ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ANDROID BASED GRAPHICAL PASWORD AND PIXEL BASED PATTERN RECOGNISATION SYSTEM

R.Akshaya Yogeswari*, V.P.Manikandan, D. Durai Kumar

* M.Tech-Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

Assistant Professor, Dept. of Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

Associate Professor & Head, Dept. of Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

ABSTRACT

Many of user using textual password. These textual passwords are easily hacked by the attackers using Guessing attacks and Shoulder Surfing attacks. Android based Application is developed in which User name and Password is provided to the Server. User name and password is entered in the system and Password characters are assigned with the corresponding Alphabetic Characters with Numbers, eg "ABCD" is considered as "1234". When all the numbers are added it equals to "10". Finally 1+0 = 1 this is corresponding to the Alphabet "A". User Chooses Two Images in A Section from server provided image set. From the two image user select t he particular pixel as password and it will be stored in server. User is authenticated with these Images. Next time Android user logins to the server by selecting the Surrounding Pixel of those Images along with the User Name and Password.

KEYWORDS: Graphical password, password, hotspots, Captcha, shoulder attack.

INTRODUCTION

When anyone wants to access the network, for security purposes every web application provides user authentication. From ancient day's secret data or code is used for hiding and giving security to information. In user authentication the process which we have to pass through is username and password. Authentication process divided into Token based authentication, Biometric based authentication and Knowledge based authentication. Most of the web application provides knowledge based authentication which include alphanumeric password as well as graphical password. In today's changing world when we are having number of networks and personal account some sort of easy authentication schema need to be provided.

In recent years, computer and network security has been formulated as a technical problem. A key area in security research is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this context, the password is a common and widely authentication method still used up to now.

A password is a form of secret authentication data that is used to control access to a resource. It is kept secret from those not allowed access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly.

This paper is based on securing cloud by using graphical password. Cloud security can also be given by alphanumeric password but thing matter is that use of alphanumeric is not that much of secure and easy to remember. One more important thing is that every time users have recalled the password. User has to give priority to security beyond their need so as to satisfy their work.

Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 1008, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password. If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take millions of years to break into the system by hitting it with random image sequences.

GRAPHICAL PASSWORDS METHODS

In this section, some graphical password systems based on recognition and recall-based are discussed. Graphical based password techniques have been proposed as a solution to the conventional password techniques because graphic pictures are more easily remembered than texts which most of researchers have nominated them as "Picture superiority effect" .A literature on most of articles regarding graphical password techniques from 1994 till January 2009 shows that the techniques can be categorized into three groups as below.

Recognition-Based Technique

In this category, users will choose pictures, icons or symbols from a collection of images. In authentication process, the users need to recognize their registration choice among a set of candidates. The research shows that 80% of users can remember their passwords only two months only.

Pure Recall-Based Technique

In this category, users need to reproduce their passwords without being given any reminder, hints or gesture. Although this category is easy and convenient, but it seems that users hardly can remember their passwords similar to DAS (1999)and Qualitative DAS (2007).

Cued Recall-Based Technique

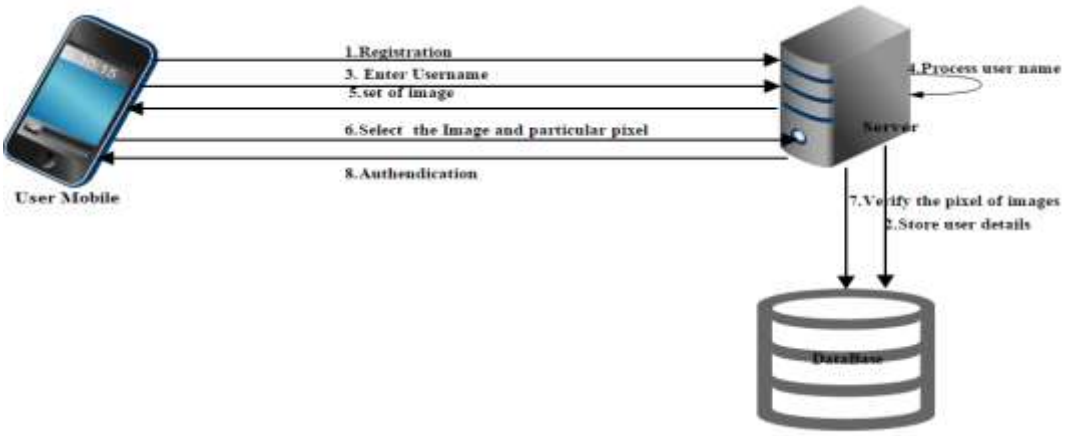
In this category, the technique proposed a framework of reminder, hints and gesture that help the users to reproduce their passwords or help users to make a reproduction more accurate similar to Blonder Algorithm (1996) and Passpoint(2005).

RELATED WORK

SYSTEM MODEL

User is register the user name and password in the sever system. The user of application will login next time in the application they give the user name in the system. They provide set of images to user. Selecting the surrounding pixel of those images along with the user name and password .The developed a graphical password technique that deals with the shoulder surfing problem . In their first scheme the system displays a number of pass-objects among many other objects as image to user . To be authenticated, a user needs to recognize pass-objects and click inside convex hull formed by all the pass objects.

Figure



Architecture diagram

User Registration

Mobile Client is an Android application which created and installed in the User's Android Mobile Phone. So that we can perform the activities . The Application First Page Consist of the User registration Process. We'll create the User Login Page by Button and Text Field Class in the Android.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

While creating the Android Application, we have to design the page by dragging the tools like Button, Text field, and Radio Button. Once we designed the page we have to write the codes for each. Once we create the full mobile application, it will generated as Android Platform Kit (APK) file. The application developed in android Emulator. This APK file will be installed in the User's Mobile Phone an Application.

They can be classified into three categories according to the task involved in memorizing and entering passwords:

- recognition,

A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Passfaces wherein a user selects a portfolio of faces from a database in creating a password.

Dhamija and perrig scheme
Pick several pictures out of many choices,identify them later in authentication.

Figure

Android Emulator

User Signin Module
When you login to cloud server the Cloud service they will be provided with options to select. For registration user have to pass through authentication process. In that on the basis of username, process will be started at the server-side. Set of images which will be provided to user are based on result of calculation. if the password and image matched then user valid other invalid.

At the server-side position of username's alphabet in alphabet series will be calculated. Then addition of all the positions is done. First digit of that sum will be considered for further calculations.

Alphabets	L	M	N
O			
Position 11	12	13	14

Finding the set to be assigned
Calculation of result: L+M+N+O=11+12+13+14=50.

Multiple-image based
In this scheme number of images will provided to user they have to select one or more of them.
Graphical Pattern Registration
There are total 26 alphabets present in alphabet series. We have values between 1-9 in password calculation. From the calculation Server has made set of images for 0-9 positions . Set of images will be assigned according to result of calculation. The set of images is given to user side ,from that images it will shown .

The server calculate the values and the resulted is shown to user application for registration phase.User side it will shown that specified image ,they selected particular image .from that image select particular position of image selected has graphical password.

Calculation Based Image Selection
In this complete password is divided in two sections ,first section is based on server provided sets of images, second section is based on user selection. From sever end two images will be provided to user so as to form complete password. For user selection, from given set of images user has to select two images as the password.

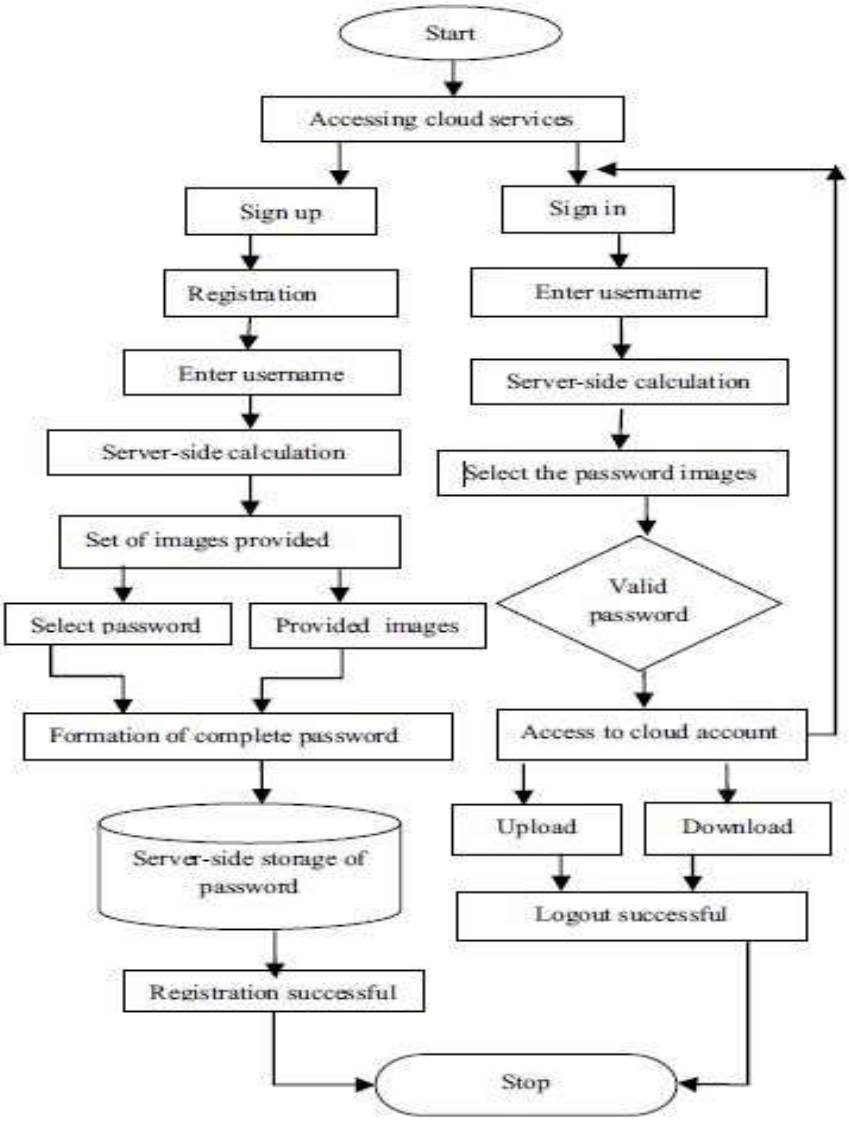
Graphical Pattern Detection Module
Image-based schemes use images including photo graphics, artificial pictures, or other kind of images as background. Based on the number of images displayed. From that two images is displayed for user application. User select particular part of image as password and then select next image user selected in registration as earlier in signup process. If user selected correct position of images pixel only, the server authenticate user to allow to access application.

Graphical password provides more security than text, sound and alphanumeric password. Most of the alphanumeric authentication chooses a plain text or easy password to avoiding the confusion. Most of the system provides image related password i.e. graphical password. In this method selectable images are used, user can have more number of images on each page and among the password is selected in the system

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

.

Figure



Flow diagram

CONCLUSION

Thus graphical password authentication can be given by taking cloud as a platform. The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password techniques .The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords It can also be useful for user in security point of view. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords,it login in android mobile application. The new scheme provides solves the many problems of existing system.

REFERENCES

1. Moin Mahmud Tanvee1, Mir Tafseer Nayeem2, Md. Mahmudul Hasan Rafee3 " 2-Layer CAPTCHA Based on Cognitive Psychology for Securing Web Services",2011

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

2. Moin Mahmud Tanvee1, Mir Tafseer Nayeem2, Md. Mahmudul Hasan Rafee3 " 2-Layer CAPTCHA Based on Cognitive Psychology for Securing Web Services",2011
3. Tapan Chauhan ,Nisha Shah" A Novel Captcha Study based on Image Selection Scheme",2014
4. Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare"Graphical Password Authentication",2014
5. Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang "A Graphical Password Based System for Small Mobile Devices ",2011.
6. Robert Biddle, Sonia Chiasson, P.C. van Oorschot" Graphical Passwords:Learning from the First Generation",
7. Yavatmal, MS" Graphical Password Authentication system in animplicit manner,SUCHITA SAWLA"2012