% easy to understand. The second test is the level of complexity of game CAPTCHA, which is too simple to complete the task. The Completion success rate comparison graph is given in Figure 10.

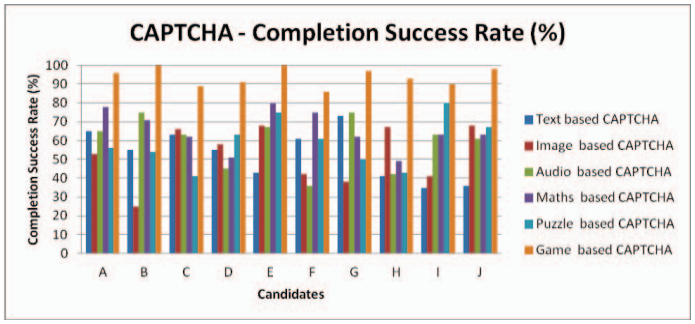

Figure 10. Completion Success Rate(%) graph

In figure 11 shows the time taken to complete the CAPTCHA is half of the time compared with any other types of CAPTCHAs, because the user need not type anything to solve CAPTCHA, they can simply click or drag-and-drop using a mouse in PC and tap or swipe in smartphones. Since no plug-in are required to run the game-CAPTCHA, it can be supported almost all king or browsers in either Mobile or PC.

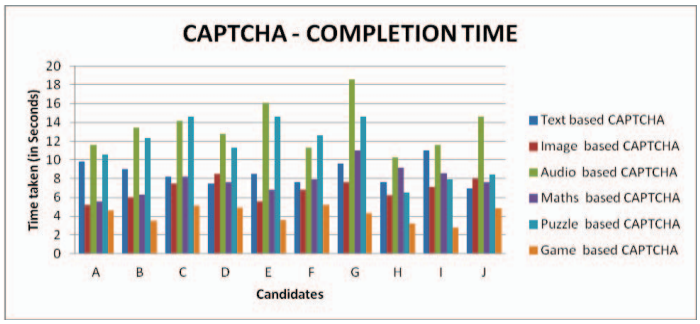

Figure 11. Completion time comparison graph

VI. CONCLUSIONS AND FUTURE WORK

In the earlier techniques of CAPTCHAs, the user sees only the text image and some CAPTCHAs provided by the particular service providers are very tedious and text will be very complicated to type and recognize and use the service. The study was conducted for 30 participants from various fields for testing the performance the future generation

CAPTCHA. On comparing the earlier technique and future generation CAPTCHAs. The time taken by the user is relatively less compared to the old technique because in the old technique the text was used and in the future technique mini games were used, the user can play the game in order to authenticate as a human being.

REFERENCES

[1] Ved Prakash Singh, Preet Pal, "Survey of Different Types of CAPTCHA" in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2242-2245, 2014.

[2] Wei-Bin Lee, Che-Wei Fan, Kevin Ho, Chyi-Ren Dow, and "A CAPTCHA with Tips Related to Alphabets Upper or Lower Case," in Seventh International Conference on Broadband, Communication, Wireless Computing and Applications, 2012.

[3] Baljit Singh Saini and Anju Bala "A Review of Bot Protection using CAPTCHA for Web Security," IOSR Journal of Computer Engineering, 2013, pp. 36-42, 2013.

[4] Are You a Human. https://www.areyouahuman.com/.

[5] CAPTCHA: http://www.captcha.net/

[6] S. Benson Edwin Raj, Deepa Devassy and Jiji Jagannivas "A New Architecture for the Generation of Picture Based CAPTCHA," IEEE, pp. 67-71, 2011.

[7] Aditya Raj, Ashish Jain, Tushar Pahwa and Abhimanyu Jain "Picture CAPTCHAsWith Sequencing: Their Types and Analysis," International Journal of Digital Society, vol. 1, no. 3, pp. 208-220, 2010.

[8] Y. Soupionis and D. Gritzalis. Audio captcha: Existing solutions assessment and a new implementation for VoIP telephony. Computers & Security, 29(5):603–618, 2010.

[9] Haichang Gao, Dan Yao, Honggang Liu, Xiyang Liu and Liming Wang. A Novel Image Based CAPTCHA Using Jigsaw Puzzle, 13th IEEE International Conference on Computational Science and Engineering,11-13 Dec. 2010.

[10] CJ Hernandez-Castro, A Ribagorda "Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study"computers & security, 2010 - Elsevier