Dynamically Generated CAPTCHA: Selection of Random Number Generated CAPTCHA for Enhancing Security

NidhiSingh[1], Mrs. ShubhaJain[2]

[1]M.Tech, Computer Science and Engineering, Kanpur Institute of Technology, Kanpur, India.

[2]Head of Department, Computer Science and Engineering, Kanpur Institute of Technology, Kanpur, India

ABSTRACT

In current scenario, most of the people having their login account on the internet sites and these sites are easily registered or accessed by human users. Sometimes, few unauthenticated software programs try to enter these sites and makes access on these sites and also keep on trying to hack the other users' resources through wrong registration. This thesis introduces "DYNAMICALLY GENERATED CAPTCHA" or it can be said that in this research we will try to select a random number that must be generated inside the CAPTCHA display for strengthen the security of the online applications that must be used by the internet. The advantage of this work is that when the random number must be entered in the enter CAPTCHA number box the correspondent CAPTCHA text must be display and after that when user type the CAPTCHA text inside the CAPTCHA text box and click on the register button then the user must reached to the home page and his or her registration must be successfully done. The proposed work has made it a flexible and reflexive by the use of dot net services to enhance the security of the web page.
Keywords: CAPTCHA, Refresh CAPTCHA. ASP.NET Using C#, Random Number Generated Levels.

1.INTRODUCTION

CAPTCHA can be described as the "Completely Automated Public Turing Test to tell Computers and Human Apart" as in [1]. CAPTCHA is a type of challenge-response test that is used in computing to determine whether a user is human or not. In this when the test is performed on CAPTCHA no computer is able to pass the test, even though they having the deep knowledge of working of CAPTCHA as in [2]. Nowadays, an internet has become an important communication tool. For using the facilities of the internet most of the time we have to register on it. But in current scenario, the hackers are performing an automatic registration on the internet sites by using computer program; this leads the wastage of resources of the sites. This can be easily resolved by the CAPTCHA. A good CAPTCHA must not only be the human friendly but also robust enough to resist computer programs that attackers/hackers write to automatically pass CAPTCHA tests. CAPTCHA resist the automatic registration over the internet provides the smooth registration process. In order to verify that registration request is submitted by individual user from online rather than the malicious software the academia proposed CAPTCHA scheme as in [1]-[3]. In this research paper, DYNAMICALLY GENERATED MULTIPLE CAPTCHA is presented. This method is implemented in such a way so that CAPTCHA levels display simultaneously along with the CAPTCHA. Each multiple CAPTCHA code is unique in nature. Multiple CAPTCHA along with their levels are refreshed at a fixed predefined interval of time. In this only CAPTCHA code and their levels are refreshing but not the whole web page. When any of the displayed CAPTCHA level is enter into box and submitted by the user then its correspondent CAPTCHA text is displayed, and when this displayed CAPTCHA text is entered and registered by the user than only the registration form is finally registered by the user over the internet. It restricts unauthenticated users to restrict illegal access to any resources.

2.LITERATURE SURVEY

The term CAPTCHA was coined by Luis Von Ahn, Manuel Blum and Nicholas.J.Hopper of Carnegie Mellon University and John Langford of IBM in 2000. The most common type of CAPTCHA was first invented by Martin Abadi, Mark.D.Lillibridge, Krishna Bharat and Andrei.Z.Border. This form of CAPTCHA requires that the user type the letters of the distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen as shown in fig. 1. Because this test is administered by the computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as the reverse Turing test.

Figure 1 Simple CAPTCHA

Pessimal Print CAPTCHA is the low quality of printed text images used certain rate of distortion was developed by Allison Coates, Henrys Baird and Richard Fate man of UC Berkeley in 2001 as shown in fig 2 in [4]. Against the attack this method is not very resistant in nature. Several times CAPTCHA can be classified on the basis of their contents. Gimpy Method is based on the dictionary. It must be having certain number of characters with some noise applied on their background either it must be horizontal or vertical in nature as shown in fig 3. Persian/Arabic Baffle Text CAPTCHA is the method in which pictures of Persian or Arabic words are shown for the purpose of distinguishing between users and computer figures but it can be used only for Arabic person language user as shown in fig 4 in [5]. Collage CAPTCHA is the method in which images of some different objects are selected, after that some rotation are done and they are merge to create a single image as in [6]. CAPTCHA2 method is just like a game. In this method instead of typing distorted text, it need just to click two times. First click on a letter given in CAPTCHA image precedes the new CAPTCHA image, click again on the correct letter and complete the process as in [7]. Time Variant CAPTCHA refreshes after a predefined fixed interval of time until final CAPTCHA submit by the user as in [8].

Figure 2 Pessimal Print CAPTCHA

Figure 3 Gimpy Method

3. PROPOSED WORK

It can always be seen that CAPTCHA is having the strong security therefore it is not easy to break it. CAPTCHA always requires the algorithm which is efficient and reflexive in nature. Unauthorized users have enough time to break the CAPTCHA security between the times of form loading to form submitting. Therefore, in this paper a new methodology to CAPTCHA is introduced known as "DYNAMICALLY GENERATED CAPTCHA". In this paper, CAPTCHA is not generated but it is implemented with the new method. In this method firstly DYNAMICALLY GENERATED MULTIPLE CAPTCHAs are displayed along with their levels it means levels are assigned to the multiple CAPTCHA that is random in nature for enhancing the security of the web page. These CAPTCHAs along with their levels are refreshing at a fixed predefined interval of time (maintain by the developer). Mainly we see that refresh CAPTCHA must be used in the online form but in this paper we will see that while entering the details on the login form that till the whole entries are not filled by the user and submitted by the respective user the multiple CAPTCHA along with their levels only refreshed at a fixed interval of time but not the whole web page. Therefore, due to regular refreshment of CAPTCHA along with their levels must be creating problem for the automated programs to break the security of CAPTCHA. Finally, for registering on a login form a user must have to filled complete entry and select one of the levels from the multiple CAPTCHA and when we register that level the correspondent CAPTCHA must be displayed, so when we enter that final CAPTCHA text and submit the form then only we can finally submit the form.

4. CONCEPT PREPARATION

Our work is to implement the methods that will select the random number generated CAPTCHA. When selected random number display in the box, then if we enter that displayed random number and submit it their correspondent CAPTCHA text will be displayed. As we introduce earlier, that multiple CAPTCHA displayed along with their levels

can only refreshed at a fixed interval of time and therefore only it cannot affect the web page. As we all know that unauthorized users and BOTs have enough time to break the CAPTCHA between the times of loading form to submitting form. Now we must write the following action:-

$$(CSC)_B \leftarrow {}_{Ttime} ((WPF)_F) \qquad (1)$$

Where, $(CSC)_B$ = CAPTCHA security checking on submit button
$(WPF)_F$ = Web Page Form is filled completely
Ttime = Total time to complete fill form
T_{time} is sufficient for the hacker to break the security of CAPTCHA due to its fixed code. Therefore, we implemented a new method for the CAPTCHA in which multiple CAPTCHA are refreshed along with their levels. This helps in enhancing the security of web page and since only multiple CAPTCHAs along with their levels are refreshed at a predefined fixed interval of time therefore it does not affect the web page. To resolve the problem of equation (1) here are some steps to select random number generated CAPTCHA with Time Variant System.

Algorithm to select random number generated CAPTCHA with Time Variant:-

1. Count ← $(S\_T)_{page\ load}$

2. Temp ← Count + T_P

3. Select Multiple $(Random\_Captcha)_{level}$ ← Temp

4. Refresh $((Captcha)_{code})$ ← Temp

5. Select Multiple $(Random\_Captcha)_{level}$ ← Refresh $((Captcha)_{code})$

6. Time ← Loop (Temp + T_P)

7. $(WPF)_F$ ← Time

8. $(CSC)_B$ ← Time

9. $(CSC)_B$ ← Time

Where, $(S\_T)_{page\ load}$ = System Time on page load
T_P = Predefined Time Period
Temp = Temporary variable for Time-Variant system
Select Multiple $(Random\_Captcha)_{level}$ = to select a level generated inside box change at each repetition
Refresh $((Captcha)_{code}$ = at each repetition Captcha is refreshed
T_{time} = Total time to complete fill form
$(WPF)_F$ = Web Page Form is filled completely
$(CSC)_B$ = Captcha Security checking on submit button
In eq (1) attackers or hackers have T_{time} to break CAPTCHA because it is enough time to break the CAPTCHA therefore we are generating levels also along the CAPTCHA in the new concept and there is (Temp + T_P) which is very small amount of time for displaying CAPTCHA and its levels because after (Temp + T_P) time CAPTCHA along with its levels will be refreshed. Now, this help in enhancing the security of CAPTCHA. The following algorithms are used to select random number generated inside CAPTCHA box after predefined time without affecting the whole web page:
Algorithm for Time Variant (System Clock):-
1. System – Time ←The time fetches by the system.
2. Temporary variable ← System – Time.
3. Temporary variable assigning to Time – Variant system ←Temporary variable + Predefined Time Period.
4. Condition: Select random number generated inside CAPTCHA box and CAPTCHA and its levels are refreshed after each time T_P.
5. Repeat step 2 & 3.

International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 1, January 2015   **ISSN 2319 - 4847**

Algorithm for generating random number inside CAPTCHA box for enhancing security:-
1. Home page and about page act as a secure page and if it redirects it reaches to login.aspx.
2. Login page is having the facility of new user which when redirects it reaches to registration page.
3. Define levels for CAPTCHA. i.e. (Captcha$_{level}$ = 1, 2, 3……., n) (For e.g.: - if we select CAPTCHA level 8 in the box, its   correspondent CAPTCHA text display in the box).
4. Now, at registration page generated CAPTCHA started working with its level.
5. Enter CAPTCHA number inside the box and submit it. (For e.g.: - (Captcha_Random) $_{number}$ = 1, 2, 3….n).
6. Generated random number from (Random number: For e.g.: - 1, 2, 3….n).
7. Enter the correspondent CAPTCHA text inside the box.
8. Repeat step 5, 6, 7 until form submits.
9. Condition: If CAPTCHA level and text matches.
10. Registration must be done successfully by the user and reaches to home page.

<div align="center">Where, (Captcha) $_{level}$ = Level of CAPTCHA text

(Captcha_Random) $_{number}$ = Random Number Generator</div>

Algorithm for submit button
1. Click on the submit button.
2. If any entry is empty then show a message dialog box.
3. Else.
4. If CAPTCHA and its level are matched then go to step 6.
5. Else next CAPTCHA and its level match.
6. End, registration complete.

5.RESULT

In this paper, the proposed work is implemented with ASP.Net Using C# technology to get efficient results. We are seeing the registration form with multiple CAPTCHA along with their levels snapshot at the time of page loading as shown in fig 5. Since, after predefined fixed time period multiple CAPTCHAs along with their levels are refreshed while the form is not completely filled.
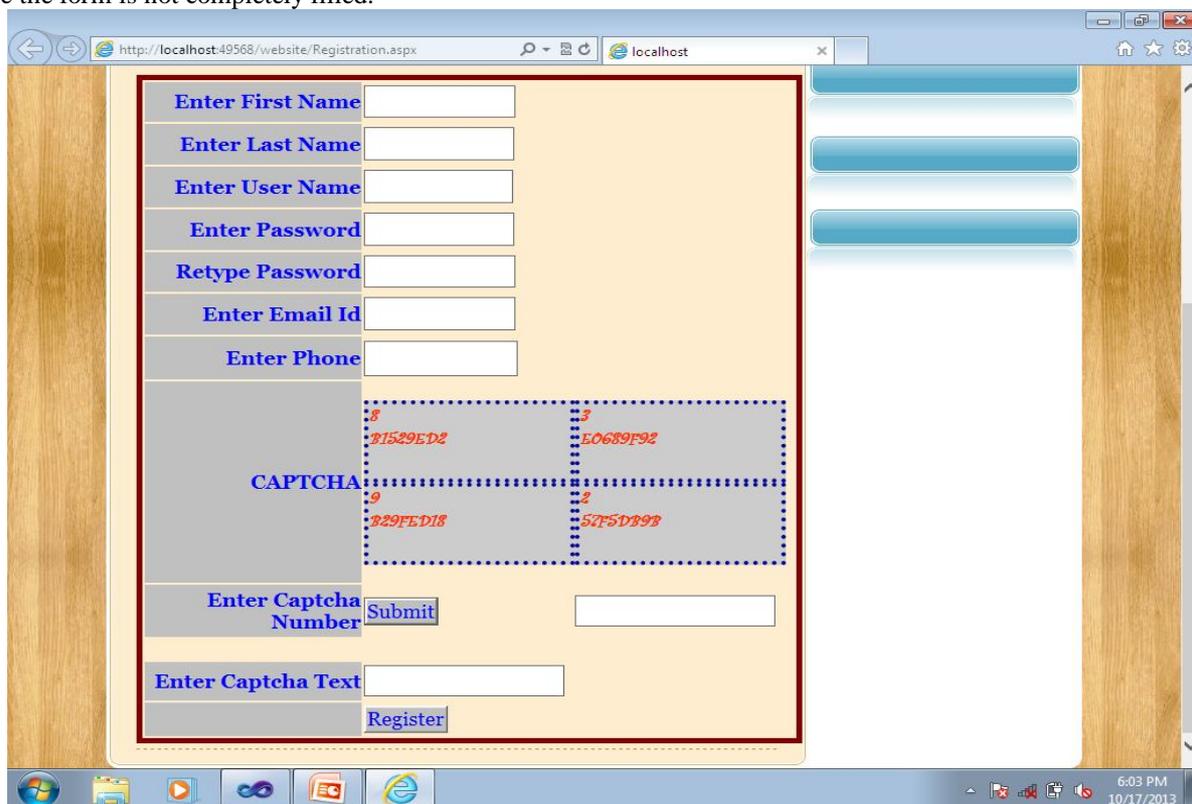

Figure 5 Registration form at the time of page loading

We can see that in fig 5 when the registration form is loaded than multiple CAPTCHAs along with their levels are different but after a predefined time period we can see that while user is filling form entries CAPTCHAs along with their levels are refreshed without affecting the whole web page in fig 6. After that in fig 7 we can see that till the whole form is filled, multiple CAPTCHAs along with their levels are refreshed after a fixed predefined interval of time again and again so that when we select any of the random number from the displayed random numbers and submit that particular random number than its correspondent CAPTCHA text must be displayed and this will enhance the security of CAPTCHA from the previous concept.
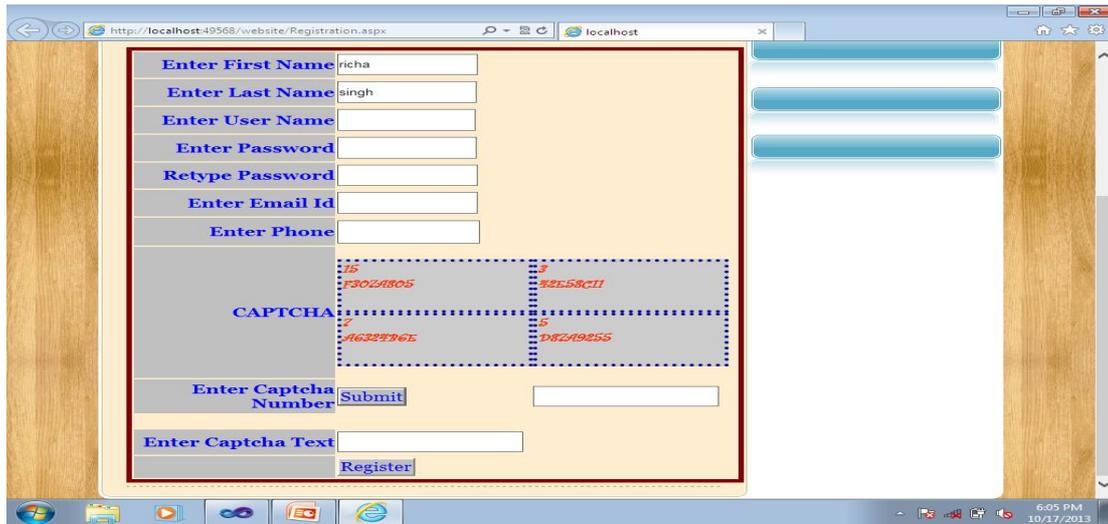
Figure 6 Multiple CAPTCHAs refreshes along with their levels after predefined fixed interval of time without affecting the whole web page

In fig 6, we can see that multiple CAPTCHAs along with their levels are refreshed again and again after a predefined fixed interval of time, since the complete required entries are not filled by the user. In this fig 6 it can also be seen that except CAPTCHA and its level all the entries remain constant in nature without affecting the whole web page. Therefore, it can be observed here that CAPTCHA and its level are working here as a security tool.
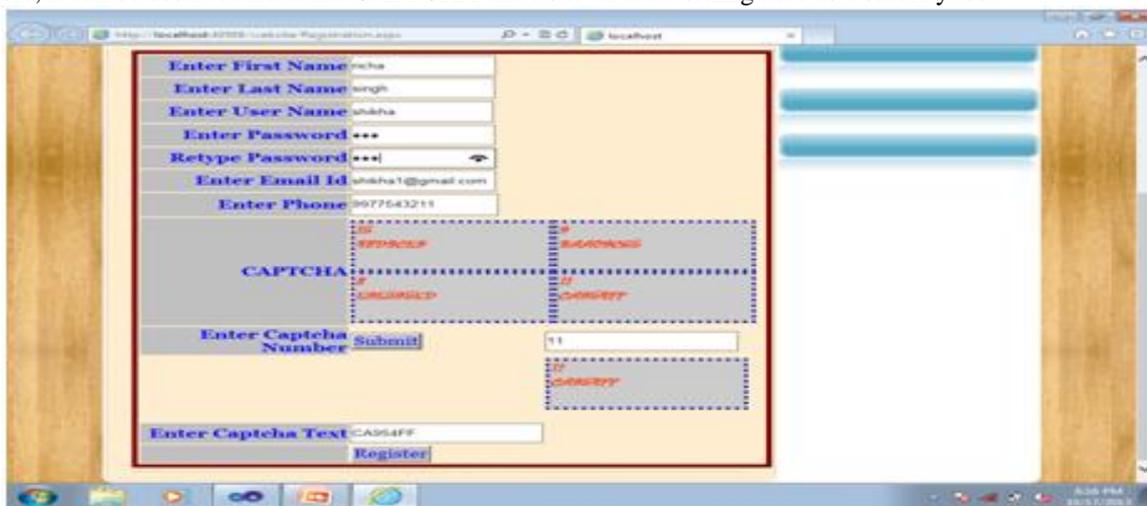

Figure 7 Registration form displays that the random number selected from multiple CAPTCHA boxes and when this number is submitted its correspondent CAPTCHA text displays without affecting the whole web page.

Figure 8 the user reaches to login page after performing registration

International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 1, January 2015   **ISSN 2319 - 4847**

Figure 9 User login id and password

Figure 10 Registration must be successfully done by the user

In fig 8 we can see that after performing registration the user reaches to login page. After login id and password by the user as shown in fig 9 the registration must be successfully done by the user as in fig 10.

6.CONCLUSION

In this paper, we introduce DYNAMICALLY GENERATED MULTIPLE CAPTCHA. These multiple CAPTCHAs along with their levels are refreshed at a predefined fixed interval of time for enhancing the security of CAPTCHA. In this paper, we are using the concept of sharing a system clock and this can be modified with the number counting calculation and the combination of CAPTCHA text and random number in the common box for enhancing the security of CAPTCHA. If we want to increase the more security of CAPTCHA then we can use the combination of CAPTCHA text, image and random number in the common box. This project is very much reflexive and efficient in nature therefore, only it can be used for enhancing the security of CAPTCHA over online applications.

REFERENCES

[1] L. von Ahn, M. Blum, N. Hopper, and J. Langford. CAPTCHA: Using Hard AI problems for Security in Advances in Cryptology EUROCRYPT 2003, page 646. DOI: 10.1007/3- 540-39200-9_18

[2] A.A.Chandavle, Dr.A.M. Sapkal and Dr.R.M.Jalnekar (2010) A framework to analyze security of Text based CAPTCHA International Journal of Forensics and Computer Application ,1 (27) , 127-132 (International Journal style)

[3] L. von Ahn, M. Blum, and J. Langford, "Telling Human and Computers Apart automatically," in Communications of the ACM, vol. 47, February 2004, no. 2, pp. 57-60. DOI: 10.1145/966389.966390

[4] Allison L. Coates, Henry S. Baird, Richard J. Fate man."Pessimal Print: A Reverse Turing Test", Proceedings, IAPR 6th Int'l Conf. On document Analysis and Recognition, Seattle, WA, September 10-13, 2001, pp.1145-1158

[5] M.H. Shirali-Shahreza and M. Shirali-Shahreja, "Persian/Arabic Baffle text CAPTCHA," Journal of University Computer Science(J.UCS), vol.12,no.12,December 2006, pp.1783-1796. DOI: 10.3217/jucs-012-12-1783

[6] M. Shirali-Shahreja and S. Shirali-Shahreja, "Collage CAPTCHA". In Proceeding of the 20th IEEE International Symposium Signal Processing and Application (ISSPA 2007), Sharjah, United Arab Emirates(UAE), February 2007. DOI:10.1109/ISSPA.2007.4555329

[7] http://Captcha2.com

[8] Time Variant Captcha: Generating Strong Captcha Security by Reducing Time to Automated Computer Programs. Prem Shankar Yadava, Chandra Prakash Sahu, Sanjeev Kumar Shukla VOL .2, NO. 12, December 2011. ISSN 2079-8407 (2)(journal style)