ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

# Data Security Using Textual and Graphical Approach for CAPTCHA

**Yogita N. Khadke[1], Mrs. Swati A. Patil[2]**

PG Student, Department of CSE., G.H.Raisoni Institute, Jalgaon, Maharashtra, India[1]

Assistant Professor, Department of CSE, G.H.Raisoni Institute, Jalgaon, Maharashtra, India[2]

***ABSTRACT*-C**omputer security depends largely on passwords in order to authenticate human users. The term password commonly refers to a secret used for authentication. Passwords are the most commonly used method for identifying users in computer and communication system. Graphical password schemes motivated by improving password usability and security. New graphical password schemes that exploit features of graphical input displays to achieve better security than text- based passwords. 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. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and more secure. Using hard AI (Artificial Intelligence) problems for security initially is an exciting new paradigm. Under this paradigm, the most notable primitive invented is CAPTCHA. It satisfies both conflicting requirement that is, it is easy to remember and it is hard to guess. This requires recognizing an image and using the recognized object as cues to enter a password. In recognition-recall CaRP, a password is a sequence of some invariant points of objects. 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 Click Text Phase. After Click Text Phase User will we be navigated to further Phase where a set of a Mathematical and Logical questions will be displayed followed by an image CAPTCHA challenge. Other technique used on log in process then generated by grid and display the 0-9 numbers. Also, this process has completed on numbers are randomly shuffle.

***KEYWORDS* –** Graphical Password, Security primitive, Captcha, Textual Password, Password, Click Text, Text Grid.

## I. INTRODUCTION

A CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) is a type of challenge-response test used to determine whether the user is human or not. Computers cannot decode the distorted words in a CAPTCHA easily, while humans 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. By definition

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

CAPTCHAs are fully automated, it requires little human maintenance. A good CAPTCHA will have two characteristics such as usability and security. Security means the strength for preventing the variant attacks, while usability means the user friendliness of the CAPTCHA [1].There are many things that are 'well know' about passwords; such as that user can't remember strong password and that the passwords they can remember are easy to guess [2]. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users 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 categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. It uses textual passwords augmented by some minimal graphical capabilities that enable the decoupling of temporal order of input and the position in which characters are input [3].

## II. PREVIOUS WORK FOR DATA 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].It proposed that various CAPTCHAs are compared in different aspects ICAPTCHA system provides simple and effective defense against 3rd party human solver attacks. The clickable CAPTCHAs will simplify and speed up the entry of the CAPTCHA solution [1].A new color based CAPTCHA is provides color based images to human and human will answer to interrogator with color name or so on the question asked during Turing test. These colored images can have single color image, more than one color image or it can have images with objects (like monitor, car, ower etc). For these types of questions, the computer machine will be unable to answer and it means unable to break CAPTCHA. That paper describes in detail 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. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to CAPTCHA relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service [6].

## II. PROBLEM STATEMENT

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

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.

**1. Registration Phase-**In this module if a user is new to the system he has to register first. We should enter his name and password along with the selection of hard AI problems from the predefined list of questionnaires. After selecting hard AI problem, one dynamic image will get generated. User need to solve that image and have to enter the answer in the textbox to register and to proceed for the login phase.

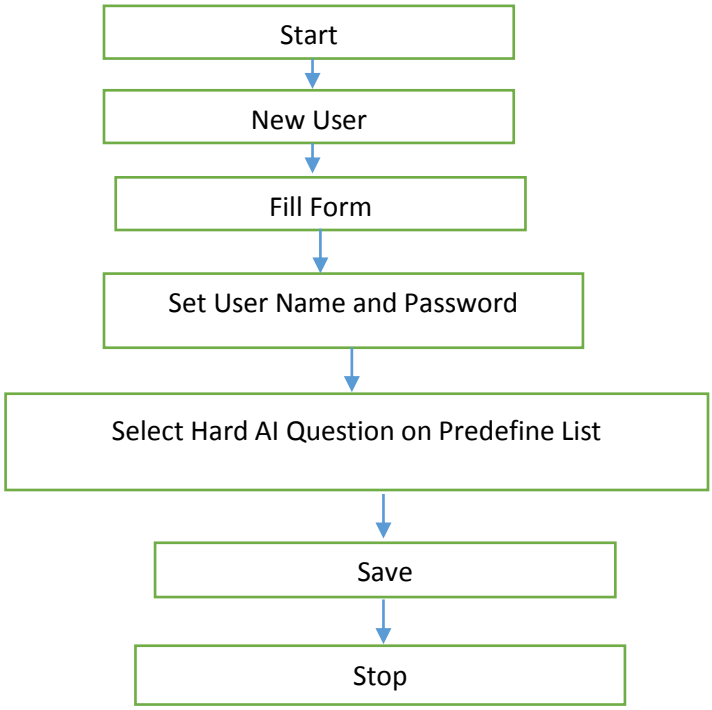


**Fig 1. Registration Process**

**2. Login Phase -** If user is Existing or registered user then user can login into the system. The proposed system is divided into two level authentication processes which consist of ClickText and TextGrid. This system will overcome the vulnerabilities of shoulder surfing attack and Thwart Guessing Attacks. While login, our proposed system will retrieve the current user's information such as IP address, Browser details and operating system information from the packets of HTTP header. Proposed system will analyses the historical data with the help of entered username. By analyzing the historical data,

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

proposed system will calculate the complexity of the user. The complexity is calculated by users' historical failed attempts per total attempts. If complexity is lower than simple CAPTCHA problems are generated and if complexity is higher than more complexes CAPTCHA get generated. As per the complexity level click text image will get generated. ClickText image is an image containing some set of clickable characters. The characters of the ClickText image will get shuffled randomly.

Every time a new ClickText image with random arrangement of characters will get generated. The ClickText complexity depends on the user's complexity level which is already calculated. Users have to click the appropriate points of characters on a ClickText image to enter password. This method will overcome the key logger problems. After ClickText a Text Grid will get generated where all character in the form of buttons will be randomly arranged into 2 dimensional matrixes. Along with the Text Grid one image will be displayed. The image will be random image which will change for each and every user for every login. User has to find the answer of Hard AI problem in the given image and have to enter the answer by using the Text Grid. Example: if User's answer is 15 than User has to select 1st Row and 5th Column and have to click the button which lies between 1st row and 5th Column. User will get authentication only after passing both authentication processes. If user gets failed in one or more authentication processes then user will be bet authentication error without any other information such as which authentication process has failed. This will resist the attackers for applying any guessing attacks.

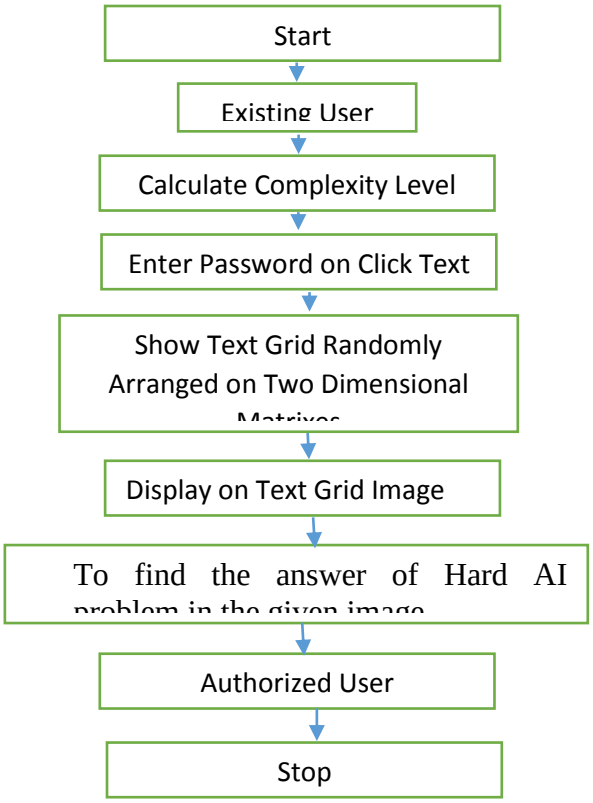


**Fig2. Login Process**

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 1, January 2016

## V. CONCLUSION

We have studied the different kinds of CAPTCHA have developed yet. In this paper various CAPTCHAs are compared in different aspects CAPTCHA system provides simple and effective defense against 3rd party human solver attacks. The clickable CAPTCHAs will simplify and speed-up the entry of the CAPTCHA solution. By using CAPTCHA as a graphical password we can ensure security better than other text based passwords which use hard mathematical cryptographic methods.

## VI. 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.

[6] 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.