Hybrid Graphical Password: A Strong Multilayer Security Primitive

Karishma Mali
Department of Computer Engineering
Dhole Patil College of Engineering
Pune, India
karishma.ml@gmail.com

Susheelkumar Benke
Department of Computer Engineering
Dhole Patil College of Engineering
Pune, India
sushilbenkeoo7@gmail.com

Anjali Tippe
Department of Computer Engineering
Dhole Patil College of Engineering
Pune, India
anjalitippe55@gmail.com

Dhaval Damania
Department of Computer Engineering
Dhole Patil College of Engineering
Pune, India
damaniadhaval.dd@gmail.com

Prof. Priyanka Kedar
Department of Computer Engineering
Dhole Patil College of Engineering
Pune, India
priyankakedar2009@gmail.com

***Abstract*—*CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a technology which humans can pass but computer programs cannot pass. Using this primary CAPTCHA, a new secondary technology is built called as Graphical CAPTCHA. It is also called as CaRP i.e., Captcha as gRaphical Password. Captcha and a Graphical Password (CaRP) is a click-based image authentication graphical password, where a sequence of clicks on image is used to derive a password. With this hybrid of CAPTCHA and graphical password, many security problems such as online guessing attacks, dictionary attacks can be dealt with. Thus, CaRP is not a solution to all the attacks, but it provides a great level of security and allows access to the authorized users. Graphical passwords are challenging techniques for authenticating by clicking on random pixels over the image. Graphical password makes use of a picture, part of a picture or number of pictures together to authenticate legitimate user. In the proposed system, pass points are used in CaRP and another new security primitive is used similar to the Matrix concept*

Keywords—CAPTCHA; CaRP; Pass Point; MOP

I. INTRODUCTION

Security in technical terms refers to securing the data stored in smart devices, cloud, or databases without allowing access to those data except for the authorized user. The most opted security measure is to involve encryption and passwords. Passwords may be in the form of word or phrase which gives access to the user for a particular system or program. But these text passwords can easily be broken allowing the security to break.

So, a new advanced technology is used which makes use of Captcha as Graphical Password (CaRP) for the security purpose. This technique uses an image as a password which will only be known by the authorized user. Then, the particular image can again increase the security by adding pass points on the image. These pass points will again only be known by the authorized user. Further adding of MOP i.e., Matrix Operation Password. The concept of MOP is new and similar to OTP concept.The key goal of using CAPTCHA as graphical password is to increase the security level of data which would prevent the data from being misused. The benefits of using such a technology is to protect yourself, protect your credibility, protect your income, protect your reputation, protect your business, and protect your investment. There are numerous applications where CaRP would play a major role. 1) Online Polling Sites, 2) Registering Web Forms, 3) E Banking, 4) To prevent Web Crawling, 5) Prevent attacks and Email spam.

II. RELATED WORK

In [2], authors proposed to reduce problems related to text passwords and to use password managers. This requires user to remember only the master password. It stores or re-generates and sends on behalf of the user the appropriate passwords to web sites hosting user accounts. In this paper, authors provide a comprehensive review of the 1st twelve years of published research on graphical passwords, and react on it. With this, it is now clear that the graphical nature of schemes does not by itself avoid the problems typical of text password systems. The motivation of the authors is multi-fold. The authentication has increasing impact on the society, as its use expands from login to a single computer, to a large numbers of remote computers hosting personal and corporate information.

In [3], the author conducts the survey of CAPTCHA as Graphical Password schemes relying on unsolved hard AI problems. As it is a combination of both Captcha and Graphical password, it makes it very hard to guess the password to the intruders. CaRP schemes are categorized as Recognition-Based CaRP and Recognition-Recall CaRP. This paper also discusses about Recognition Based CaRP which include ClickText, ClickAnimal and AnimalGrid techniques. In the paper, CaRP image for particular user will get generated. User can sign up by giving the username and password which will be displayed in CaRP image which is

combination of password characters and non-password characters.

[4]In this, the author has explained in detail the concept of One Time Password (OTP). The use of OTP for security purpose is talked about. This OTP concept can be used to further advance the system.

[5] It tells us all the security measures needed for internet banking. It tells us about the authentication process used in E Banking.

[6] Last paper deals with the idea of improved security authentication using CaRP concept. This concept of CaRP is used in the area of web application.

III. PRAPOSED SYSTEM

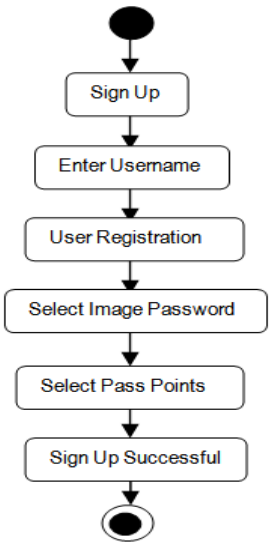
The aim of the proposed system is to increase the security level by using CaRP and some other techniques such as MOP and. The proposed system consists of two main parts being the Sign Up and the Sign In part.

A. Desing Consideration

- Sign Up:
  User Registration,
  Select Image Password,
  Select Pass Points.
- Sign In:
  Username,
  MOP,
  Selected Image Password Verification,
  Selected Pass Points Verification.

B. Describtion of desing

Sign Up: The Sign Up part basically deals with the signing up process of the user. Here, the user has to start by entering the user details as the registration part. Then the user will have to select an image from number of images as a password. On the selected image, user has to select 3 points, called as 3 Levels, in a sequence which will act as a password. After doing this, user will be done with its registration.



Sign Up Flow

Sign In: In the Sign In process, the user has to enter the username along with the answer for the MOP. MOP stands for Matrix Operation Password. This concept is used to enhance the security level.

MOP as the name says, is a password generated from the matrix by the user. Once the user enters the username, a matrix will be sent to the registered email id and the phone.

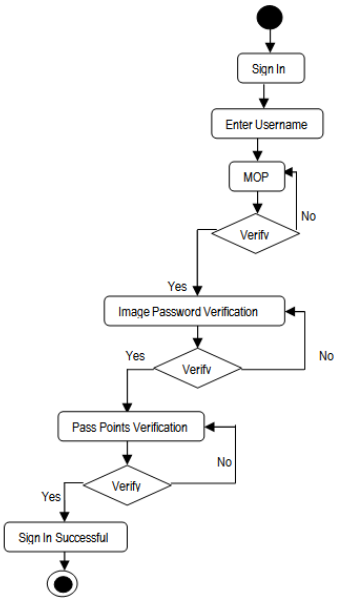
Also, a question will be asked related to the matrix. For example the question can be like, what is the addition of the numbers from 2^{nd} row 4^{th} column and 5^{th} row 1^{st} column? In this case, the answer would be 5 + 9 = 14.

In similar way, the user has to find the answer to the question from the matrix shown on the phone or email id. Various operations can be used for the matrix question such as addition, subtraction, multiplication.

2	5	9	0	7
1	6	8	5	3
3	2	0	9	4
6	7	4	1	7
9	3	5	3	9

Matrix

Once the user enters the correct answer, then the user has to select the same image which he has selected during the time of Sign Up process. As this is the password level, next the user has to select the same points on the image in the same sequence which he had during Sign Up. If the user selects the correct sequence, then he will be done with the Sign In process



Sign In Flow

The third part is the database part of the project. It deals with the database for the Banking purpose. Here after the Sign In process, the user performs the desired action on the system. It includes selection of My Account, Fund Transfer, and E Deposit etc.

Also, the technique of Virtual Random Keyboard (VRK) will be used. This will increase the security in case of typing of the passwords for the banking transaction.

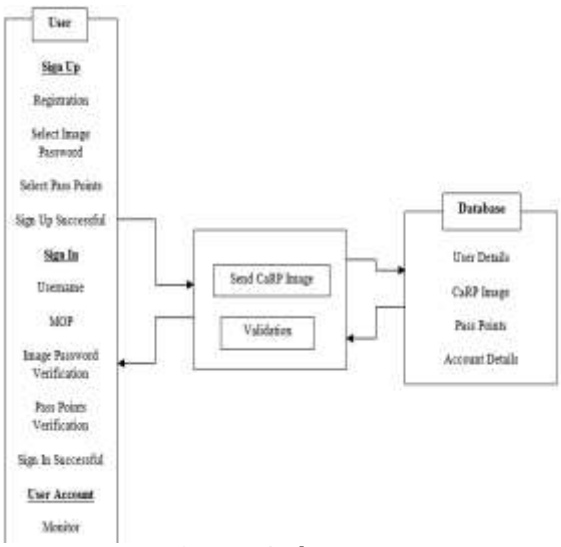
IV. ARCHITECTURE

The architecture of our system consists of the user part, interface part and the database part.

The user part consists of the tasks which the user will perform on the system. It includes Sign Up, Sign In and the account part.

The next is the interface part which connects the user part to the database part. It deals with the connecting the two parts of the architecture.

The next is the database part in which all the details, images, passwords, pass points, etc. will be stored. During the time of verification, the data will be verified from the database.



System Architecture

V. EXPERIMENTAL RESULTS

A. *Starting page*

B. *sign up*

C. *sign in*

D. *Image password*

E. *Pass Point Password*

F. MOP

G. E Bank

CONCLUSION

The proposed system of Hybrid Graphical Password: A Strong Multilayer Security Primitive aims to provide new security methods which will be used for enhancing the levels of security. CAPTCHA as Graphical Password introduces a new family of graphical passwords which can further be improved to get higher outcomes. It has vast number of applications and can be used to overcome attacks and spams.

However, the idea of CAPTCHA i.e., Completely Automated Public Turing Test to Tell Computers and Humans Apart still holds areas to be discovered for many reasons. This technology can further be worked upon and can be researched

The present system uses taking of an image saved from the set of images. But this can be worked upon by taking an image of the authorized user at the time of registering itself. That is, the system will take a picture of the face of the authorized user every time the user uses the program and matches with the picture taken before. In such a way, if an unauthorized user comes in then the system will not match the face because the user is not the authorized one. Further more such new ideas can be implemented and researched.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project on `HYBRID GRAPHICAL PASSWORD: A STRONG MULTILAYER SECURITY PRIMITIVE'.We would like to take this opportunity to thank our guide Prof. Priyanka Kedar for giving us all the help and guidance we needed. We are really grateful to them for their kind support and their valuable suggestions were very helpful.

We are also grateful to Dr. Arati Dandavate, Head of Computer Engineering Department, Dhole Patil College of Engineering, for her indispensable support and suggestion. We would also like to thank our Principal, Dr. Abhijit Dandavate for giving us the opportunity to do this project.

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 AND SECURITY, VOL. 9, NO. 6, JUNE 2014 891

[2] Robert Biddle, Sonia Chiasson, P.C. van Oorschot "Graphical Passwords:Learning from the First Twelve Years" ",lACM Comput. Surveys, vol. 44, no. 4, 2012

[3] Mirza Tanzila Maqsood, Pooja Shinde "A Survey on One Time Password" Volume 5 Issue 3, March 2016

[4] Radha Damodaram, Dr.M.L.Valarmathi, "SECURITY MEASURES OF RANDVUL KEYBOARD", International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010, 619-625

[5] "Secure InternetBanking Authentication" IEEE COMPUTER SOCIETY 1540-7993/06/2006 IEEE

[6] Alok Ranjan, Mansi Bhonsle "Improved Security of Authentication Scheme using Carp for Web Application" International Journal of Computer Applications (0975 – 8887) National Conference on Advances in Computing, Communication and Networking (ACCNet – 2016)