ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

# MOUSE CURSOR BASED AND TEXT BASED CAPTCHA SECURITY

**Ms. Sonika A. Chorey[*1] and Prof. S.V.Dhopte[2]**
[*1]M.E. in Information Technology, P.R.M.I.T.R,,Badnera.
[2]Associate Professor Dept. of Information Technology.P.R.M.I.T.R, Badnera.

## ABSTRACT

CAPTCHA is an image of distorted letters is dynamically generated. Since the letters are a part of an image and not text, it is difficult for a spam bot or other computer program to read. CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and humans Apart." The process usually involves one computer (a server) asking a user to complete a simple test which the computer is able to generate and grade . Captcha is a so called win-win solution, in that if a bot cannot break it, it provides security, but if it is automatically broken, that means that a difficult task in computer vision or related areas has been solved. . In this paper combination of image based capcha and text based captcha. When both CAPTCHA's are passed by the user then user got authenticated.

***Keywords***— *CAPTCHA, Cryptography, Authentication,cursor,image captcha.*

## I. INTRODUCTION

CAPTCHA is an acronym for "**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **h**umans **A**part." It is a type of challenge-response test used in computing to ensure that the response is not generated by a computer. The process usually involves one computer (a server) asking a user to complete a simple test which the computer is able to generate and grade. Because other computers are unable to solve the CAPTCHA, any user entering a correct solution is presumed to be human. A common type of CAPTCHA requires that the user type letters or digits from a distorted image that appears on the screen [1].

CAPTCHA is an image of distorted letters is dynamically generated. Since the letters are a part of an image and not text, it is difficult for a spam bot or other computer program to read. A human, in fact, has little trouble reading the letters in a captcha image. Using a captcha test on a website is a great way to ensure, for instance, that a person and not a spambot is filling out a web form. For example, humans can read distorted text as the one shown in Figure 1, but current computer programs cannot. Captcha is a so called win-win solution, in that if a bot cannot break it, it provides security, but if it is automatically broken, that means that a difficult task in computer vision or related areas has been solved. The problem with current visual text based captcha systems is that most of them have proven to be either not robust enough (they have been broken) or they are too complicated or annoying to read even for humans [2].

One common application of CAPTCHA is for verifying online polls. In fact, a former Slashdot poll serves as an example of what can go wrong if pollsters don't implement filters on their surveys. In 1999, Slashdot published a poll that asked visitors to choose the graduate school that had the best program in computer science. Students from two universities -- Carnegie Mellon and MIT -- created automated programs called **bots** to vote repeatedly for their respective schools. While those two schools received thousands of votes, the other schools only had a few hundred each. If it's possible to create a program that can vote in a poll, how can we trust online poll results at all? A CAPTCHA form can help prevent programmers from taking advantage of the polling system [3].

Registration forms on Web sites often use CAPTCHAs. For example, free Web-based e-mail services like Hotmail, yahoo mail or gmail allow people to create an e-mail account free of charge. Usually, users must provide some personal information when creating an account, but the services typically don't verify this information. They use CAPTCHAs to try to prevent spammers from using bots to generate hundreds of spam mail accounts [1].

**Figure.1.CAPTCHA**

ISSN 2348 – 8034
Impact Factor- 3.155

The most common form of CAPTCHA requires visitors to type in a word or series of letters and numbers that the application has distor-ted in some way. Because computers aren't always able to identify words from a digital scan, humans have to verify what a printed page says. Then it's possible for search engines to search and index the contents of a scanned document [4].

## II. CAPTCHA CHARACTERISTICS

The Website implements two kinds of CAPTCHAs, audio and visual. In the audio CAPTCHA, two male voices speak simultaneously, and the user has to type only the numbers that are spoken. The visual CAPTCHA has a wide vocabulary and uses different backgrounds, fonts, and texture. For example, in the CAPTCHA in Figure 5, the letters are made of separated dots, which are not trivial to cluster together to a letter shape by an algorithm [5].

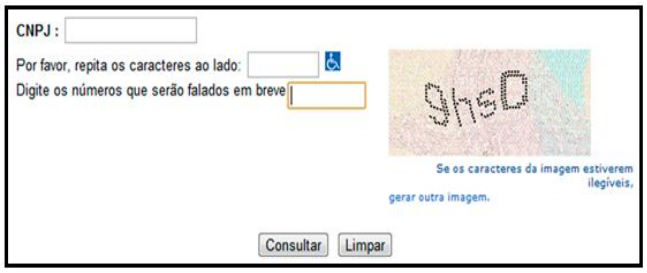


**Figure 2.The CAPTCHA interface provided by Agency**

## III. TYPES OF CAPTCHAs

CAPTCHAs are classified based on what is distorted and presented as a challenge to the user. They are:

### 3.1Text CAPTCHAs

These are simple to implement. The simplest yet novel approach is to present the user with some questions which only a human user can solve. Examples of such questions are:

1. What is twenty minus three?
2. What is the third letter in UNIVERSITY?

Such questions are very easy for a human user to solve, but it's very difficult to program a computer to solve them. These are also friendly to people with visual disability – such as those with colour blindness. Other text CAPTCHAs involves text distortions and the user is asked to identify the text hidden.

### 3.2Gimpy

Gimpy is a very reliable text CAPTCHA built by CMU in collaboration with Yahoo for their Messenger service. Gimpy is based on the human ability to read extremely distorted text and the inability of computer programs to do the same. Gimpy works by choosing ten words randomly from a dictionary, and displaying them in a distorted and overlapped manner [6].

### 3.3 Ez – Gimpy

This is a simplified version of the Gimpy CAPTCHA, adopted by Yahoo in their signup page. Ez – Gimpy randomly picks a single word from a dictionary and applies distortion to the text. The user is then asked to identify the text correctly.

ISSN 2348 – 8034
Impact Factor- 3.155

**Figure 3. Yahoo's Ez – Gimpy CAPTCHA**

### 3.4 Baffle Text

This was developed by Henry Baird at University of California at Berkeley. This is a variation of the Gimpy. This doesn't contain dictionary words, but it picks up random alphabets to create a nonsense but pronounceable text. Distortions are then added to this text and the user is challenged to guess the right word. This technique overcomes the drawback of Gimpy CAPTCHA because, Gimpy Division of Computer Science, SOE, CUSAT **8** uses dictionary words and hence, clever bots could be designed to check the dictionary for the matching word by brute-force.

### 3.5 Bongo

Another example of a CAPTCHA is the program we call BONGO [2]. BONGO is named after M.M. Bongard, who published a book of pattern recognition problems in the 1970s [3]. BONGO asks the user to solve a visual pattern recognition problem. It displays two series of blocks, the left and the right. The blocks in the left series differ from those in the right, and the user must find the characteristic that sets them.

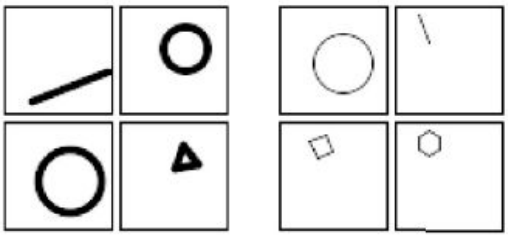

**Fig 4. Bongo CAPTCHA**

These two sets are different because everything on the left is drawn with thick lines and those on the right are in thin lines. After seeing the two blocks, the user is presented with a set of four single blocks and is asked to determine to which group the each block belongs to. The user passes the test if she/he determines correctly to which set the blocks belong to. We have to be careful to see that the user is not confused by a large number of choices [7].

### 3.6 Vidoop CAPTCHA

VidoopCAPTCHA2 is a verification solution that uses images of objects, animals, people or landscapes, instead of distorted text, to distinguish a human from a computer program. By verifying that users are human, the site and users are protected against malicious bot attacks. As shown in Figure 2, a Vidoop challenge image consists in a combination of pictures represen ting different categories. Each picture is associated with a letter which is embedded in it. In order to pass the challenge, the user is asked to report the letters corresponding to a list of required categories [8].

ISSN 2348 – 8034
Impact Factor- 3.155


**Fig 5.Example of an image challenge from VidoopCaptcha.**

### 3.7 Graphic CAPTCHAs

Graphic CAPTCHAs are challenges that involve pictures or objects that have some sort of similarity that the users have to guess. They are visual puzzles, similar to Mensa tests. Computer generates the puzzles and grades the answers, but is itself unable to solve it.

### 3.8 MSN CAPTHCHA

Microsoft uses a different CAPTCHA for services provided under MSN umbrella. These are popularly called MSN Passport CAPTCHAs. They use eight characters (upper case) and digits. Foreground is dark blue, and background is grey. Warping is used to distort the characters, to produce a ripple effect, which makes computer recognition very difficult.[8]


XTNM5YRE

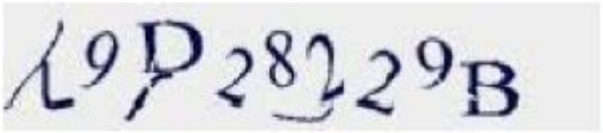
L9D28229B

**Fig 5 MSN Passport CAPTCHA**

## IV. PROPOSED SYSTEM

Incorporating a CAPTCHA into a web application, automated attempts to abuse the application can be thwarted. Existing CAPTCHAs have mainly focused on visual characters or object recognition tasks and have been deployed on many online services. A key area in security research and practice is authentication, the determination of whether a user should be allowed to access to a given system or resource. Generally, the most common and convenient authentication method is the traditional alphanumeric password. However, their inherent security and usability problems led to the development of graphical passwords as an alternative. To date, there have been several graphical password schemes, they have overcome some drawbacks of traditional password schemes, but most of the current graphical password schemes remain vulnerable to spyware attacks. CAPTCHA is a program that generates and grades tests that are human solvable, but beyond the capabilities of current computer programs.

ISSN 2348 – 8034
Impact Factor- 3.155

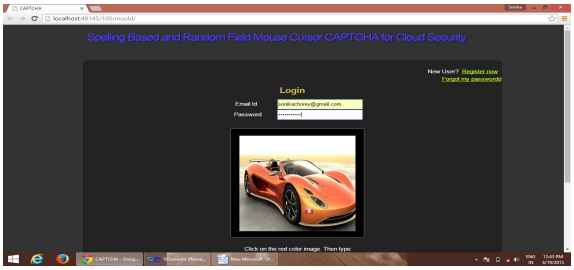


**Fig.6. image captcha**

So here we are going to present CAPTCHA which include a new technique that utilizes image from custom mouse cursors and outperforms some most popular CAPTCHA techniques such as Text – based CAPTCHAs and previous Image – based CAPTCHAs. So here we are providing combination of both image based and text base CAPTCHA first of all use will able to see one image that contains one small cross image which is diametrically situated in the main image user has to identify X co-ordinate and Y co-ordinate then challenge to click on that image and then user will going to clear the CAPTCHA test.

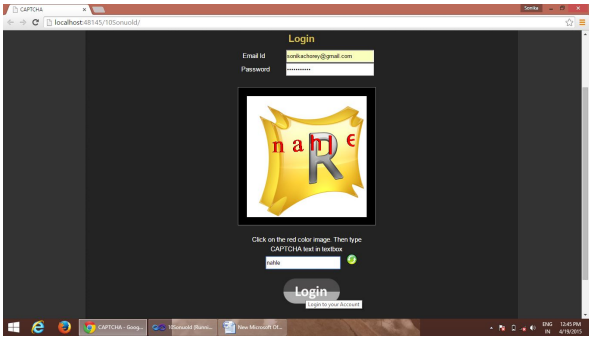


**Fig.7 text based captcha**

In figure 6 you can see that there is one image based captcha user has to clik on icon image which is place on background image that time user will clear that captcha test and get next test which is text based captcha you can see in fig 7. And once user enter correct text that time this test also get clear and user get authentication.

In this project we will going to give an environment of CAPTHCA creation under new concept of cursor in which first of all user has to click on the image in the area of nested image (image on image), then user can able to see CAPTCHA text image then user will going to type that CAPTHCA text after that user will clear that CAPTCHA.

## V. CONCLUSION

Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on Visual Cryptography".

The proposed methodology preserves confidential information of users using 3 layers of security. 1st layer verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website (website that is a fake one just similar to secure website but not the secure website), then in that situation, the phishing website can't display the image captcha for that specific user (who wants to log in into the website) due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website. Second layer cross validates image Captcha corresponding to the user.

The image Captcha is readable by human users alone and not by machine users. Only human users accessing the website can read the image Captcha and ensure that the site as well as the user is permitted one or not. So, using image Captcha technique, no machine based user can crack the password or other confidential information of the

ISSN 2348 – 8034
Impact Factor- 3.155

users. And as a third layer of security it prevents intruders' attacks on the user's account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

## REFERENCES

1. *Varun Ambrose Thomas, Karanvir Kaur "Cursor CAPTCHA – Implementing CAPTCHA Using Mouse Cursor" IEEE Conference 978-1-4673-5999-3/13-2013 IEEE*
2. *Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method'", in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.*
3. *karanvir kaur ,varun thombas " cursor CAPTCHA- captcha mechanisam using mouse cursor" international jornal of computer science volume 67 no.22,april 2013.*
4. *Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010*
5. *Nourian, A.; Ishtiaq, S.; Maheswaran, M.;" CASTLE: A social framework for collaborative antiphishing databases", in Proceedings of IEEE- 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2009.*
6. *Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3, n 4, p301-311, October/December 2006*
7. *Nirmal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'", in Proceedings of IEEE- International Conference on Emerging Trends in Robotics and Communication Technologies, 2010.*
8. *Tianyang Li.; Fuye Han.; Shuai Ding and Zhen Chen.; "LARX: Large-scale Anti-phishing by Retrospective Data-Exploring Based on a Cloud Computing Platform", in Proceedings of IEEE- 20th International Conference on Computer Communications and Networks, 2011.*
9. *Qingxiang Feng.; Kuo-Kun Tseng.; Jeng-Shyang Pan.; Peng Cheng and Charles Chen.; "New Antiphishing Method with Two Types of Passwords in OpenID System", in Proceedings of IEEE Fifth International Conference on Genetic and Evolutionary Computing,2011.*