Graphical Password Authentication using Images Sequence

Saranya TS[1], Elizabeth Mathew[2], Anju Mathew[3] and Ms. Rini Kurian[4]

[123] PG Scholar, Amal Jyothi College of Engineering, Kanjirapally, Kerala

[4] Assistant Professor, Amal Jyothi College of Engineering, Kanjirapally, Kerala

Abstract: A graphical password is associate authentication system that works by having the user choose from pictures, in an exceedingly specific order, conferred in an exceedingly graphical interface (GUI). For this reason, the graphical-password approach is termed graphical user authentication (GUA). The most common computer authentication methodology is to use alphabetical usernames and passwords. This method has been shown to have significant disadvantages. For e.g., users tend to choose passwords that can be easily guessed. On the other hand, if a password is difficult to guess, then it is often difficult to remember. To overcome this drawback of low security, Authentication strategies square measure developed by researchers that use pictures as password.

Keywords: Images based password, Recall based technique and Recognition based technique, Watchword

I. INTRODUCTION

Graphical passwords talk over with victimization photos (also drawings) as passwords. In theory, graphical passwords area unit easier to recollect, since humans bear in mind photos higher than words. Also, they ought to be a lot of proof against brute- force attacks, since the search space is practically infinite. In this methodology, the user can transfer pictures from his/her personal gallery/directory for watchword choice and pictures uploaded by one user won't be visible to different users. Graphical positive identification is employed as an alternative to textual/traditional alpha-numerical positive identification. Traditional alphanumerical positive identification is troublesome to con and typically forget by users as times passes once user stays unattached from the system, but in case of the graphical password there are fewer probabilities to forget positive identification as a result of folks bear in mind pictures a lot of simply than text primarily based positive identification. There are fewer probabilities for hackers to steal the graphical primarily based positive identification as a result of hackers are going to be unable to access the photographs uploaded by the user as positive identification.

Password is a secret that is used for authentication. Passwords are the commonly used method for identifying users in computer and communication systems. It is supposed to be known only to the user. There area unit several authentication techniques like matter, graphical, biometric, charge account credit, etc.

II. LITERATURE REVIEW

Ahsan et al[1]Graphical password authentic- ation using image sequence: Graphical passwords techniques are classified into two main categories: recognition based and recall based graphical techniques. In recognition based techniques some images are shown to the user during registration. The user has to select some images from the number of images. Afterward, as the name indicates for valid login user has to recognize those preselected images in a correct sequence. In recall based techniques user has to draw some shapes such as circle, square, etc., at the time of the registration phase. While login to the system, the user has to produce the same pattern on the two-dimensional grid.

Gupta et al[2]Combination of textual and graphical based authentication scheme through the virtual environment: The user performs a series of actions on the objects which are provided on the tile board. Each object has its own property such as object type and object position. The movement of objects performed by the user is tracked down at each step. In this process, both mouse events and keystrokes are tracked. The sequence of the password generated is decided by the serial movement of the objects on the board for each individual move. The location and the properties of the involved objects which are tracked during the above process are stored in the database.

Asmat et al[3]Conundrum-pass: A new graphical password Approach: Two algorithms are involved: picture_Division( ), image_Shuffling( ). Firstly: Application asks the user to pick in their desired image which they would want to have on their lock screens. Secondly: User will be asked to selected image will be divided in the form of a square matrix of selected number .i.e. if the user selects 2, 3, 4 Image will be in the form of order 2*2, 3*3, 4*4 matrix respectively. picture_Division ( ) algorithm is used to divide the picture into multiple chunks. Thirdly:The user will consider the sliced picture as dial pad and generate the desired pattern by selecting pictures chunks.This pattern will be stored in the database. Fourthly: The selected chunks will be noted, and later whenever the user will try to unlock.

Biswas[4]Password Security system with 2-way authentication: The proposed system requires a new user to provide a text password, a bitmapped graphics image, and a secret key while signing up along with a unique user name and other details. The proposed system identifies two different sets of pixels on the bitmapped image. One set of pixels and the secret key are used to cater to the image verification process. The other set of pixels is used to prepare the password derivative. The secret key is stored in the user record in the host database. Creating password derivative: The ASCII value of each character of the text password is compared against the decimal value of a specific color segment of a specific pixel. The proposed solution asks the users to enter the text password and upload the bitmapped image for a successful login. Once the required steps are completed, the image authentication is performed followed by the user authentication.

Shen et al[5]Random Graphic Grid Pattern Generation State: Running a specific self-development algorithm to generate 9-digit number random positions is able to merge to different Recognition Grid Patterns while Random Grid Pattern Generation State occurs. The random two-dimensional three X three grid pattern is that the main distinction with robot Unlock Pattern. The mobile device has the ability to pre-process one-time authentication grid pattern referring to the pre-stored passwords for saving graphic pattern processing time in case of the hardware limitation.

III. IMPLEMENTATION

There are four main features of the proposed technique

i. Valid email: throughout registration user can offer a sound email address which can be entered throughout the login section. After coming into the valid email address system can direct to next page which can show pictures choice page

ii. Range of pictures: throughout registration, the user can have to be compelled to choose most half-dozen and minimum of four images that are necessary to be uploaded to finish the registration method. During login, section user can have to be compelled to choose a range of pictures that were uploaded throughout the registration section. If the amount of elect pictures is wrong then the user is unable to login.

iii. Pictures from the personal directory: The user uploads desired pictures from the personal directory. Advantage of this system is that pictures uploaded from the personal directory are simply memorized and these pictures aren't visible to alternative users. These images are only visible to the authorized user.

iv. Sequence of pictures: vital and key issue of this method is a sequence of images. The sequence of images is stored in a database. At the time of login, the user selects uploaded pictures in the same sequence because the sequence of pictures was elect throughout the registration section. If the sequence of elect pictures is wrong then the user can unable to login.

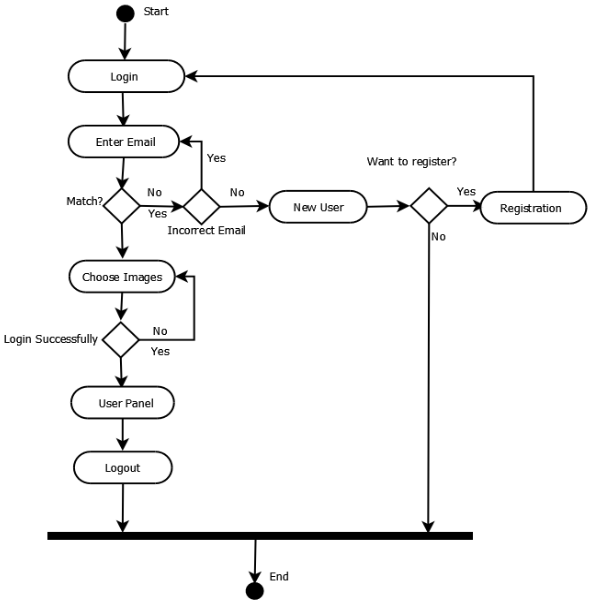

FIGURE 1: ACTIVITY DIAGRAM

IV. METHOD IMPLEMENTATION

To check the similarity of images 6 functions are used:

1. mimeType() : Returns array with mime type and if its jpg or png. Returns false if it isn't jpg or png
2. createImage() : Returns image resource or false if its not jpg or png

3. resizeImage() : Resizes the image to a 8x8 square and returns an image resource
4. colorMeanValue() :colorMeanValue fun- ction to take out the color mean value of the image. It will also list the pixels of the colors. This function will return the mean value array.
5. bits(): Returns an array with 1 and zeros. If a color is larger than the average of colors it's one
6. compare():It is the main function.

Returns the hammering distance of two images' bit value.

```
public function compare($a,$b)

{$i1 = $this->createImage($a);
$i2 = $this->createImage($b);
if(!$i1 || !$i2)

{ return false; }
$i1 = $this->resizeImage($i1,$a);
$i2 = $this->resizeImage($i2,$b);

imagefilter($i1,IMG_FILTER_GRAYSCALE);
imagefilter($i2, IMG_FILTER_GRAYSCALE);
$colorMean1= $this->colorMeanValue($i1);
$colorMean2=$this->colorMeanValue($i2);
$bits1 = $this->bits($colorMean1);
$bits2 = $this->bits($colorMean2);

$hammeringDistance = 0;
  for($a = 0;$a<64;$a++)
                              {
        if($bits1[$a] != $bits2[$a])
                                     {

                $hammeringDistance++;
                                             } }
                return $hammeringDistance; } }
```

V. RESULT

The comparison was based on Security, Installation Cost, Data Redundancy, Acceptance, and how much easy to memorize proposed system is acceptable over the textual password, images uploaded from the personal gallery are easily memorized, it is easy to use, uploaded images are not shown to unauthorized users.

VI. FUTURE WORK

Having studied totally different recent graphical positive identification authen- tication techniques and subjecting them for usability options that's memorability, creation time and login time and comparing the security features of each of them by considering their password space, dictionary attack, shoulder surfing, and brute force attack. Every technique has sensible resistance to varied positive identification attacks, however not one technique is ideal with subject to usability.

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

Is the scheme easy to execute?

Memorability of the image.

Prevention against Social Engineering, Shoulder surfing, Brute force, Dictionary attack, Guessing.

VII. CONCLUSION

Graphical passwords are another to matter character set password. It satisfies both conflicting requirements that are it is easy to remember and it hard to guess. Graphical passwords could supply higher security than text-based passwords as a result of many folks, in an effort to study text-based passwords, use plain words (rather than the suggested jumble of characters).

REFERENCES

[1].Muhammad Ahsan, Yugang Li. “Graphi- cal Password Authentication using Images Sequence.” International Research Journal of Engineering and Technology (IRJET). Volume: 04 Issue: 11 | Nov - 2017.

[2].Deepika Gupta, Akhand Pratap Singh, Dr. Vishal Goar, Shikha Mathur.” combination of textual and graphical based authentication scheme through virtual environment”.IEEE.2017.

[3].Nida Asmat, Hafiz Syed Ahmed Qasim.”Conundrum-pass: A new graphical password approach.” 2nd international conference on communication, computing and digital systems(C-CODE).2019.

[4].Subhradeep Biswas.” Password Security system with 2-way authentication.”Third International conference on research in computational intelligence and communi- cation network(ICRCICN).IEEE.2017.

[5].Sung-Shiou Shen, Tsai-Hua Kang.” Random Graphic User Password Authenti- cation Scheme in Mobile Devices”. IEEE. 2017.