International Journal of Engineering Research and General Science Volume 4, Issue 3, May-June, 2016
ISSN 2091-2730

A Novel Approach for Dynamic Authentication by combining Captcha, Graphical Password and OTP in a Web Enabled System

A. Nagarathinam[1], R. S. Subashinee[2]

[1]Associate Professor, Department of Computer Applications, AVC College of Engineering, Mayiladuthurai, India
rathnaarumuga@gmail.com

[2]Project Engineer, Wipro Technologies, India

Abstract— Password authentication is the major issue in implementing any access control. In general, a text comprising of alphanumeric characters of a minimum length will be the password to enter into a system. When the user enters the correct sequence of characters, it will be considered as a valid password and he/she will be allowed to access the system. However, when the password is not correct, the access will be refused. Software applications such as Internet bot or the web robot are used to execute simple and repetitive tasks automatically over the Internet at a much higher speed than human beings. They imitate the real user and continuously try for different combinations of password to break the authentication process.
Captcha is mainly applied to prevent automated execution of actions by the Internet bots on behalf of authenticated humans. The aim of Captcha is to make difficult for automated programs to break the authentication by asking them to pass an assessment that is simple for human beings and is rigid for computer programs. The combination of Captcha, graphical password and OTP is applied to ensure a higher level of authentication.

Keywords– Captcha, Graphical password, OTP, internet bot, challenge-response test, HIP, clickable point, click fraud.

1. INTRODUCTION

CAPTCHA is a backronym for "Completely Automated Public Turing tests to tell Computers and Humans Apart". It is the category of Turing test namely challenge-response test and a part of Human Interaction Proof system (HIP) [1]. A backronym is created by generating an innovative phrase to fit an already existing word, name, or acronym.
Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford were proposed the term captcha in the year 2003 [2]. It is pronounced as cap-ch-uh. The intention of using a captcha is to assure that the response has been generated by a human being and not by a computer.

Some of the significant malicious problems of internet bots are Denial-of-service attack. DoS attack is enforced to make a server or a network resource unavailable to users. A temporary suspension or interruption may happen because of the oversupply of a service.

The other problem of internet bots is click fraud. In some online marketing, a kind of scam called a click fraud reproduces a legal user of a web browser by clicking on an advertisement to make a charge per click without having a real concern. They are used to get money from advertisers or publishers. In addition to that, they are also used to increase the hit count of a service supported by a particular website such as YouTube videos.

2. RELATED WORK

Different types of captcha are used for authentication.

2.1. Types of Captcha

i. Text-based Captcha

The text based Captcha may consist of either simple questions that are easy to answer or some distorted image of a word [3]. Some Captcha designs follow the principle of hard to separate text from background [4].

Fig. I A Text-based Captcha

ii. Audio-based Captcha

Audio based Captcha is developed for visually disabled users. After listening to the spoken word, the user has to enter the captcha.

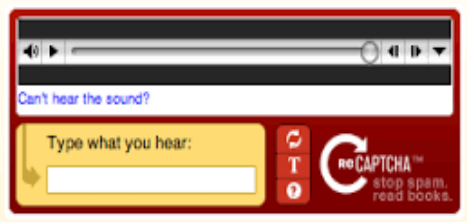


Fig. II An Audio-based Captcha

iii. Image-based Captcha

In the picture based captcha, the images of objects, animals, flowers, persons, places and fruits or birds are given for authentication. The human being can easily identify the correct picture from the visual puzzle. The important characteristics of images namely edge detection with thresholding, shape matching and random guessing have played an important role in picture based captcha mechanism [5].

Fig. III A Picture-based Captcha

iv. Video-based Captcha

VidoopCAPTCHA is a verification solution that uses Video based CAPTCHA. It will show a video, and then ask the user to enter some tags related to the video [6]. The user's tag must match with the set of automatically created tags. Then only the test is said to be accepted [12].

Fig. IV A Video-based Captcha

v. Mathematical-based Captcha

In this type, some simple mathematical problem has to be solved. Example,
What is two plus seven? The user should not type 2+7. Instead he/she has to enter the solution 9.

Fig. V A Math-based Captcha

vi. 3D Captcha

3D captcha works based on human imagination and ability to distinguish between different types of objects. The assumption is that a computer program cannot identify 3D content as it is an inherent part of human visual system. Hence, a high level of resistance against attacks can be assured [7].

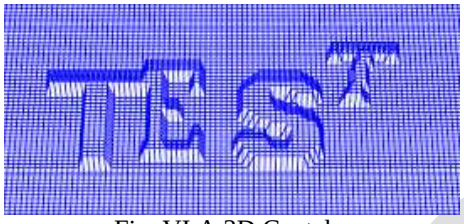


Fig. VI A 3D Captcha

vii. Ad-Injected Captcha

Ad-injected captcha is also known as commercial captcha. It is used to earn some money when the ad has been clicked. It is normally used for promoting and recognizing a brand.

Though the text based captcha is very simple, it is easy for the bots to identify and reproduce the same by making different combinations of characters randomly. For the automated software programmes, picture captcha is quite complex to identify the correct password. It is difficult for them to differentiate the type of objects given in an image, whether it is a flower or animal or fruit etc [8].

There are three categories of a graphical based password schemes namely recognition-based system, pure recall based system and cued recall based system [9]. Recognition-Based Captcha as a graphical password includes ClickText, ClickAnimal and AnimalGrid techniques [10] [11].

In general, Captcha satisfies three properties namely, easy for the human being to pass, flexible for the tester machine to grade it and rigid enough for a bot to pass [12]. Captcha with graphical password is used in visual cryptography [13].

3. MODULES OF PROPOSED SYSTEM

A high level security has been given to the proposed system namely Web Enabled System for Petrol Bunk Dealership Management. The system is used for automating the various activities that have been carried out in the petrol bunk. In the proposed system, a graphical picture is used as a captcha. Instead of selecting an entire image as a password, now the user has to register a particular pixel of the image as a password. After a clickable point in an image is selected, an image of n × n grid will be created internally, with the grid-cell size equaling the bounding rectangle of the selected image. The corresponding pixel of that clickable point will be stored in the authentication database for future verification. Also, the user has to enter his/her mobile number.

When the user wants to access the web system, first he/she has to identify the corresponding clickable password point on the image. Then the server will try to check whether this point is same as already stored in the database. If so, the user will be allowed to access the system. Otherwise, the system will give chance to the user to find the correct nearest clickable point for maximum of three times. Within that threshold (three) times, the user has to identify the correct pixel (a location closest to the pixel) as the captcha to access the system.

If still it is not possible to identify the correct pixel, the system will deny the access to the user. In addition to this security level, an OTP will be automatically generated to the user mobile. This correct OTP has to be entered in order to access the system. Thus, a two level authentication has been provided.

The major modules of the system are listed below.

3.1 Adding captcha images

The admin uploads the image for the client. By using this image, client can set the image password for security.

3.2 Add product info

The admin adds information about the availability of a stock to the client. It consists of how much amount of petrol, diesel they have. It also specifies the rate of petrol, diesel and the capacity of the tanker.

3.3 View Product Information

The admin maintains the record for determining how many liters of petrol and diesel were sold. Date wise transaction detail will be displayed.

3.4 View Client Information

The admin can view the profile of the registered client. After the admin activated the client, the client will be able to login to the particular account.

3.5 View Order Information

The admin will see the client's order. The client can purchase the specified petrol and diesel through online after getting the approval from the admin.

3.6 Export Petrol and Diesel

The client can purchase the petrol and diesel. The client has to specify the requirement. The amount will be automatically calculated.

3.7 View order status

The client can see whether his/her requests are accepted by admin or not. Initially, the order will be in pending state until the admin accept the request.

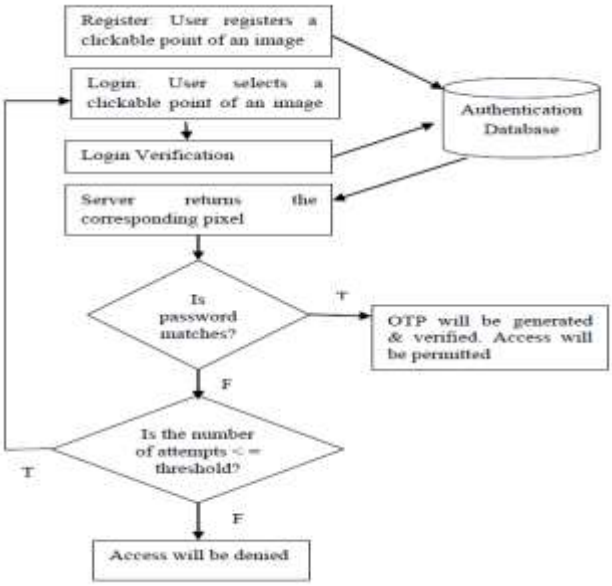


Fig. VII Overall module diagram of Proposed System

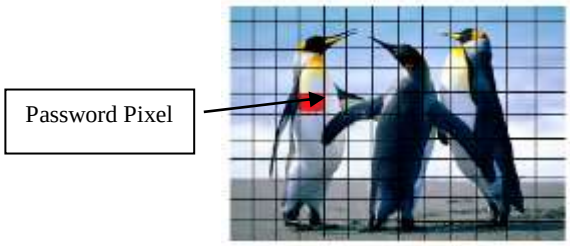
The figure VII shows the overall module diagram of the proposed system.

4. WORKING PRINCIPLE OF PROPOSED SYSTEM

The original image used for authentication is:

Fig. VIII Original Image

Now, the user has to register a particular clickable point (pixel) in this image. The red color shows the selected pixel. The corresponding position will be stored in the database for future verification.



During the login, when the user selects pixel, the corresponding location will be retrieved and sent to database for verification. Once both are matched, an One Time Password will be generated to the user to ensure higher level authentication. An user may select alternative pixel only for the given threshold (three times). Thus, click fraud can be eliminated.

5. CONCLUSION

Users normally choose passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often difficult to recollect. Graphical password and Captcha are the alternative solution for the above problem. As the picture is more attractive for the human beings than text, it can be easily remembered by them. Unlike the static passwords, the OTP is non vulnerable to replay attacks. Hence the combination of using Captcha, Graphical password and OTP leads to more security to the Web application. It is also the most applicable safety method on touch-screen devices.

REFERENCES:

[1] Chellapilla K, and Simard P, "Using Machine Learning to Break Visual Human Interaction Proofs (HIPs)", NIPS 2004, MIT Press, 2004.
[2] Wei-Bin Lee, Che-Wei Fan, Kevin Ho, Chyi-Ren Dow, "A CAPTCHA with Tips Related to Alphabets Upper or Lower Case", in Seventh International Conference on Broadband, Communication, Wireless Computing and Applications, 2012.
[3] Ved Prakash Singh, Preet Pal, "Survey of Different Types of CAPTCHA", International Journal of Computer Science and Information Technologies, Vol. 5(2), pp. 2242-2245, 2014.
[4] Niket Kumar Choudhary, Rahul Patil, "CAPTCHAs based on the Principle-Hard to Separate Text from Background", International Journal of Computer Science and Information Technologies, Vol. 5(6), pp. 7501-7503, 2014.
[5] S. Benson Edwin Raj, Deepa Devassy and Jiji Jagannivas, "A New Architecture for the Generation of Picture Based CAPTCHA", IEEE, pp. 67-71, 2011.
[6] http://vidoop.com/captcha.
[7] V. D. Nguyen, Y. W. Chow and W. Susilo, "On the security of text-based 3D CAPTCHAs", Computers and Security, Elsevier, pp. 84-99, 2014.
[8] Matthew Dailey, Chanathip Namprempre, "A Text-Graphics Character CAPTCHA for Password Authentication", in Tenth IEEE Conference, TENCON 2004.
[9] Mira K. Sadar, Pritish A. Tijare, Swapnil N. Sawalkar, "Review on Captcha: Graphical Password for Security", International Journal of Research in Advent Technology, Vol. 3(1), pp. 80-84, 2015.
[10] Jayshree Ghorpade, Shamika Mukane, Devika Patil, Dhanashree Poal, Ritesh Prasad, "Novel Method for Graphical Passwords using CAPTCHA", International Journal of Soft Computing and Engineering, Vol. 4(5), pp. 77-79, 2014.
[11] Anuradha. V, M. Nagesh, N. Vijaya sunder sagar, "A Survey on Graphical Passwords in Providing Security", Journal of Advanced Engineering and Global Technology, Vol. 3(8), pp. 1022-1027, 2015.
[12] S. Karthika, Dr. P. Devaki, "An Efficient User Authentication using Captcha and Graphical Passwords - A Survey", International Journal of Science and Research, Vol. 3(11), pp. 852-855, 2014.
[13] Khadija Kaousar M A, "Trio Framework For Secure Online Transaction Using Visual Cryptography", International Journal of Science and Research Publications, Vol. 3(5), pp. 1-4, 2013.