M-Banking using Steganography and Persuasive Cued Click Points (PCCP) based Authentication

Arshad Awati, Namrata Pawar, Shikha, Aparna Hambarde

Computer Engineer, arshadawati11@gmail.com, 8149830332

Abstract — Graphical password using cued click points is one of the alternative and better solutions to alphanumeric passwords. As it is very tedious and lengthy process to remember alphanumeric password in any application. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits and one can easily break the passwords by several simple means such as dictionary attacks, social engineering attacks& shoulder surfing attacks,. In this paper we are representing the authentication given to mobile banking application by using graphical password. Authentication is a process by which the identity of the user is verified by the system. Thus we have proposed mobile banking application with graphical security by means of Steganography and Persuasive Cued Click Points. We are providing one of the algorithms which are based on selection of username and alphanumeric password for logging in into the application and series of images as a password for Fund Transfer. Implicitly the Persuasive Cued Click Point based authentication system provides more immunity to the common attacks suffered by other authentication schemes.

Keywords— Persuasive Cued Click Points, Grid, Graphical Password, Steganography, Image Processing, Authentication, Security, Cloud Security.

INTRODUCTION

When someone wants to access the network, every web engine provides user authentication for security purpose. For hiding information secret code is being used from ancient time. Previous survey concludes that text passwords can be detected. Easily by intruders by various simple means such as attacks due to shoulder surfing, social engineering attack, dictionary attacks. Hence to deal with such traditional problems with traditional methods, advancement in methods have been proposed using graphical/images as passwords, such as Persuasive Cued Click-Points (PCCP).This paper basically provides cloud security by using graphical password. Alphanumeric password can also be done by using cloud security but the problem is that this method is not much secure as well as easy to remember. The important thing is that each and every time the user has to recall the password. Priority has to be given by user for security purpose in order to satisfy their work. The aim of this work is to provide 2 levels in terms of security for transaction in banking applications. First we are making use of Steganography for sending user id and password on server using Steganography encoded image from the user's mobile phone. Once the user is authenticated he will be shown with a graphical password screen. A sequence of images will be provided to the CCP User with 4x4 blocks and user will have to select one block for each image. Secondly, if incorrect image is selected by the user during login, the successive image displayed will also be incorrect. Authenticated users who know the correct sequence of the images would know that they clicked on a wrong point and would go for the right image. So this feedback is not at all helpful to the attacker who is unaware of the expected sequence of images.This way security level is improved by using "Steganography" technique and graphical authentication in mobile banking applications.

LITERATURE SURVEY

Many attempts were made to improvise the means of securing. Various researches have been done and many methods for the graphical password authentication have been proposed till date. Some of the methods are as follows:

A. Image based scheme

Image-based schemes use images including photo graphics, artificial pictures, or other kind of images as background.

Advantages:

User can easily remember the password as it given in images.

Disadvantages:

Image based password is very long process user have to pass through selection of number of images. It consumes user's time also.

B. Graph based scheme:

In this scheme graphical passwords are at grid background.

Advantages:

There is no need of storing graphical database at server- side. Grid is simple object so no extra displays are needed.

Disadvantages:

During authentication the sequence can be changed or grids may be different as it is a drawing.

C. Hybrid authentication:

In hybrid scheme user needs to rate the number and thus finds a particular sequence of colours and remembers it.

*Advantages***:**

Since the colours are already provided to the user so user has to remember only the sequence.

Disadvantages:

It becomes quite difficult to remember the sequence of colour as well as sequence.

D. Signature based scheme:

In signature based passwords user has to set a signature kind of password and every time he authenticates he needs to draw the same signature for the password authentication.

*Advantages***:**

Signature as password is very difficult to be get cracked. A small mistake in drawing the signature will deny the access to the password authentication.

Disadvantages:

Remembering the grid signature is not easy to remember. So the authenticate user may fail many times to access it properly.

PROPOSED SYSTEM

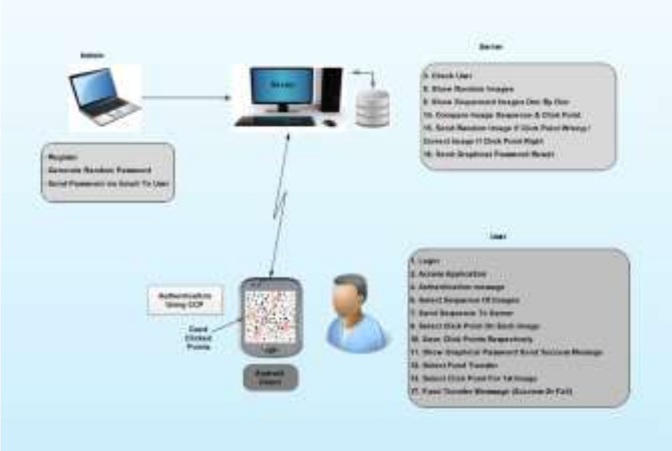


Fig.1 Block diagram

1. How to start

When one starts 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.

Username: ABCD

2. *Flow of proposed system*

When the user tries to access the application they will be provided with two options sign in and sign up. If it is new user, user will have to first sign up. After sign up process user will be allowed the access to the application. And if the user has already signed up, he simply has to sign in with the username and password with which he had signed up, and the user can now access the application according to his need. At server side calculation in sign up registration is made for user.For accessing the application further like fund transfer, User have to enter the username based on that particular image set which will be provided to them on the basis of algorithm. In this algorithm first username is checked. After calculation set of images will be provide to user. User has to select five images as client side and it will be saved on server side as server side selection. So the complete password will be stored in database of server. In sign in the user have to give username which he or she has given during sign in and select the password from given set of images. Validation of user is done then cloud access is given to particular user. They access their account with uploading and downloading facility.

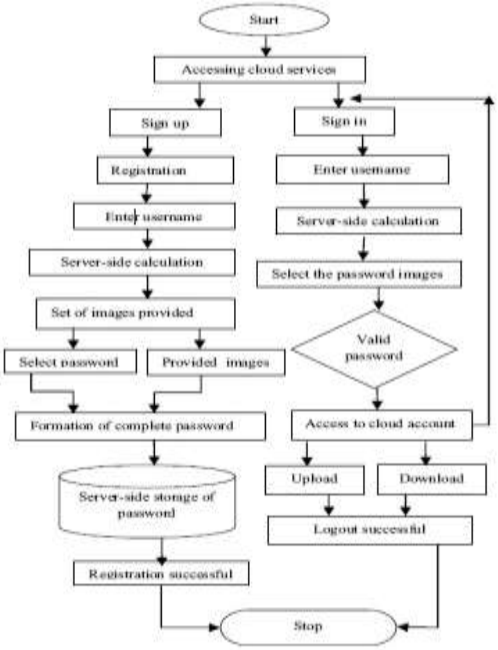


Fig. 2 Flow of proposed system

SYSTEM ARCHITECTURE

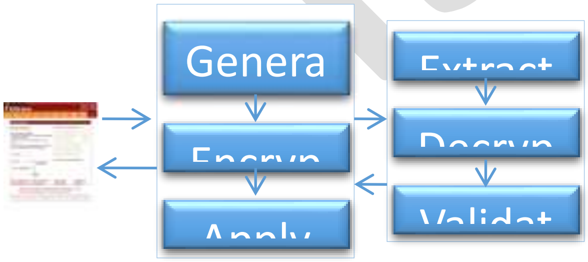


Fig. 3 System Architecture

EXPERIMENTAL SETUP AND RESULTS

The setup includes three sections of experiments in research. First of which is used to create server side which provides the cloud service and also used for authentication of the user. Second is to create client side where the login form is created for applying to the application. And the third is the admin where user authentication is done. Basically, the setup includes server, client and database. Server checks the user, shows random images to client in order to select images for password, server shows the images in sequential order and compares the sequence as well as the click point, and it checks whether the sequence is correct or not, according to the result it shows the graphical password. At the admin side registration of the client is done, it helps to create random images for the user, the password which is created by the admin for user to access the application is send via email. At the client side, user has to login via the login page present at this side, user can access the application through the username and password set, authentication message is send to the admin, the sequence of images which is provided by the server user has to select click point on every image, when fund transfer function is appeared on the application graphical password is being used, user has to click the point respectively according to the images to gain access of fund transfer, according to the password message is generated whether the login is successful or failed.

Software requirements:

Android sdk 2.3

Eclipse 3.3

***Hardware requirements**:*

Intel p4 with 256 Mb ram

Software interfaces:

XML

Servlets

Object Serialization

***Hardware interfaces*:**

RS232/ Ethernet/ Wi-Fi

Communication interface:

TCP / IP

***Tools to be used**:*

Netbeans 7.1

Eclipse 3.3

Android application:

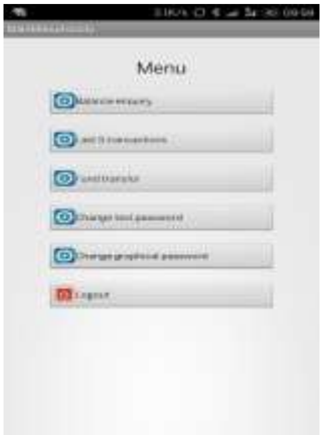


Fig. 4 Menu

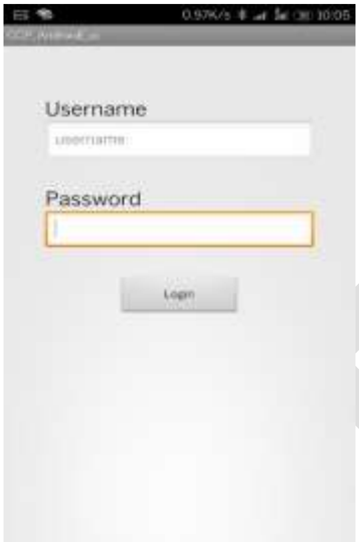
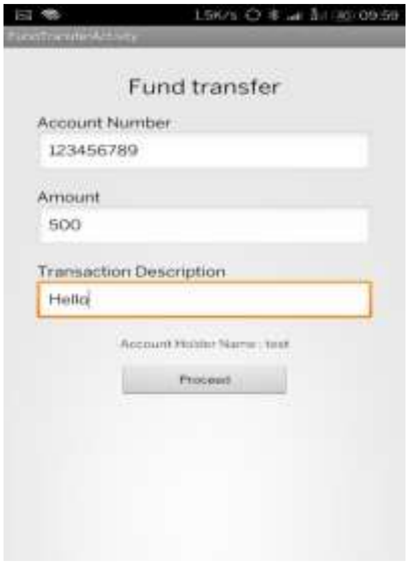


Fig. 4 Text password

This android application consists of various bank functions. For logging in to the application text password is provided to the client via email by the admin. Once we enter the application we can access the functions. Graphical password is provided for the fund transfer, as fund transfer nowadays is crucial process to follow. The graphical password is set by the images generated randomly by the server. Minimum five images should be selected by the user for generating graphical password. The above procedure is shown in the figure below.



Fund transfer

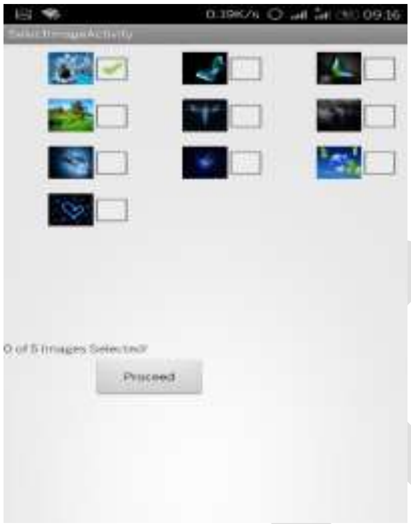
Account Number
123456789

Amount
500

Transaction Description
Hello

Account Holder Name : test

Fig. 5 Fund Transfer



0 of 5 Images Selected!

Fig 6 Graphical password

APPLICATIONS AND FUTURE SCOPE

Applications

1. Internet banking application Login.
2. Fund transfer and balance enquiry.
3. Graphical Authentication Using Cued Click- Points (CCP).
4. Secure E-banking applications for all banks.

Future Scope

Instead of direct sending of the information, it is encrypted and hidden in a picture using random bit Steganography Technique. Then the picture is sent to the server. After receiving the picture on server, the sample http download socket program downloads the image, decrypts it and decodes to receive the message. The message is then processed on the server to verify user Credentials such as user name and password. Once the user passes credential test, camera is switched ON, On the client side and image is captured. This image is then compared with the server face database images, on Successful match – is taken to the menu screen.

EMAINING CONTENTS

You can add the remaining content as it is but the heading must be Time New Roman Front of size 11 with bold and the content must be as of introduction i.e time new roman of size 10 and must be justified alignment

ACKNOWLEDGMENT

We consider it is our privilege to express our gratitude and Respect to all those who guided us in the completion of Technical paper. The research presented in this paper is supported by management of K.J's College of Engg. & Mgmt Research. It's a great privilege to place on record our deep Sense of gratitude to our HOD Mr. D.C. Mehetre, of Computer Dept. I am grateful to thank Dr.Sanjeev Wagh, Principal, KJCOEMR. We are grateful to our guide Mrs. Aparna Hambarde, for her invaluable support and guidance. We would like to thank the reviewers for their time and expertise, constructive comments and valuable insights

CONCLUSION

Thus graphical password authentication can be given by taking cloud as a platform. The new scheme provides solves the many problems of existing system. It can also be useful for user in security point of view. These results demonstrate that graphical password schemes can suffer from drawbacks similar to those of textual password schemes, notably biases in human tendencies to select memorable passwords. The proposed Graphical Password Authentication System in an Implicit Manner provides authentication information to be implicitly conferred to the user. If the user clicks the same points of interest compared with the server, the user is implicitly authenticated. No password information is exchanged or changed between the client and the server. Since the authentication information is conveyed, it can secure shoulder surfing and screen dump attack, which none of the existing schemes can tolerate. The strength lies in creating a good authentication and authorization space with a sufficiently large collection of images to avoid repeating cycles. Compared to other methods reviewed in this paper, it requires a lot of human-interaction and careful selection of images and Click points. It may also need user training. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware.

REFERENCES:

[1]Graphical Passwords, FABIAN MONROSE AND MICHAEL K. REITER, August 5, 2005
[2]Graphical Password Authentication system in an implicit manner, SUCHITA SAWLA*, ASHVINI FULKAR, ZUBIN KHAN, Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India. March 15, 2012
[3]Authentication Using Graphical Passwords: Basic Result Susan Wiedenbeck Jim Waters,College of IST Drexel University Philadelphia, PA, 19104 USA.
[4]S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.
[5]Steganography in digital media by Jessica Fridrich
[6]Graphical Passwords,FABIAN MONROSE AND MICHAEL K. REITER, August 5, 2005
[7]Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Susan Wiedenbeck Jim Waters College of IST Drexel University
[8]A Survey on Recognition-Based Graphical User Authentication Algorithms Farnaz Towhidi Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia .
[9] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.
[10] http://en.wikipedia.org/wiki/Steganography
[11]Zone-H.org (http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf