Securing Graphical Password Using Selected Region

1. *Jagadhane Vijaya H., Information Technology, Sanjivani COE, Kopargaon, Maharashtra, India*
2. *Barahate Savita E., Information Technology, Sanjivani COE, Kopargaon, Maharashtra, India*
3. *Salve Shubhangi S., Information Technology, Sanjivani COE, Kopargaon, Maharashtra, India*
4. *Yeole Gayatri D., Information Technology, Sanjivani COE, Kopargaon, Maharashtra, India*
5. *Rajput Shital B.,Information Technology, Sanjivani COE, Kopargaon, Maharashtra, India*

ABSTRACT

Most of the System demands high degree of integrity to secure users personal data. Now a days all system present various password strategies including textual password as they are easy to remember if they are simple and hard to remember if they include hard symbols to have strong password authentication strategy, and Biometric system having physical damage problem of human. Number of strategies to crack textual password are present Securing Graphical Password Using Selected Region is one of the solution to this problem. They avoid dictionary attack as compare to textual password. We introduced three feasibility studies to secure password using selected region by examining its usability present Locimetric password includes reliability study, image featured based system. The usability evaluation study measure static digital images error rate and completion time. The Draw a line highlights resistance to observation. We introduced cued click point algorithm to increase the password space to make system more protected. Securing graphical password maintains the security by various usability of current password scheme on android device.

Keyword: - *textual password, dictionary attack, Locimetric password, usability evaluation, Draw a line, graphical password, security.*

INTRODUCTION

Authentication is important for every system to make it secure. It plays a major role from high secure applications to less secure applications. [1] It is important to secure the information exchanges from daily transactions to daily user email account. The most critical issue in today's world is providing security in applications such as military and ATM centers which need high security. In this system we develop or use particular image region as a password. In that image we are Choosing a few particular point that point is nothing but our system password. User has to click this point again at the time of log into the system. If user forget these point at the time of log in then user cannot log in into the system.[3]

In that system we are using mainly three technics.

1. Locimetric Password Schemes. [2]
2. Usability Evaluation. [4]
3. Draw Password.

Locimetric Password Scheme[2]: In this technique the user can select one image, In that image they can select a particular point as a password. If the user can enter a point that can be selected previously at the time of registration then user can log into the system successfully.

Usability Evaluation: In this technique the user can select public image or private image.

In public image the image can already available in system or the image can publically available.

In private image user can use their choice of image.

Draw Password: In this technique the user can draw password on image in that point will be consider to store in database.

LITERATURE SURVEY

The Graphical password system uses the android smart phone with image as a password. Now a day's use of computers has many security method concerns. Where, legal resources should be determined. Authentication is the major security concern. Techniques are classified as follows:

• Textual Passwords

• Biometric schemes

• Graphical Passwords

2.1 Textual Password Textual password includes various passwords using keyboard keys present special symbol, character etc.[4] Increasing use of this password more attacks are there related with textual password. User prefers this password as they are faster as an input.

2.2 Biometric Password Biometric authentication validate the user by body parts such as face, finger print etc. Biometric Password finding more problems with their implementation requires more hardware cost. By proper utilization they are more secure than other password strategies[5]-[7].

2.3 Graphical Password Authentication This scheme includes various graphical methods to use as a password. They use static as well as dynamic images as password. They are having advantages and disadvantages.

2.3.1 Perrig and Song They introduced Hash Visualization System [8] which is recognition based graphical password. This system is not resistant to brute force attack, shoulder surfing attack and random guessing attack as it is using static images are randomly presented and user has to select one of the images from that as a password. This is better than Textual password but it is very slow

2.3.2 Passface Passface [9] This proposed system similar to Perrig and Song system. Instead of random images the faces are provided. In a present system it is easy to remember faces, But this system cant resistant to brute force attack and shoulder surfing attack.

2.3.3 Sobrado and Birget This system introduced password scheme with different method. Large number of images is provided to the user at registration phase, user has to select the correct order at the time of login. This system is faster as compare to previous system used and easy to implement. They effectively avoid shoulder surfing attack but not resistant to brute force attack at better level.[10]

2.3.4 Draw-a-Secret (DAS) Draw a secret. This technic includes drawing a secret password using graphical grid or draw a symbol. Drawing reproduce password correctly after Authentication. Symbol and grid requires more space to store password. [8]

2.3.5 Persuasive Cued Click Point (PCCP) Technique prevents the user from selecting easily guessable spot in the click based graphical passwords. [6] Random images are provided at the time of registration, user click the point on the images as images appeared. At the time of Login user has to recall all the click of registration phase. This is advantages graphical system and prevents guessing attack. [12]

Existing Graphical password limitations:

- Shoulder Surfing Attack
- Brute force search Attack

We have concentrated in these two attacks because, till now these two attacks have not been eliminated in existing graphical passwords.

EXISTING SYSTEM

The previous system using textual character, special symbol as a password for authentication that are resistant to brute force attack [5] still is having various attacks to be introduced. They are difficult to remember if strong textual password used then they are difficult to remember. User tends to choose short and simple password.

Biometric password scheme give physical body parts as a password. This system includes cost effective software. Difficult to implement requires additional hardware cost and deployment cost. Authentication method [7] includes strategies to be used in manual manner.

SYSTEM ARCHITECTURE

Locimetric password scheme:

Cued-recall (locimetric) password system involves user selecting region on one or more images. During login users are choose a previously selected image and they enter a password by clicking on a sequence of location on the image. If users log in to the system successfully, means the x y coordinates of these click match a previously stored set of password point. In loci-metric system is there is one problem that is observation a password. Click point can be acquired by attacker after viewing a single authentication process. But securing against observation attack for graphical passwords system is used. We are providing UMI (user interface Manipulation) such as reducing the text size of the mouse cursor or dimming.

Usability Evaluation:

In this system users can be authenticated by using two techniques.

1. Private image

2. Public image.

The public image can be available publically on user's device or it can be available on internet. If attackers know the public image they can try to attack on users system. But there is one problem in that the attackers' public image and user's public image region may be different. The resolution is depend on the device.so the attack van be avoided. Private image can be stored on user's private phone memory or the user can choose of picture as a password.

In this system users need to first register on system. At the time of registration user will provide all their personal information such as name, email and phone number and choose the technique they want. For example Locimetrc technique, Usability Evaluation, Draw password schem.at the time of registration user need to select image in that image select particular point as password. After registration user need to log in to the system. In login process user provide their name and technique that they previously chooses. In login process user need to enter the password again that selected previously.

The user will select the picture from the gallery and upload in to the server and also upload the details like Employee name, Employee name, Employee id and bill details. All the details uploaded here is stored in to the server. After uploading the details the user can check the status of the request using same application. The user requested data can be view by the higher authority. Admin is the authority to accept or the reject the request.

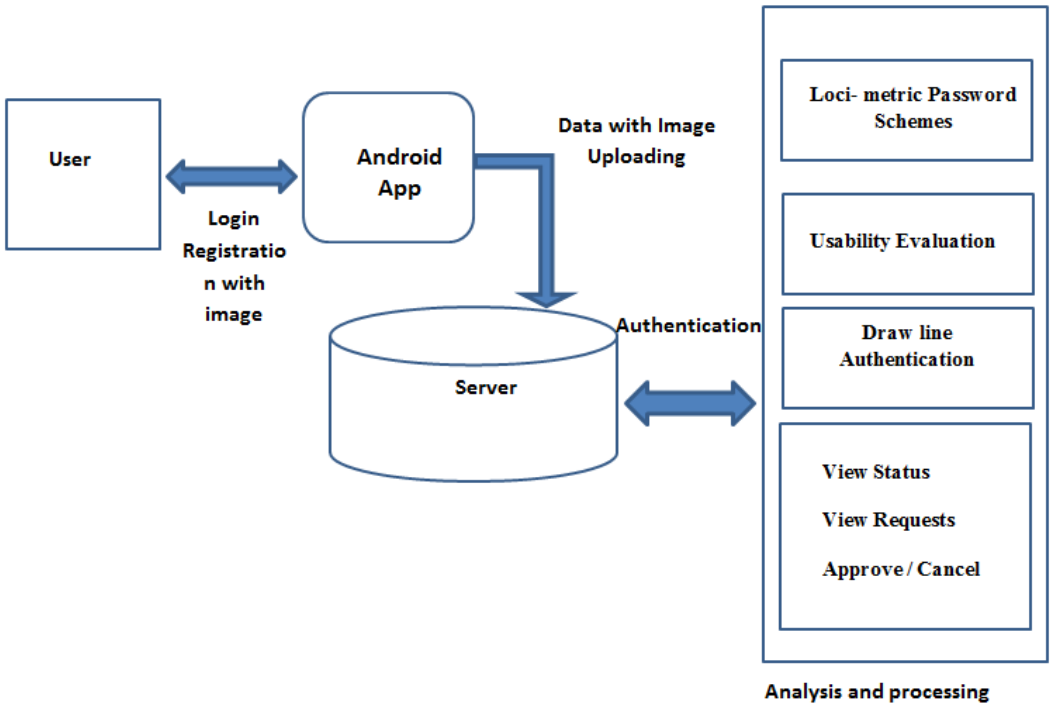

Fig.1. Architecture Graphical Password System.

In figure 1 shows our proposed architecture system. There are Seven components in our Graphical system: User phone, Android app, server, Locimetric password, Usability study, Draw line Authentication, View status, View Request, Approve/Cancel. Fundamentally the research method followed the architecture system in 1. We develop application on android smartphone utilizing java. Then developed the application for admin. The last step was developed Analysis and Processing connected to all component.

RESULT

In this research we build coding for graphical password authentication system. We introduce three studies to have a more secure graphical password.

A. Locimetric password study:

This application runs on android in which user has to register on the admin side by selecting image region as a password.in that feature includes curd click point algorithm which extract selected image feature that will store in database. At the time of login user has to select password which selected at a registration time that will produce secure system.

B. Usability evaluation:

In these study users will be authenticate in two condition

1. Private image
2. Public image

In private image participants has to ensure image for password is there in a smart phone and share in its memory. In public image the image is already available in participants' smart device gallery to choose.

C. Draw Password:

In these technique the user can draw password on image in that points will be consider to store in database as a password.

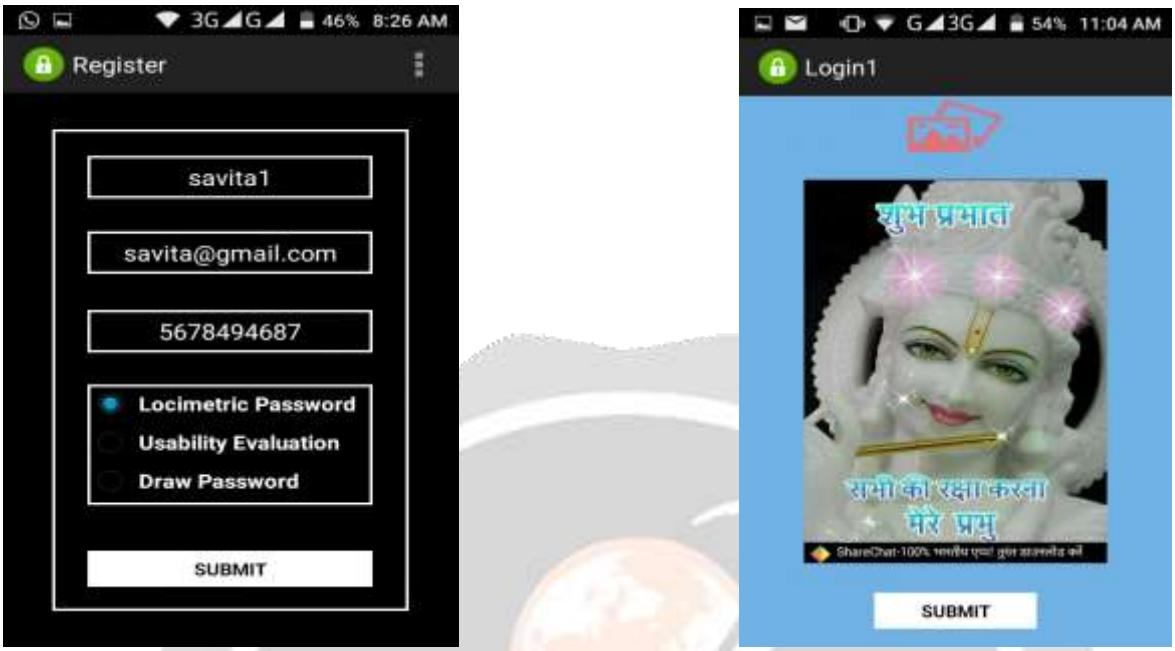

Fig.2. Registration and Login System

CONCLUSIONS

In today's world increasing habitude of web services and digital app. Users are able to access this Application in any android device. In order to protect user's digital device Authentication is very important. If we are try to protect our system in publically might be possible to occur shoulder surfing attack. Even though the complicated password, numerical password are easily guessable.

To overcome these problems we are proposed securing graphical password using selected region. Help of these system we can protect our device as well as personal account.

REFERENCES

[1] A. Adams and M. Sasse Users is not the enemy Commun. ACM pp 40–46 1999.

[2] M. Adham and A. Azodi and Y. Desmedt and I. Karaolis How to attack two factor authentication internet banking in Financial Cryptography 2013 pp 322–328.

[3] ARTigo http://www.artigo.org/.

[4] F. Aloul and S. Zahidi and and W. El-Hajj Two factor authentication using mobile phones Proc. Comput. Syst. Appl 2009 pp 641–644.

[5] R. Biddle and S. Chiasson and P. van Oorschot Graphical passwords: Learning from the first twelve years ACM Comput. Surveys vol. 44 no 4 p. 19 2012.

[6] G. E. Blonder Graphical passwords U.S. Patent 5 559 961 1996.

[7] J. Bonneau and C. Herley and P. C. van Oorschot and F. Stajano The quest to replace passwords: A framework for comparative evaluation of webauthentication schemes in Proc. IEEE Symp. Security Privacy 2012 pp 553–567.

[8] S.Chiasson and R. Biddle and P. van Oorschot Asecond look at the usability of click-based graphical passwords in Proc. 3rd Symp. Usable Privacy Security 2007 pp 1–12.

[9] S. Chiasson and P. C. van Oorschot and R. Biddle Graphical password authentication using cued click points in Proc. 12th Eur. Symp. Res. Comput. Security 2007 pp 359–374.

[10] S. Chiasson and A. Forget and R. Biddle and P. C. Oorschot User interface design affects security: Patterns in click-based graphical passwords Int. J. Inf. Security vol. 8 no. 6 pp. 387–398 2009.

[11] S. Chiasson E. Stobert A. Forget R. Biddle and P. C. Van Oorschot Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism IEEE Trans. Dependable Secure Comput., vol. 9 no. 2 pp 222–235 Mar./Apr. 2012.

[12] A. De Luca and E. von Zezschwitz and N. D. H. Nguyen and M. Maurer and E. Rubegni and M. P. Scipioni and M. Langheinrich Back-of-device authentication on smartphones in Proc. SIGCHI Conf. Human Factors Comput. Syst 2013 pp 2389–2398.

[13] B. Dodson and D. Sengupta and D. Boneh and M. S. Lam Secure consumerfriendly web authentication and payments with a phone in Proc. 2nd Int. ICST Conf. Mobile Comput. Appl. Serv. 2010 pp 17–38.

[14] K. M. Everitt and T. Bragin and J. Fogarty and T.Kohno A comprehensive study of frequency, interference, and training of multiple graphical passwords in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2009 pp 889–898.