Captcha as a Graphical Password

Shaikh Mohd Asad[1], Ansari Aaqib[2], Patil Ganesh[3], Sinkar Saiprasad[4], Gadhire Prachi[5]

[1-4]Student VIII SEM, B.E., Computer Engg., DRIEMS, Neral, India
[5]Professor, Dept. of Computer Engineering, DRIEMS, Neral, India

***

Abstract – *In today's world, password security is very important. This paper presents the idea of a new graphical idea for authentication. For password protection various techniques are available; this technique is based on Captcha technology named Captcha as graphical passwords (CaRP). CaRP is a combination of both a Captcha and a graphical password. CaRP is a click-based graphical password scheme. Graphical passwords are most recommended for users to overcome the drawbacks faced in the existing system. Graphical Passwords are introduced to resist the Shoulder surfing attack, online-guessing attacks, and relay attacks. This method extends the existing system by adding effective features, motivating user to choose more secure random point clicks on the image which is difficult to find. This system can be used for any online/offline system.*

Key Words: **Graphical password, Pass points, Authentication, Password security, Local Server, DB SQLite**.

1. INTRODUCTION

There has been a great deal of hype for graphical passwords for two decades because Primitive's methods suffered from an innumerable number of attacks which could be imposed easily, Eavesdropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords. The idea of graphical passwords first described by Greg Blonder (1996). For Blonder, graphical passwords have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. Since then, many other graphical password schemes have been proposed. The desirable quality associated with graphical passwords is that psychologically humans can remember graphical far better than text and hence is the best alternative being proposed. There is a rapid and growing interest in graphical passwords for they are more or infinite in numbers thus providing more resistance.

The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

2. LITERATURE SURVEY

2.1 Existing System

Surendra Karanam [2015] The graphical passwords are not fully secure even though they are alternatives to text passwords. CaRP doesn't depend on any single Captcha scheme. There is a good scope for the refinements in CaRP because of the security and usability. By using different images of varying difficulty levels based on the user's login history and the machine used to log in.

Dr.BK Raghavendra [2019]: The proposed CaRP, A new security primitive relying on unsolved AI problems. CaRP is both a Captcha and a graphical password scheme. Graphical password is the method used as an alternative to traditional passwords. Cued Recall password technique provides an external cue which helps the user to memorize and enter a password. 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.

2.2 Proposed System

The proposed system is "Graphical password authentication using cued click points" which is a combination of pass faces and pass points. In this system during the registration process user has to select the number of images the user needs and a particular point in each image. Then image click co-ordinates stored in the database. When a user wants to login he has to click on the point of the images. Cued click points as shown in Fig1 when a user clicks on a particular point on the image which he has chosen during the registration process, the next image will be displayed, and like we have to click on points on images that we have selected for an authentication process. This technique provides more security and it is hard for hackers to attack. Because when a hacker clicks on the wrong point on the image a different image will be displayed to him. Therefore he has to click on those wrong images and at last, only he can understand that it was wrong.

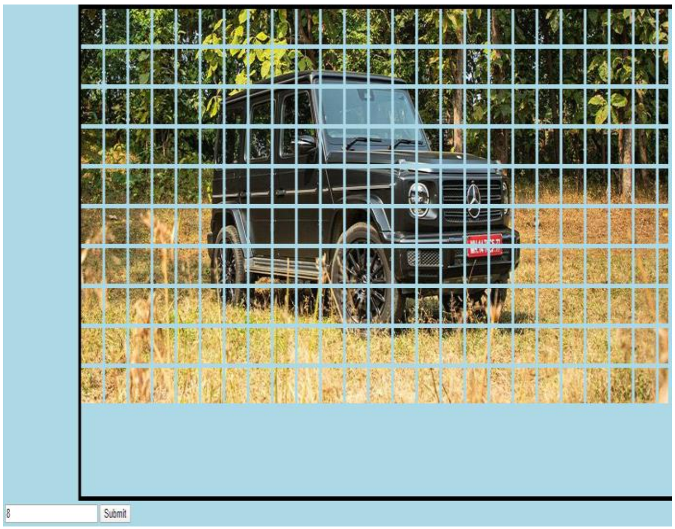


Fig 1: Cued click points

3. SYSTEM DESIGN

Graphical passwords use pictures as passwords instead of using alphanumeric characters. In recognition-based systems, users would choose pictures, icons from a collection of images. In the authentication process, the users need to recognize their registration choice among a set of candidates.

The system design consists of three modules such as user registration module, a picture selection module, and system login module (see Figure 2).

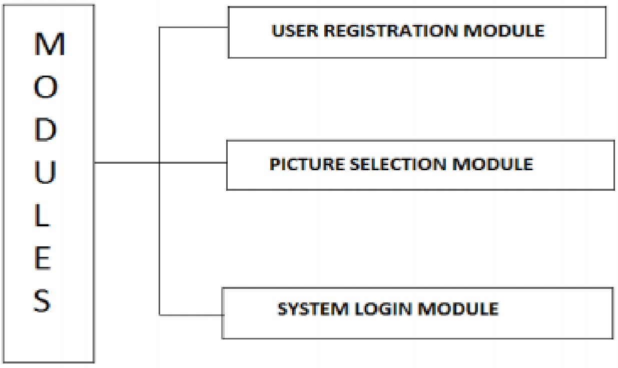
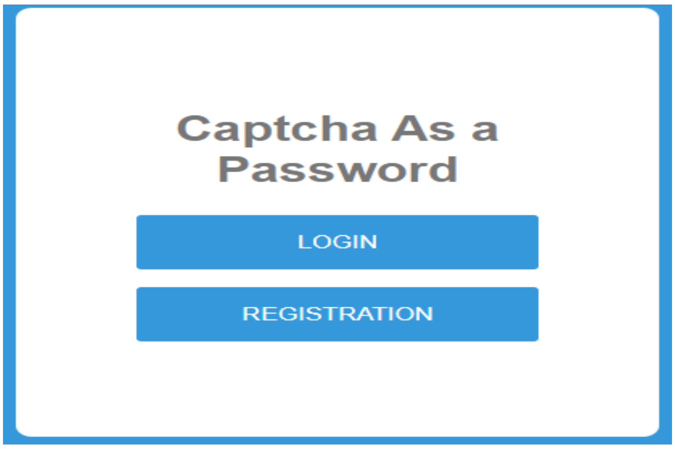


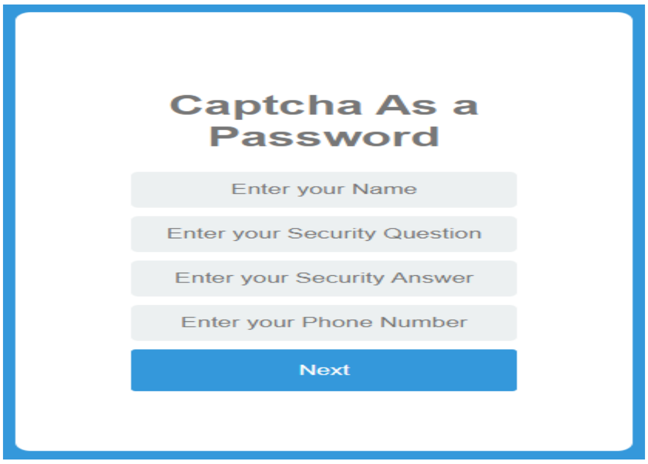
Fig. 2 System design module

The implementation of the proposed design of the Graphical Password requires the following components:

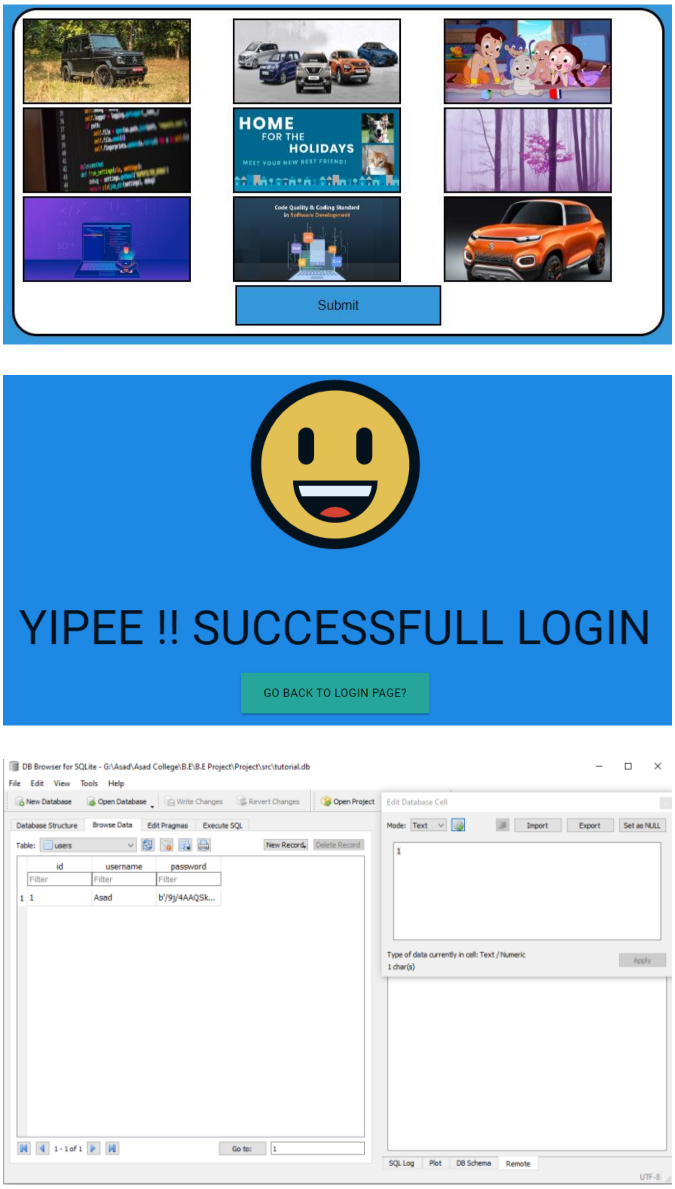
1. Laptop/Computer
2. Cmd (Command Prompt)
3. Google Chrome/Firefox/Internet Explorer
4. DB SQLite



Captcha As a Password



Captcha As a Password



	id	username	password
	Filter	Filter	Filter
1	1	Asad	b'/9j/4AAQSk...

Fig 3: System Design

4. FUTURE SCOPE

The future work is to balance the trade-off between Usability and Security by considering the following factors:

1. Memorability of the image.
2. The Simplicity of the steps involved.
3. The Simplicity of the user training.
4. Simple and nice interface.
5. Password space.
6. Prevention against Social Engineering.
7. Prevention against Brute force.
8. Prevention against Dictionary attack.
9. Prevention against Guessing.

5. CONCLUSION

The proposed CaRP, a new security primitive relying on unsolved 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. This work is one step forward in the paradigm of using AI problems for security. CaRP has good potential for refinements, which call for useful future work

6. REFERENCES

[1]. Dr. Manjula Sanjay Koti , B BinduMalini , Lalitha A H “A NOVEL METHOD FOR CAPTCHA AS GRAPHICAL USER AUTHENTICATION USING SHA-1 ALGORITHM” in International Journal of Computer Engineering and Applications, Volume XII, Issue I, Jan. 18, www.ijcea.com ISSN 2321-3469.

[2]. Sanjay Sharma and Devendra Kumar “Highly Secured Intellectual Graphical CAPTCHA” International Journal of Modern Engineering & Management Research Volume 6 Issue 1| March 2018.

[3]. Ganesh .D. Satkar, Vrushali Desale “A Survey on Secure Login Authentication System using Captcha Based Graphical Password Technique” International Journal of Engineering Science and Computing, July 2017 Volume 7 Issue No.7.

[4]. Surendra Karanam “Novel Security Method Using CAPTCHA as Graphical Password” Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 3159-0040 Vol. 2 Issue 4, April - 2015

[5]. Sandeep H, Dr.B K Raghavendra “A New Security Primitive Model Based on Artificial Intelligence Using Captcha as Graphical Passwords” International Journal of Computer Engineering and Applications, ICCSTAR-2016, Special Issue, May.16