Data Security using Textual and Graphical Approach for CAPTCHA

Yogita N. Khadke
PG Student
Department of Computer Science & Engineering
G.H.Raisoni Institute, Jalgaon, Maharashtra

Mrs. Swati A. Patil
Assistant Professor
Department of Computer Science & Engineering
G.H.Raisoni Institute, Jalgaon, Maharashtra

Abstract

The Passwords are most commonly used method for identifying users in computer and communication system. Graphical password schemes motivated by improving password usability and security. A password authentication system should encourage strong and less predictable passwords while maintaining security. Users have difficulty remembering a password that is long and random-appearing. It satisfies both conflicting requirement that is, it is easy to remember and it is hard to guess. A method is proposed a new security using registered details with secured using generate CAPTCHA images. In the Registration Phase User will input the Password in graphical CAPTCHA image Phase. After Click on graphical CAPTCHA image User will be navigated to further Phase where a next step of button grid process and Select question process in this process set of a Mathematical and Logical questions will be displayed followed by an image CAPTCHA challenge. In Button grid technique used on log in process then generated by grid size on 10 * 10 matrix format and display on this matrix 0-9 numbers. Also, this process has completed on numbers are randomly shuffle. In this system security has been provide on user online guessing attack.

Keywords: Graphical password, CAPTCHA, Online security, Authentication, Security primitive

I. INTRODUCTION

CAPTCHA is a Completely Automated Public Turing test to tell Computers and Humans Apart. A type of challenge and test used to determine the user is human or not. Computers cannot get the distorted words in a CAPTCHA easily, but humans being can easily decipher the text. In the most common type of CAPTCHA user is provided with letters of a distorted image. Then the user solves the CAPTCHA by entering the correct characters. Security means the strength for preventing the variant attacks. The usability means the user friendliness of the CAPTCHA [1]. A password authentication system should encourage strong and less predictable passwords using for security. This password authentication system allows user choice towards stronger passwords [2]. Indeed, such an approach would entail of CAPTCHA inside a Graphical Password, Textual Password or both types of Password. The graphical password as classified into three parts to be mention on passwords: recognition, recall, and cued recall. It uses textual passwords augmented by of temporal order of input and the position in which characters are input [3].

II. PREVIOUS WORK FOR SECURITY USING CAPTCHA

First time CAPTCHA was invented in 2000 at CAPTCHA is an acronym for "Completely Automated Public Turning Test to tell Computers and Humans Apart". The progress of Internet, Web security has become an important issue [4]. The computer machine will be unable to answer and it means unable to break CAPTCHA. The proposed CAPTCHA technology principle, method of implementation, variations and comparison of the accuracy rates. They conducted various experiments to measure the viability and usability of this CAPTCHA approach [5]. A new security primitive relying on unsolved hard AI problems. CaRP is both a CAPTCHA and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a CAPTCHA challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. CaRP can also help reduce spam emails sent from a Web email service [3].

III. PROBLEM STATEMENT

An information security is a data security using CAPTCHA. CAPTCHA is a technique of information security that focuses on data security of existence information. In CAPTCHA in Authentication protocol use the both CAPTCHA and password. In guessing attacks, password guesses decreases with more trials, leading to a better chance of finding the password.

IV. PROPOSED SOLUTION

The proposed system which is called as Captcha and Graphical Password whose main intension is to provide security to the users of the system. The Proposed system is divided into two modules which are stated below.

A. Registration Phase:

In this module if a user is new to the system has registration. User should fill the information in registration form. In registration process user to fill in basic information. In Complete the registration process then user selects the CAPTCHA in animal name. In registration Process will be successful then user goes to in logging process.

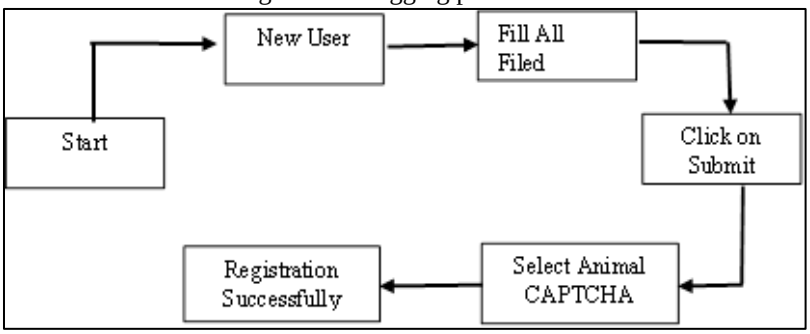

Fig. 1: Registration Process

B. Login Phase:

In Login process user is Existing or registered then user can login into the system. The proposed system is divided into two level simple login and complex login. In login process user will be select on one login process has been choose in depending on user. User will be select on simple login process. User fill on only user name then select on CAPTCHA animal name will be select on in existing CAPTCHA image. User has to click on wrong CAPTCHA image then system will be going to the next step on Button gird process. When the user will select on wrong two digit number then system will be go to the next step on Select Question process. In Select Question process user has to ask on mathematical and logical question. In this process randomly generated on this mathematical and logical question. User solves to the mathematical and logical question and answer will be depending on in same process of button grid process.

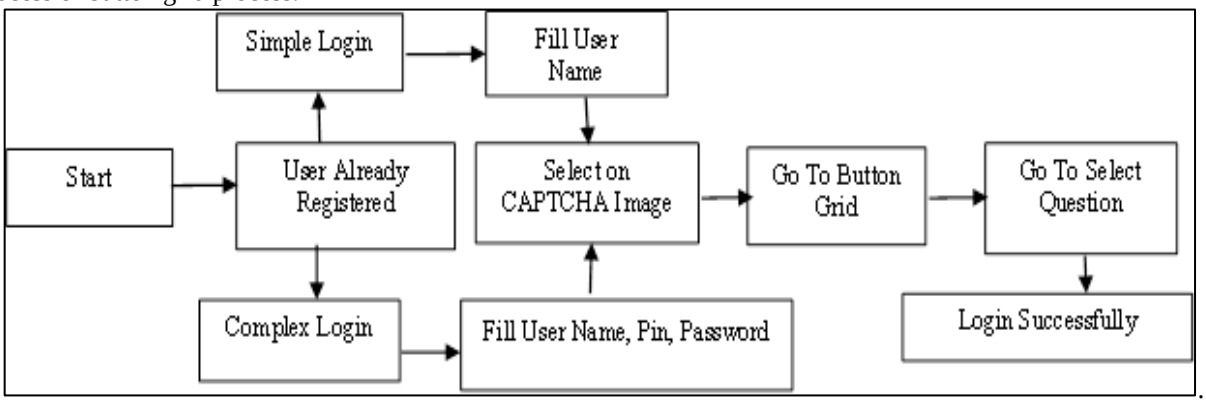

Fig. 2: Login Process

V. IMPLEMENTATION

A. Registration Phase:

New user on firstly completed on registration process. In New user has been Registration process then Fill about all Registration filed. After that user has to select a CAPTCHA image then display on massage this CAPTCHA for click and select a name of CAPTCHA image. This CAPTCHA image will be randomly generated on selected CAPTCHA then registration successfully.

B. Login Phase:

In login process using on two technique.

1) Simple Login -
   Logging using only graphical CAPTCHA as password.
2) Complex Login –

Logging using user name, Pin and Graphical CAPTCHA as password.

- Simple Logging Technique –
  User will be already registered on this process then user Fill on user name. After this process submit on user select CAPTCHA image. Then go to next process on button grid. After wrong select button grid then go to select question process and submit to logging process.
- Complex Logging technique-
  Step 1- User will be already registered on this process then Fill on user name, Pin and Password. After this process submit on user select CAPTCHA image. Then go to next process on button grid. After wrong select button grid then go to select question process and submit to logging process.

3) Pair-based Authentication scheme
   In this process is depending on button gird process and select question process.

- In Button Gird Process-
  In button grid of 10 * 10 on grid size and display on 0-9 numbers. This number is randomly placed and shuffle. This process will be depending on 4 digit pin. The 4 digit pin on divided in two pair. User consider on pair in digit number first two digits on one pair and last two digit on second pair then submit.
- In Select Question Process-
  In select question display on Mathematical and logical question image will be randomly generated. User will be solving this question on same concept of button gird technique. In this concept answer will be on two digit then consider as the before two digit put on zero-zero. After this process completed then this answer will be store on textbox then submit.

VI. RESULT AND ANALYSIS

A. User Opinion:

During each user has to trial on this process and user will be registered and login on this process. In these process 50 users has to register on this system. In this case user will be on three chances of login process. After this process will be completed then user answered on questions corresponds to that report in studies on question. In this process involved in research those users' questionnaires. It is most widely used approach to scaling responses in survey on research, such that the term is often used interchangeably with rating scale. In this process password were easy to create and quick to enter, but they remained impartial on their preference between text and graphical password. In this project we have survey for 50 users. The user will be rating on score is out of 10. The scores for those questions were reversed prior to calculating the mean and median, thus higher scores always indicate more positive results for this system as shown on Table 1 [2].

Table – 1
Questionnaire responses for Score is out of 10

Question	*Mean*	*Median*
I Could easily create a graphical password	*8.52*	*8.6*
Logging on using a graphical password was easy	*7.58*	*7.4*
Graphical passwords are easy to remember	*7.13*	*6.9*
I prefer text password to graphical Password	*5.54*	*5.8*
Text password are more secure than graphical password	*5.54*	*5.5*
I think that other people would choose different points than me for a graphical password	*4.34*	*4.4*
With practice, I could quickly enter my graphical password	*7.72*	*7.8*

B. Calculate Efficiency of Success Rate in Users:

Our project is survey on 50 users. User will be login process get on three chances then user depend on which login process will be selected. In this process calculate efficiency of user login successful or login failure. In this system 50 users is divide on group of 10 users. When each one user has to 3 chances then first group of 10 user is getting on 30 chances of our project result will be conclude. In first group of 10 users is mention on out of 30 chances will be get successful on 23? In second group of 10 users is mention on out of 30 chances will be get successful on 23? In third group of 10 users is mention on out of 30 chances will be get successful on 23? In fourth group of 10 users is mention on out of 30 chances will be get successful on 24? In fifth group of 10 users is mention on out of 30 chances will be get successful on 22. On this process will be calculated on percentage of success rate as shown on Table 2.

Table – 2
Efficiency of the success rate value in users

Users	*Success rate*	*Percentage of success rate*
1 – 10	*23/30*	*76.66*
11- 20	*23/30*	*76.66*
21- 30	*23/30*	*76.66*
31- 40	*24/30*	*80*
41 – 50	*22/30*	*73.33*

C. *Comparison between Simple Login Process and Complex Login Process Is Depend on User Login Time:*

In login time average will be calculate on participant of 50 users. The login time average over the 50 user participants on successful login attempts and the sample on maximum and minimum login time for each scheme. In simple login and complex login scheme average login time. Each scheme had to the average login time, indicating large variations of login time for each scheme. Which is confirmed by the great difference between the minimum and maximum login times in each column shown in table 3? In this project survey on 50 user depend on login process will be select on process. In this survey 32 user will be select on simple login process and 18 user will be select on complex login process. In this survey we are conclude the login time will be decrease on as compare to complex login process. In this survey we conclude that on this system complex login is better than as compare to simple login process. In this process minimum time is set on 0 as shown on Table 3.

Table – 3
Average Login Time For simple and complex method

Scheme	*Simple Login*	*Complex Login*
Average (T)	*45.30*	*47.22*
Maximum	*110*	*107*
Minimum	*0*	*0*

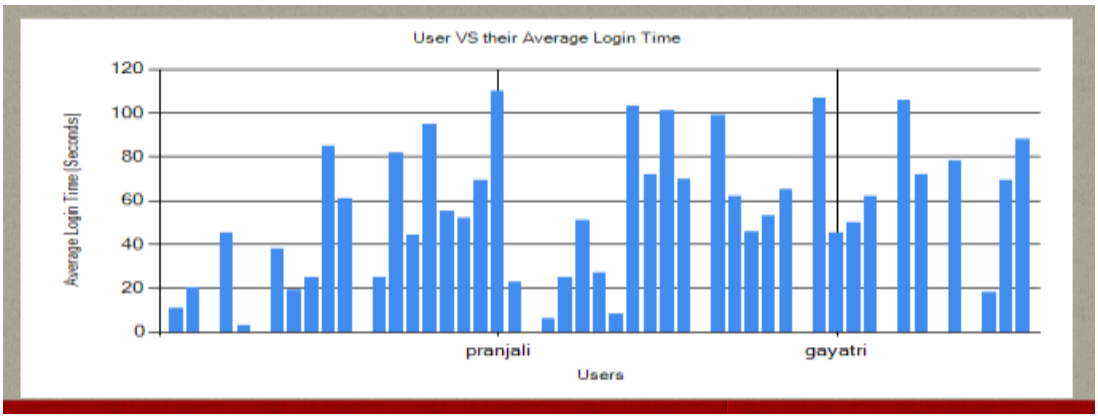

Fig. 3: The average login time increases with the decreases in the user.

Above graph shows the average login time increase with the decrease in the user login attempt. In this process calculate the average login time in user login attempt. Average login time is calculated in terms of seconds. In this process user will be depend on three chances to login phase, then user is derived on these three attempts will be of successful or failure. Fig. 3 shows average login time increases with the decreases in the user. In this process user will be attempt on login phase then calculate the average login time as shown in Table 3.

VII. CONCLUSION

We have studied the different kinds of CAPTCHA have developed yet. The clickable CAPTCHAs will simplify and speed-up the entry of the CAPTCHA solution. In this paper, a new security provide on the registration and login process. Graphical CAPTCHA process is better then click text CAPTCHA image because the human being in easily understand the graphical CAPTCHA password. In this way to proposed on pair-based authentication scheme is depend on button gird process and select on mathematical logical question. These techniques generate session password and resistant to remove on online guessing attacks. In this project it is concluded that on this system complex login is better than as compare to simple login process. Because user will be easily understand on graphical CAPTCHA password. In this paper also conclude as Graphical password will be better than on click text password. In this paper is depending on time consuming process. This project provides the security of user through login attempt. When user identity will change then login CAPTCHA also changes and this CAPTCHA will be send on your registered Email-Id.

REFERENCES

[1] Kumary R Soumya, Rose Mary Abraham, Swathi K V, "A Survey on Different CAPTCHA Techniques", International Journal of Advances in Computer Science and Technology, Volume 3, No.2, February 2014.
[2] Iranna A M, Pankaja Patil, "GRAPHICAL PASSWORD AUTHENTICATION USING PERSUASIVE CUED CLICK POINT", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, July 2013.
[3] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "CAPTCHA as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.
[4] Ved Prakash Singh, Preet Pal, "Survey of Different Types of CAPTCHA", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (2), 2014.
[5] Mandeep Kumar, Renu Dhir, "Design and Comparison of Advanced Color based Image CAPTCHAs", International Journal of Computer Applications (0975 – 8887) Volume 61– No.15, January 2013.