# ENHANCED SECURE LOGIN SYSTEM USINGCAPTCHA AS GRAPHICAL PASSWORDS.

HAJIRA MUSKAAN
DEPARTMENT OF MCA
AMC ENGINEERING COLLEGE
BANGALORE
hajiramuskaan2@gmail.com

MR.RAJESH N
DEPARTMENT OF MCA
AMC ENGINEERING COLLEGE
BANGALORE

## ABSTRACT

□ *Now a day, vulnerability is a major problem in computer security. Computer & IT security is supported by passwords. The password is used in user Authentication process. The traditional user authentication method uses alphanumeric text-based password, but it has some drawbacks, so that graphical password technique is design & developed to overcome the vulnerabilities of this alphanumeric traditional password problem. The graphical is easier to remember and difficult to guess also than text. But biggest drawback of graphical password technique is vulnerable or crack to shoulder surfing attack, log attack and also sometimes to spyware attack too. So another technique to graphical password a Captcha technique is developed.*

□ *The Biggest advantage of Captcha is that it can't be identified by bots or computer. From the unwanted bots attacks, Captcha gives protection but with this protection there are also some limitation of Captcha & to overcome this limitations or weaknesses a new technique Captcha as Graphical Passwords is developed. This can be useany user authentication process.*

□ *Captcha as Graphical Passwords CaRP is mixture of graphical password & captcha. It is clicking an event which is performed at various points on image in sequence to get new password. So, In this paper, we are going to survey existing CaRP techniques & new scheme.*

□

□ **Keywords:** *Graphical Password, Carp,Captcha, Security Primitive, Password,Bots.*

□

## INTRODUCTION

Security is the most important aspect in an information security program for authentication. The textbase & Graphical passwords technique are used in the user authentication process, but the best alternative for textbased password is definitely a graphical password. The graphical password can reduce the stress on human memory as human mind to remember graphics and images better.

Graphical passwords are vulnerable to shoulder surfing and other attacks. A new security technique namely, a group of graphical password systems builds Captcha technology that is called a (CaRP) Captcha as graphical Passwords. CaRP is click based graphical passwords, in which an order of clicks on respected image is used to get a password. Conflicting other click- based graphical passwords and images usedin CaRP as a Captcha challenges and a newCaRP image is shows for every login attempt.

The application where used captcha as a graphical password are:

- The captcha as graphical password is used in many internet applications specifically in the e-backing application,e-commerce site, where users had to solve the different captcha at the momentof login.

- By using the carp the entry of spam or unwanted mail send through bots emails are reduced. Here the email service provider uses the captcha as a graphical password to log into the user system so the spam bots cannot log into the systembecause they are not able to solve and understand the captcha.

Authentication is imp and it allows users to confirm their identity for any web application. The three important areas where human computer interface is important these are Authentication, Security operations and developing secure systems. We concentrate on the both authentication and transaction problem as well as provide extra security for authorization of suer. A password is mainly used for authentication. The password is need to secret from unauthorized access, and those who want to gain access to that resource are tested on whether or not they know the password and they are accordingly granted or denied access.

Traditional password method is text-based password. Many researchers have found an alternative method that is graphical password. The password input is user- friendly as well as it is easy to understand in terms recall ability. The main motivation of graphical passwords is the very user friendly that people are better at remembering images than alphanumeric words. In addition, graphical password is an easier as well as more human friendly and memorization strategy recognition-based memory used, instead of a recall-based memory for textual password.

## RELATED WORK

### A. Graphical PasswordTechniques

Graphical password methods are developed to overcome the boundaries of text-based passwords. Graphical passwords contain recognizing the images or occasionally to recognize the image and click the particular points on the image rather than typing the characters like text-based alphanumeric password. In this way, the problems that rise from the text-based passwords are minimize. Graphical password techniques are categorized as follows:

1) Recognition Based scheme 2) Recall Based scheme 3) Cued Recall Basedscheme.

A recognition-based scheme needs to select the number of images from a random image in an order as a user password, and for authenticating the user has to identify thoseimages in a same order as user enter.

### B. Captcha

Completely Automated Public Turing Test to tell Computers and Human Apart [1] (Captcha) discoveries the difference in humans and bots in cracking the hard AI problems. It is a one kind of test to check user is Human means not a computer device.

There are two types of Captcha:

**1) Text Captcha**: PayPal and Microsoft Captcha are both relied on background noise as well as random character strings to resist to automated attacks. The Captcha used by Google, Bing or Yahoo All share similar characteristics, such as a absence of background noise of alteration for a character or word images and extreme assembling for an adjacent character. Random Captcha images are captured humanly by site in the form of pixel, borderline probabilities and site by site covariance.

EZ-Gimpy uses word images which employ character misrepresentation and clutter. Personal print uses a lowquality picture by degrading parameters to thicken, fragment,crowd and add noise to character images.

**2) Image Recognition Captcha**: Captcha involve of a combination of images [6]. The user needs to recognize theimages given to him to solving the given puzzle problem.

As shown in Figure.2 user has to select the cat images as the password characters.

### C. Captcha as Graphical Password(CaRP)

An Overview CaRP has a new image is created for every login attempt also for the same user. Alphabet which is used in CaRP of visual shown based objects (E.g. Alphanumerical characters, similar animals, etc.) to create or generate a CaRP image, which is a mainly Captcha challenge. A Recognition-based CaRP technique used password is in a series of visual shown based objects alphabet. Per view for the traditional recognition based on graphical password technique of security, recognition-based CaRP seems to have access to multiple times of different visual objects.

We present two kind of recognitions-based CaRP techniques and a variation next. A recognition-recall based CaRP, Password is a also sequence of some points of objects. An invariant point of an object is also one point that has a fixed relative position in different personifications of the object and it may be uniquely identified by users or humans no issue to how the object appears in CaRP images.

**1) ClickText:** ClickText has a recognition-based CaRP scheme. CaRP techniques use CAPTCHA as its principle. Alphabet set of ClickText comprises of alphanumeric characters. A ClickText password is a series of alphanumericcharacters in the alphabet e.g.
=DEF@b2SK78, which is a similar to the text password. A ClickText image is different from usual CAPTCHA as all the characters of alphabet set must be included in the CaRP image. The CAPTCHA engine generates such CaRP image. When image is generated, then each characters location in the image is recorded which is used in the authentication. Characters can be put randomly in 2D space in these images which changes from text CAPTCHA where characters are typically ordered from left to right in order for users to type them sequentially. Fig. 3 shows a ClickText image with alphabet of 36 characters [1].

**2) ClickAnimal:** ClickAnimal is a recognition-based CaRP technique. It has a series of similar animals such as dog, pig, like that. The password in this technique is a sequence of animal names like = Cat, Dog, monkey,.. Most of the models are created or each and every animal. CAPTCHA generation activity are used to get 2D models by applying different types of views, colours, and optional distortions and it is used to generate the Click Animal image. The final resulting 2D animals are then arranged on clustered backgrounds like grassland. The number of similar animals is less than the number of available characters.

**3) Text Points 4 CR:**. Text Points sometimes, it can be modified to fit challenge response authentication. Thisvariation is called as Text Points for Challenge Response or alsoTextPoints4CR.

CaRP have some benefits given below:

1) CaRP offers protection against Automatic Online Guessing Attacks on passwords.
2) It offers protection against ShoulderSurfing Attack.
3) It offers security against spam emails sentfrom a Web email service.
4) It offers security against spam emails sentfrom a Web email service.

CaRP has some limitation:

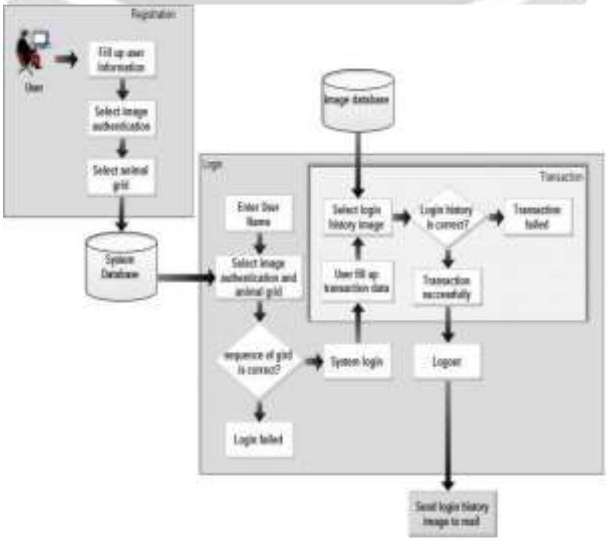
1) CaRP scheme is vulnerable to phishingattack.
2) CaRP is vulnerable if both the image anduser clicked points can be captured.

## PROPOSED SYSTEMOVERVIEW

### A. Problem Statement

To improve the CaRP System with valid authentication and enhance the Security by using login details send to emails of three layer of difficulty based on CaRP Technique with an animal grid as graphical password and generate the Login login details of time and date or otp system.

### B. System Architecture:


Registration
User
Fill up user information
Select image authentication
Select animal grid
System Database
Image database
Login
Transaction
Enter User Name
Select image authentication and animal grid
sequence of grid is correct?
Login failed
System login
User fill up transaction data
Select login history image
Login history is correct?
Transaction failed
Transaction successfully
Logout
Send login history image to mail

ALGORITHM

```
Step 1: Start
Step 2: User registers with his username and the specific Animal Grid as his password Step 3: Login Process
Step 4: If Login successful perform Steps 5to 7 else step 8
Step 5: During Transaction, User has toenter the login details.
Step 6: If the login details is correct thenstep 7 else step 8
Step 7: Transaction is successful and login history details sent to the user via email. Step8: Stop
```

## EXPERIMENTALRESULTS

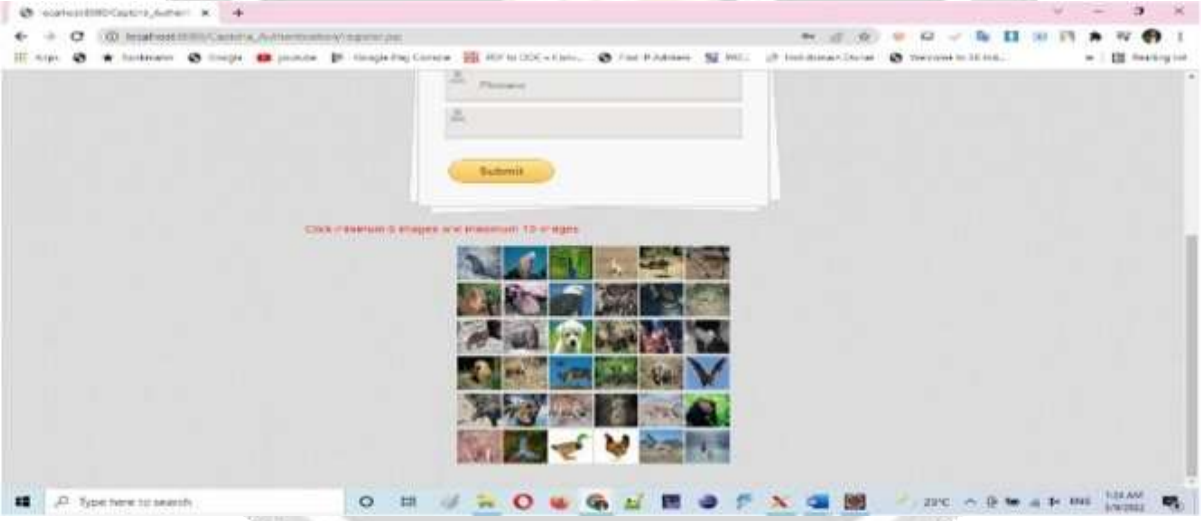
- **Registration Process**

First user starts the registration process, where the user fills up the information and selects at least 6 images from animal grid.

The animal grid image is generated by the system from the system's database. Then the selected graphical password by the useris saved in database.

- **Login Process:**

During the login process the first step is user entered the username and selects the image which he has selected during theregistration process. Then the user selects.

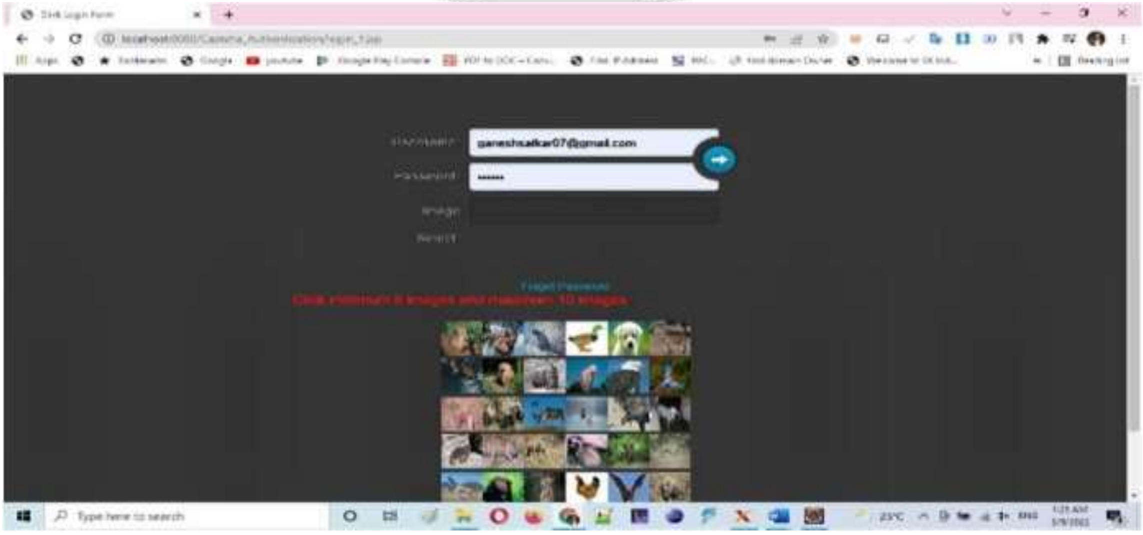


Phonenu

Submit

Click maximum 6 images and maximum 10 images

REGISTRATION PROCESS



Username ganeshsatkar07@gmail.com

Password ••••••

Image

Select

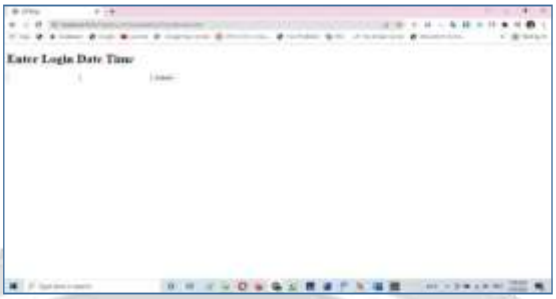
Forgot Password

Click minimum 6 images and maximum 10 images

## LOGIN PROCESS

### Authentication Process:

After the successful login automatically send one email to user. In this mail include time and date details of login or opt details for authenticate transaction or authenticate process.



Enter Login Date Time

Our proposed system overcomes various demerits of earlier existing systems by using a dynamic nimal Grid, along with theintroduction of Login History details.

Login History details to be used during Transactions or authentication in order to increase security with three layer of security..

## .CONCLUSION

CaRP authentication system is developed by graphical password based on animal grid method which uses both the combination of recall based and recognition-based system. This system provides animal grid from which user will select his graphical password. To overcome this type of attack, the advance system generates the login details where the generated details automatically generate and send to the user’s email id. only user can select correct details at the time of transaction or authentication. If password is stolen by interceptor, the advance system will notallow the interceptor to do transaction or authentication into the system.

## REFERENCES

[1] 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 AndSecurity, Vol. 9, No. 6, June 2015.

[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, 2014.

[3] S. MASOUD ALAJMI, IBRAHIM ELASHRY, HALA S. EL-SAYED, and OSAMA S, FARAGALLAH, A Passwordbased Authentication System based on The CAPTCHA AI Problem, IEEE 2020

[4] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, CAPTCHA: Using hard AI problems for security, inProc. Eurocrypt, 2013,

[5] S. Altaf Khan, and Dr. Alexander G. Chefranov, A Captcha-Based Graphical Password With Strong Password Space and Usability Study, International Conference on Electrical, Communication andComputer Engineering(ICECCE)12-13 June 2020, Istanbul, Turkey

[6] Mangal Sain, Kim Ki-Hwan, Hoon Jae Lee and Young-Jin Kang, An Improved Two Factor User Authentication Framework Based on CAPTCHA and Visual Secret Sharing. Security, 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on