

CAPTCHA as graphical passwords

Mr.Sagar Kambale¹,Mr.PramodKamble², Mr.Yogesh Dhavan³,Ms.Dipali Mahajan⁴,

MsRenuka Jadhav⁵,

¹²³⁴⁵ Student, Computer Science & Engineering ,Sanjay Ghodawat Institute, Atigre, Maharashtra, India

Abstract –The test that is generated and graded by computers in order to check the users to be human is Completely Automated Public Turing Test to Tell Computers and Humans Apart(CAPTCHA).

CAPTCHA can protect online and free services from bots that can access to services in huge numbers[5].A novel family of graphical password systems built on top of Captcha technology, which is called Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks and relay attacks. Paper provide a comprehensive overview of published research in the area, covering both usability and security aspects, as well as system evaluation. The paper _rst catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. The paper reviews usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats that such systems must address[1].

Keywords:-Server,Client,Remote, Monitoring, LAN

1. INTRODUCTION

1.1 Background

Security is most important in our daily life.In early system only text password is used which is very difficult to remember if enter a long password. If we use smaller password then it can be easily identified and we also use common password for many accounts so for that Image based captcha provide more security during authentication Captcha as graphical passwords (CaRP) is a program that has been used for preventing the robot to access the information and resources. There are a number of password guessing attacks that are prevented by CaRP.

Types of attacks :

_ Brute Force Attack: A Brute Force attack is a type of password guessing attack and it consists of trying every possible code, combination, or password until you _nd the

correct one. This type of attack may take long time to complete. A complex password can make the time for identifying the password by brute force long.

Dictionary Attack: A dictionary attack is another type of password guessing attack which uses a dictionary of common words to identify the user's password. It only tries complete options which are likely to work. The dictionary of possible combinations is based upon some likely values and tends to exclude remote possibilities. It may be based on knowing the key information about a particular target(family members names, birthdays, etc).

_ Relay Attack: A relay attack in computer security is a type of hacking technique related to man-in-the-middle and replay attacks. In a classic relay attack communication with both parties is initiated by the attacker who then merely replace messages between the two parties without manipulating them or even necessarily reading them.

1.2 Aim & Objective

The project aim is to show different techniques of captcha and graphical passwords in order to secure any application on network.To prevent various security attacks and give a reliable system.

1. To provide better security than traditional passwords.
2. To generate passwords di_cult to detect by bots.
3. To solve the limitations of the conventional text based password techniques, because pictures are easier to remember than texts.

1.3 Motivation

The most common computer authentication method is to use alphanumerical usernames and pass-words. This method of authentication forces you to remember username/password combinations to access accounts or special sections of a website. Password authentication protocols fail when you

don't address them seriously. This means constructing complex passwords and maintaining secrecy.

2. Literature survey

2.1 Related work

It was introduced to use both Captcha and password in a user authentication protocol, which is called *Captcha-based Password Authentication (CbPA) protocol*, to counter online dictionary attacks. The CbPA-protocol in requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access.

2.2 Problem statement

Bots are generated to perform guessing attacks on alphanumeric passwords. Captcha as Graphical passwords are proposed to prevent this vulnerability of alphanumeric passwords .CAPTCHA as graphical passwords provides high level of security than the previous password system.

3. PROPOSED SYSTEM

CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Our graphical password system is based on text password and graphical password. For successful login user has to select correct image which is chosen by user during a registration

3.1 Proposed Architecture

The fig 1 shows overview of proposed system.

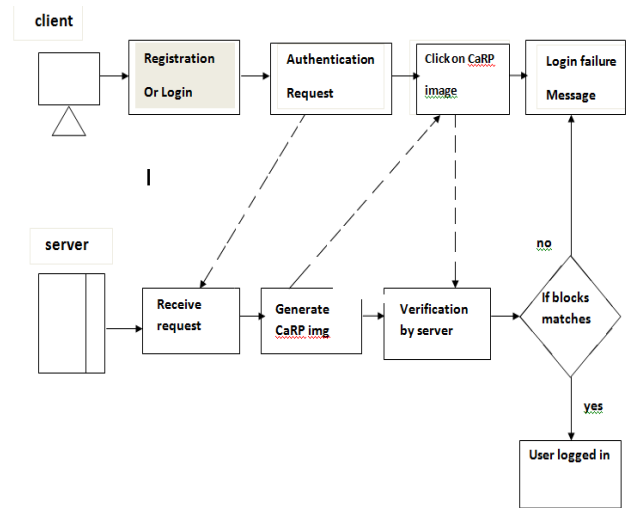


Fig -1: Basic Architecture model of System

4. WORKING METHODOLOGY

In CAPTCHA as a graphical passwords system ,there are four types or methods of CAPTCHAs implemented as follows :

4.1 Text CAPTCHAs

Text CAPTCHAs are randomly generated. These text CAPTCHAs are displayed to the user during the signing up process. These text CAPTCHAs distinguishes humans from bots.

4.2 Audio CAPTCHAs

Audio CAPTCHAs are second technique implemented in the system. During the user sign in process, user is provided with audio CAPTCHAs which are also generated randomly. User has to listen to it and type it as it is to sign in. This again distinguishes humans from bots.

4.3 Image CAPTCHAs

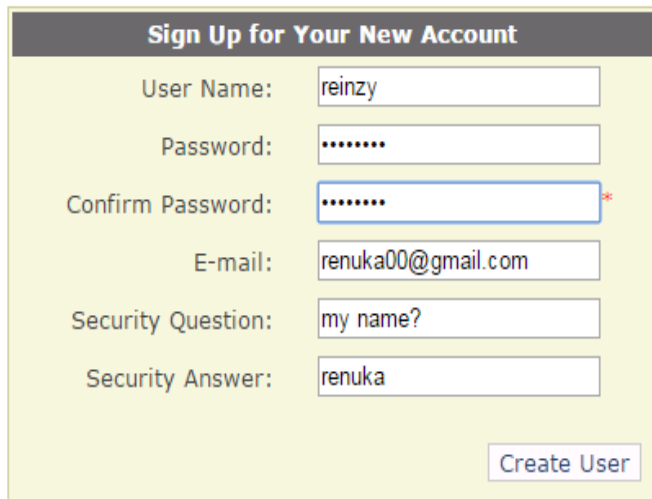
A method called Cued Clicked Points(CCP) is implemented under the image recognition based CAPTCHAs. Here the user will be provided with images, amongst which he has to select one and make five clicks anywhere on the image. These clicks are saved as password.

4.4 Video CAPTCHAs

Video CAPTCHAs are yet another technique in the CAPTCHA system. Here in this method a video is provided to the user during signing up process. There will be few questions displayed for user to answer based on the video. If the answers matches to the answers stored in the database user signs up successfully.

5. MODULE IMPLEMENTATIONS

5.1 User login:-



Sign Up for Your New Account

User Name: reinzy

Password:

Confirm Password:*

E-mail: renuka00@gmail.com

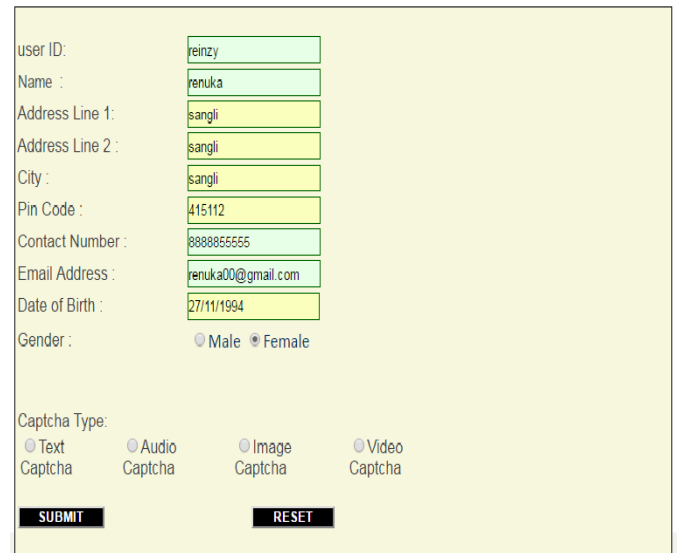
Security Question: my name?

Security Answer: renuka

Fig-5.1:User login

The above module is to get the basic details of the user. It includes fields like name, password, confirm password, email id, security question and its answer.

5.2 CAPTCHA Types:-



user ID: reinzy

Name : renuka

Address Line 1: sangli

Address Line 2 : sangli

City : sangli

Pin Code : 415112

Contact Number : 8888865555

Email Address : renuka00@gmail.com

Date of Birth : 27/11/1994

Gender : Male Female

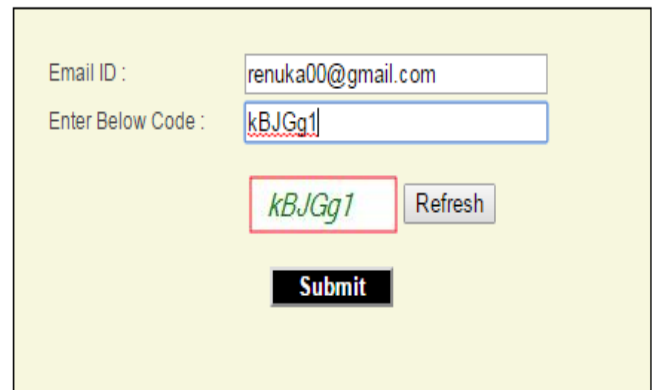
Captcha Type:

Text Captcha Audio Captcha Image Captcha Video Captcha

Fig-5.2:CAPTCHA types

The above module shows types of CAPTCHAs user can use to sign up.

5.3 Text CAPTCHA:-



Email ID : renuka00@gmail.com

Enter Below Code : kBJGg1

Fig-5.3:Text CAPTCHA

User has to see and enter the correct text CAPTCHA displayed in the text box.

5.4 Audio CAPTCHA:-

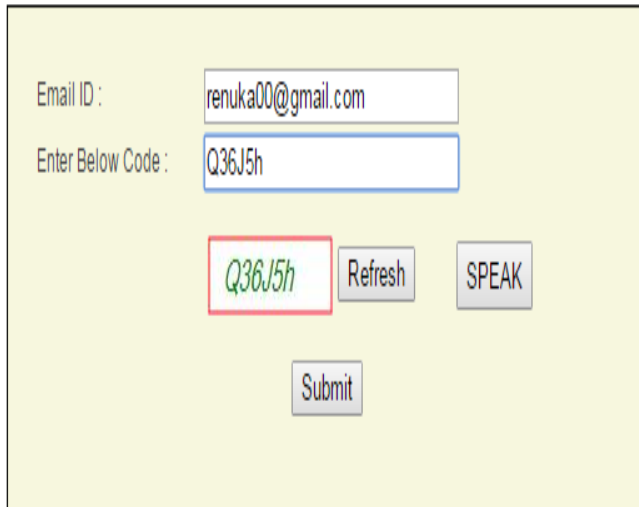


Fig-5.4:Audio CAPTCHA

An audio is provided to the user. User is suppose to listen to the audio correctly and type in the text box. If the text matches the audio user can sign up correctly.

5.5 Image CAPTCHA:-



Fig-5.5: Image CAPTCHA

An image is provided to the user. User is suppose to click five points anywhere randomly on the image. These points will be considered as password and stored in the database.

5.6 Video CAPTCHA:-

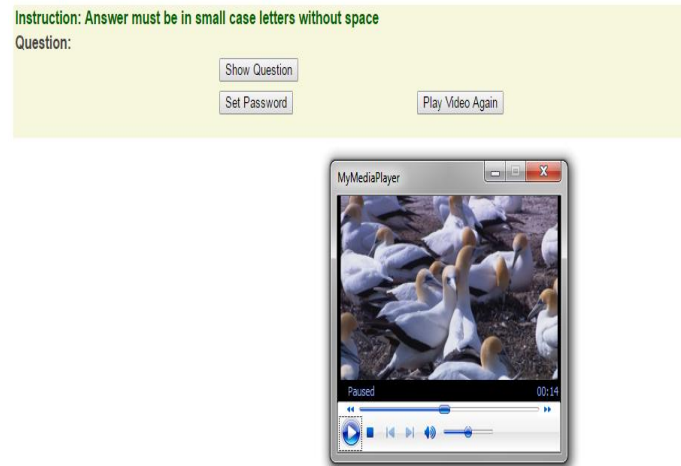


Fig-5.5: Video CAPTCHA

An video is provided to the user. User has to watch the video and answer the questions provided based on the video. If the answers match to the answers stored in database the user signs up successfully.

6.CONCLUSION

This paper explains concept of using CAPTCHA as graphical passwords. Security primitives due to which it becomes necessary to develop systems like graphical passwords which are hard to crack and are more secure than the traditional passwords. How this system prevents attacks made by bots.

7.REFERENCES

1. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.
2. R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4, 2012.
3. Bin B.Zhu, Je_Yan, Guanbo Bao, Maowei Yang, and NingXu. Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems. *IEEE TRANSACTIONSON INFORMATION FORENSIS AND SECURITY, VOL.9, NO 6, June 2014.*

8. BIOGRAPHIES



Mr.SagarMarutiKamble
final year student of
Computer science and
Engineering at Sanjay
Ghodawat institute,atigre.



Mr.YogeshMallikarjunDhavan.
final year student of Computer
science and Engineering at
Sanjay Ghodawat institute,atigre.



Mr.PramodKambale.
final year student of Computer
science and Engineering at
Sanjay Ghodawat
institute,atigre



Ms.Dipali Sanjay Mahajan.
final year student of Computer
science and Engineering at Sanjay
Ghodawat institute,atigre



Ms.RenukaShamkantJadhav.
final year student of Computer
science and Engineering at Sanjay
Ghodawat institute,atigre