ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Hybrid Graphical Password: A Strong Multilayer Security Primitive

Karishma Mali[1], Anjali Tippe[2], Susheelkumar Benke[3], Dhaval Damania[4], Prof. Priyanka Kedar[5]

Students, Dept. of Computer Engineering, Savitribai Phule Pune University, Pune, India[1,2,3,4]

Assistant Professor, Dept. of Computer Engineering, Savitribai Phule Pune University, Pune, India[5]

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. 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.

KEYWORDS: CAPTCHA, CaRP, Pass Points, OTP, LTP, VRK, Graphical Password.

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 OTP-LTP i.e., One Time Password and Long Term Password and also Virtual Random Keyboard (VRK) enhances the security level.

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]Hotspots in CaRP images can no longer be broken to automatic online guessing attacks. Our usability study of two CaRP schemes implemented is encouraging. Both AnimalGrid and ClickText had better password memorability than the conventional text passwords. [5] In this, the authors have explained about keyloggers which are self installing programs being installed either on a web browser or as a device driver, which monitor data being input and send relevant data to a phishing server. The paper tells us about Virtual Random Keyboard (VRK) which is a dynamic keyboard. The format of keyboard changes depending upon the time and client. So each client will have separate keyboard format. [6]In this, the authors have increased the level of security by adding a 3 level security method. They have added the concept of OTP-LTP and also the technique of VRK. These are used to increase the authentication process.

III. PROPOSED ALGORITHM

A. *DESIGN CONSIDERATIONS:*

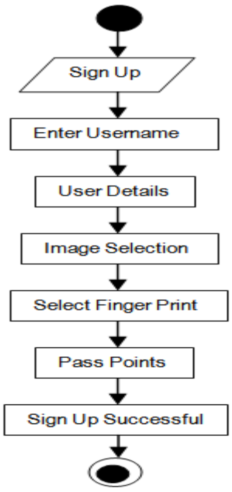
- User sign up is done with details filled by user.
- Selection of an image and 3 pass points by the user along with a finger print.
- Sign In includes username and LTP verification sent on the email id registered.
- Selecting the same finger print, image and placing the same 3 pass points as done during registration.
- Entering the OTP sent to registered phone number and email id.
- Using of Virtual Random Keyboard during the whole process.

B. *DESCRIPTION OF THE PROPOSED ALGORITHM:*

Aim of the proposed algorithm is to increase the security level by using CaRP and some other techniques such as OTP-LTP and VRK. The proposed algorithm mainly consists of three important steps.

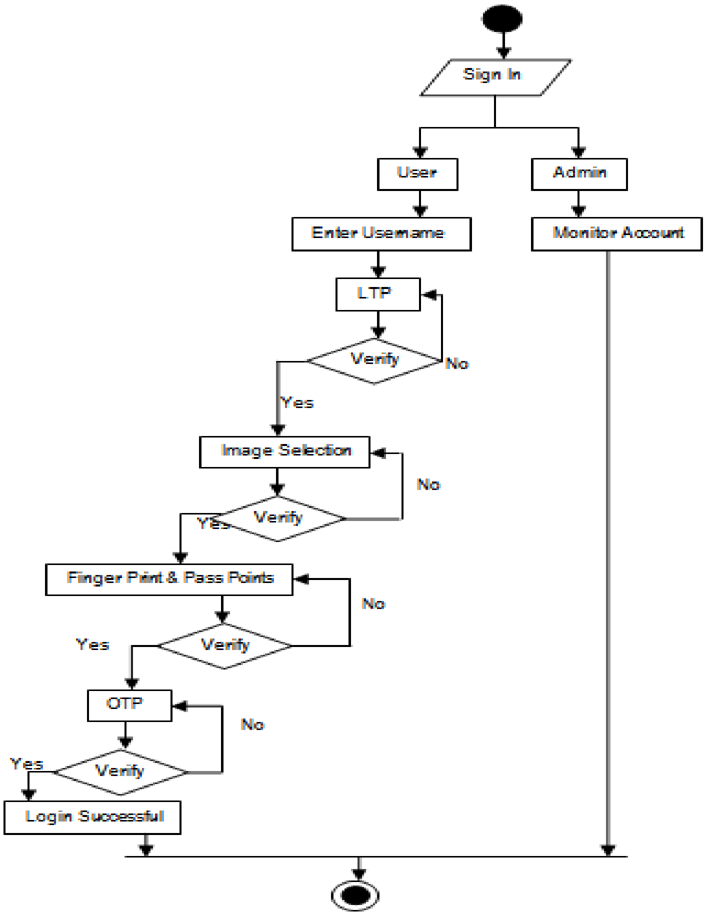
Step 1: Sign Up:

In this, the user does the registration process which would include the filling of data asked by the system. The user then will be asked to select an image which will be used as a password during sign in. On the same image selected, user has to select three pass points which will reduce the chances of attack. User also has to select a fingerprint for security. With this, the sign up process completed.



Step 2: Sign In:

In this, the user goes for sign in process. The user has to enter the user name along with LTP which will be sent to the email id as per registered. Then, user has to select the same image which was selected by the user as a password. Then, a page comes up which will show the user name and the selected image. After this, user has to select the same finger print which was selected during registration. Then, user selects the 3 pass points level wise as selected before. This ends the process of sign in. Now, the user has to enter the OTP which the user will get via message on registered phone number and via email on registered email id.



Step 3: Virtual Random Keyboard:

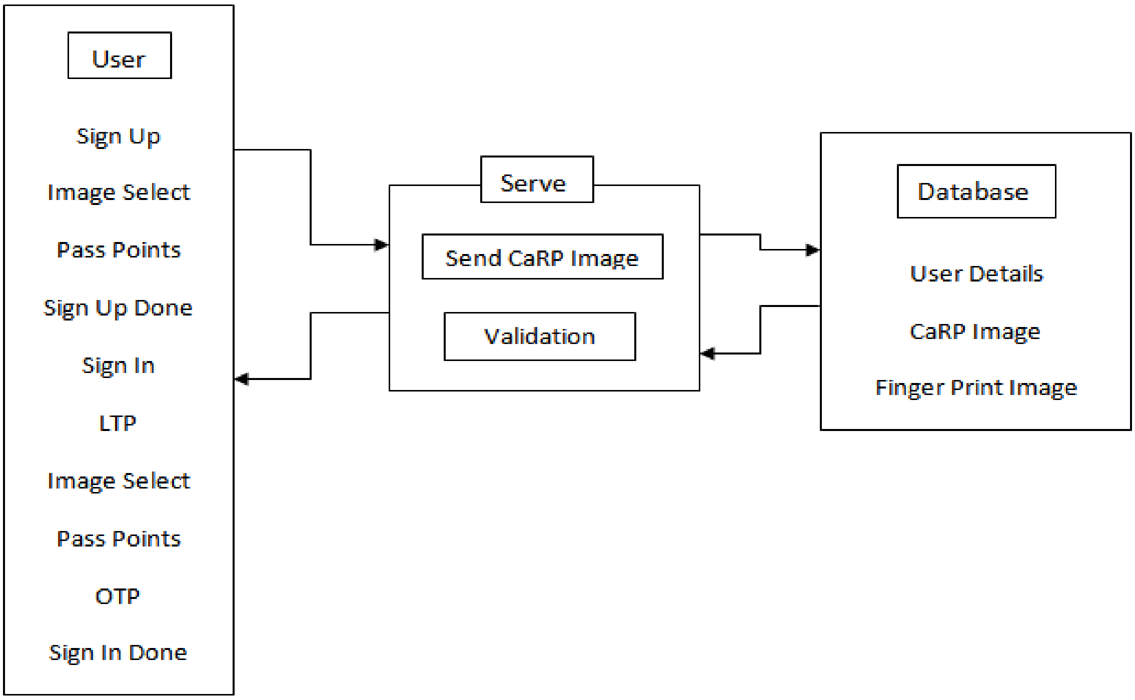
Virtual Random Keyboard is basically a virtual keyboard generated which will have the characters shuffled every time the user uses the keyboard. So, when the user tries to enter through normal keyboard, the software will not allow it to enter. User has to enter through virtual random keyboard. So, using this technique attacks can be avoided. We will be using this technique during the sign up and sign in process.

IV. PSEUDO CODE

```
Step 1:  Enter user name and details.
Step 2:  Select image.
Step 3:  Select finger print image and 3 level points.
Step 4:  Registration successful.
Step 5:  Enter LTP.
Step 6:  Select the same image as selected in Step 2.
Step 7:  Select the same finger print and pass points as done in Step 3.
Step 8:  Enter OTP.
Step 9:  Login successful.
```

V. Architecture

The figure below shows the architecture of the proposed system. The architecture consists of mainly three parts being user, server and database. The user will send request to the server and the server will respond via the database.



VI. Conclusion and Future Work

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.

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. 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. M. M. Vamsi Priya, Sushma Nallamalli, D. Bhanu Prakash, K. Ramya Sri, “Authentication Using CAPTCHA as Graphical Password”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015

4. Abhijit Nawale, Ajay Thorat, Sujeet Somwanshi, Sandesh Bharati, "CARP-A NEW SECURITY PRIMITIVE BASED ON HARD AI PROBLEMS", IJCSMC, Vol. 4, Issue. 6, June 2015, pg.12 – 20
5. 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
6. Vijayalaxmi Daundkar, Shyam Gupta, "Implementation of Simple Text Based Shoulder Surfing Resistant Graphical Password using CAPTCHA and VRK", IJSR, Volume 5 Issue 6, June 2016
7. http://www.tutorialspoint.com/cryptography/pdf/advanced_encryption_standard.pdf
8. https://www.youtube.com/watch?v=-Jb-BZvEoZs

BIOGRAPHY

Prof. Priyanka Kedar is an assistant professor of Computer Department in Dhole Patil College of Engineering, Savitribai Phule Pune University, Pune**. Karishma Mali, Anjali Tippe, Susheelkumar Benke and Dhaval Damania** are the students of the college mentioned above and all are in Final Year of Computer Department of Engineering.