ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (392-398), Month: January - March 2015, Available at: www.researchpublish.com

Pel Based Secure Corroboration Using Graphical Cipher

Suvithra Udhayakumar[1], Vanishree Chandru[2], Vidya Venkataraman[3], J. Faritha Banu[4]

[1, 2, 3,4] Department of Computer Science and Engineering, R.M.K. Engineering College, Kavaraipettai, India

***Abstract*: Security plays a principal role in every part of internet services like E- Mail, E-Banking etc. Android appliances are becoming trendy in today's world. Pattern toning is used to provide security in all android phones. The employ of ciphers is known to be primordial. Cipher can be easily predictable by shoulder-surfing attack and guessing attacks, which stimulates the system to go out of order leading to timorous login. It can send unsolicited mails and reconnoiter all the personal minutiae. It is perilous to all cyberspace services. A new pel based secure corroboration is proposed to overture security by overcoming the sundry cipher attacks. The objective of the paper is to render impregnable corroboration in the field of wireless android mobile communication by customary login and encipher login. The encipher login is achieved by scheming the codes corresponding to the typescript of password based on which it is calibrated to a set of portraits. In the interim of registration, the ultimate user should elect any two metaphors from the rendered snapshot and then select a pel in each selected portrait. During login, username, cipher, metaphor and pel selection will vanguard to secure corroboration.**

***Keywords*: CAPTCHA, Metaphors, Cipher, Pel, Corroboration.**

I. INTRODUCTION

Security and legalization is of chief concern of every user in all fields. Since time immemorial, secret data or code is being used for hiding and giving security to information. Smart phones are waiting to be attacked by the hackers. Initially, corroboration process was carried at hand providing username and cipher in the field of mobile communications. Authentication process is classified into Biometric, token and Knowledge based authentication. Most of the web applications provide cognizance predicated authentication which include alphanumeric password as well as graphical passwords like CAPTCHA. A cipher is verbalized to be good and facile for a user if the ability to recollect the secret word is adequate and the efficiency of input is very high.[1] In general alphanumeric characters are used as password. Alphanumeric passwords can certainly be hacked. Whenever user ratify the alphanumeric password , some hint option provided, utilizing which hackers can effortlessly gain ingress to the system in less time. Drawback is that if one user has a number of accounts, to recollect all those passwords is simply not possible. In some of the cases it may transpire that one can forget the password when there is no frequent utilization of a particular account. Cipher or PINs can be easily resolved or bypassed. Even without passwords or PINs to bolt the contrivance, there is increased peril that embezzled phones' minutiae could be accessed by illicit users. To surmount this issue, pattern locks were introduced for mobile apps which also has its own downside. Password can be given in different ways, but there are different drawbacks of that which can be overcome by graphical password.[2]Graphical password provides enhanced security than alphanumeric password. In alphanumeric password, an eight character password is required to gain access of a particular system. But in graphical password a user has to select the images and approve the password. Whenever user passes through the authentication process, it is easy to remember the images which ever they have chosen previously.[3]Graphical password is providing more memorable password than alphanumeric password which can minimize the efforts for recalling a password. Since in today's world everyone is having a number of networks and personal accounts, some marginally handy and secure corroboration schema is highly essential.

II. SURVEY OF EXISTING SYSTEM

In the prevailing system, unstructured data, a rudimental task in security is to engender cryptographic primitives predicated on hard mathematical problems. Hard mathematical problem was used to provide security. Due to advancement in technology, security based on hard AI problem was introduced. Using hard AI (Artificial Intelligence) problems for security, initially proposed in is an exhilarating new paradigm. [4]Under this paradigm, the most significant primitive invented is CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond. These typescript ciphers are easily hacked by Guessing and Shoulder Surfing attacks. The major technical issues with CAPTCHA are 1) It is not compatible with all kinds of browsers. 2) Sometimes it is very arduous to read. 3) The deciphering time is drawn out.

Owing to these disadvantages researchers innovated a concept which allows every user to login into their financial records or accounts safely in short span of time.[5] The concept was just mapping of username typescript with the numbers and calibrating a crypt code based on which a user will be shown metaphor during selection. But there is a security issue in this concept because usernames are very easily guessable even by a customary chap. So we go in for a new concept with a minimum modification to crack this imperfection.

III. SYSTEM ARCHITECTURE

I. SYSTEM A:

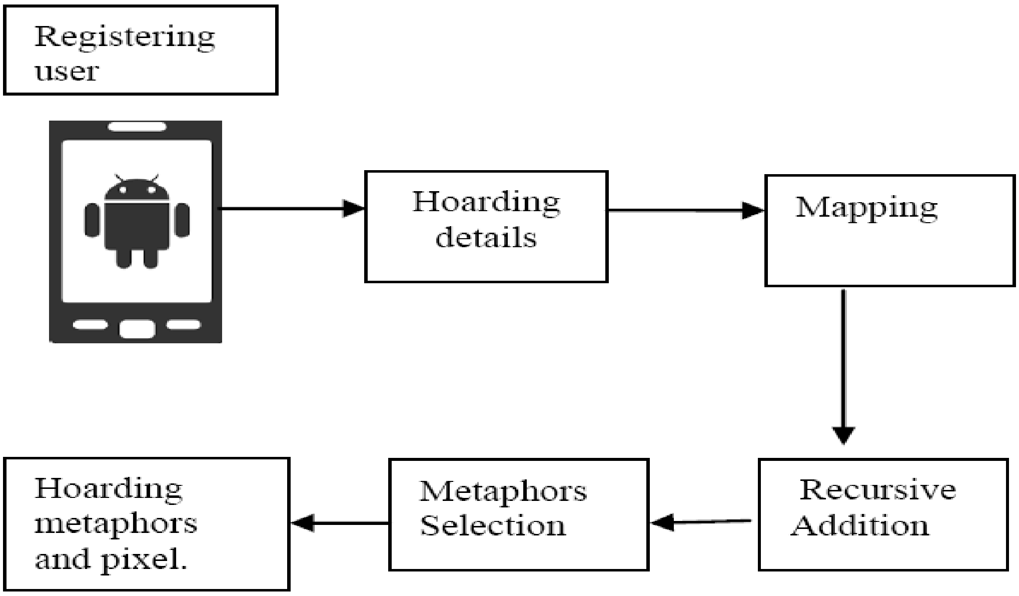


Fig: 1. During Sign Up

A. DURING REGISTRATION:

The mobile user must sign up firstly to do the finance operation. The mobile user gives all the required personal niceties during registration. The personal minutiae and the cipher given by the client will be stored in the database. Then the cipher's individual characters are ascertained and mapped to its arithmetic values. In order to perceive the cryptogram for the cipher entered, server will perform the recursive accumulation until a single digit cryptogram is attained. The default set of metaphors are ascribed to the nine distinctive single numeral cryptograms. Based on the aftereffect of computation, the set of metaphors will be displayed to the mobile client. User will elect two metaphors from the given set of metaphors .The selected metaphors are stored in the database. The user, then has to select the pel in each chosen metaphors .The selected pel in each of the metaphors is stored in the database. Subsequently, the user will be registered. Eventually, an exclusive account number will be provided to the successfully registered user.

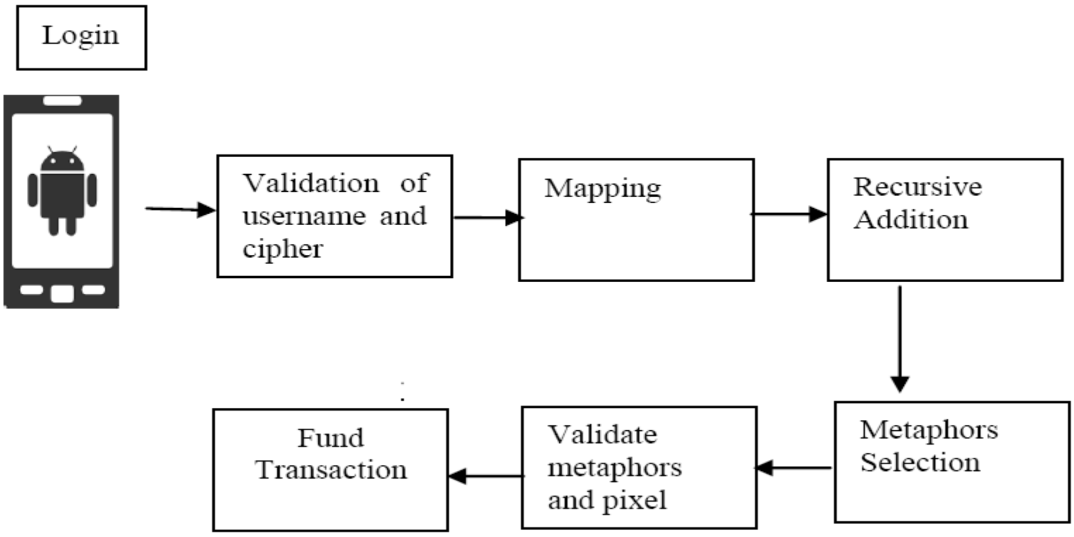


Fig .2.During Sign In

B. DURING LOGIN:

The registered user should sign in before doing a secure fund transaction .The details entered by the user will be correlated with the details stored in the database. If all the details meet, then the mapping of the cipher individual typeset with the analogous numeric values will be performed via the server. The cryptogram parallel to the cipher entered by the user is found by recursive totaling. The set of metaphors equivalent to the cryptogram premeditated will be publicized to the user. The user ought to elect the identical two metaphors which were selected at some stage in the registration. The selected metaphors and the stored metaphors will be compared. If both match, then the user should select the identical pel in the metaphors which was selected during registration. Here, the comparison between the pel selected and the stored pel information will occur. If both match again, then the user will be authorized to do the fund transaction. Authentication is done by diagramed the User's password's letterings with the numbers.. For e.g. "ABCD" is the cipher entered by the user during registration. It is mapped to "1234" as same as Z Corresponds to the Numeric Value of 26. Let us contemplate the instance of "ABCDE" when all typescripts are added, it equals to "15". Finally 1+5= 6 this is corresponding to the alphabet "F". User will be choosing two metaphors in (F Section) from the given set of metaphors.

IV. MODULE DESCRIPTION

A. APK GENERATION:

Mobile Client is an Android application which is generated and mounted in the User's Android Mobile Phone so that user can accomplish the deeds. The Application's activity page comprises of the User registration Process. The User Login Page is fashioned by Button and Text Field Class in the Android. While creating the Android Application, Drag the tools like Button, Text field, and Radio Button to design the page. Once the page is designed, the codes for each page should be transcribed. Once the full mobile application is created, it will be generated as Android Platform Kit (APK) file. This APK file will be mounted in the User's Mobile Phone as an Application.

B. SECURE CORROBORATION FOR FUND TRANSACTION

- **Graphical Pattern Registration:**

There are utterly 26 alphabets present in English alphabet series. Any two digit numeral can start with a numeral 1-9. Server has by this time made set of images. Set of images will be assigned according to result of scheming.

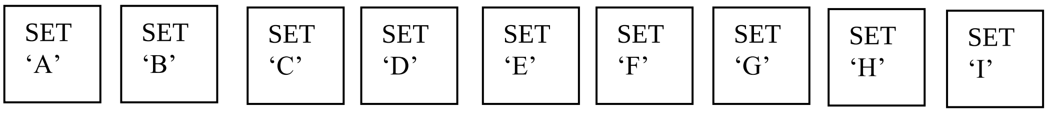


Fig. 3. Each set contains more than 100 metaphors

- **Calculation based Image Selection:**

In this comprehensive watchword is alienated in two sections. First is user selected secret code and second is the server provided sets of metaphors based on calculation. User has to select two imageries as the secret code. Both the textual keyword and the graphical secret word will forms the complete cipher.

Fig: 4. Metaphors based on computation

- **Graphical Pattern Detection:**

Image-based schemes use imageries which comprises of photo graphics, artificial pictures, or other kind of metaphors as background. Based on the number of phantasmagorias displayed, it is further divided into two subclasses. They are single-image schemes and multiple-image schemes. In the single-image scheme, user has to choice single image from the given set. In the multiple-image scheme, number of imageries will be provided to the user and they have to select more than one image.

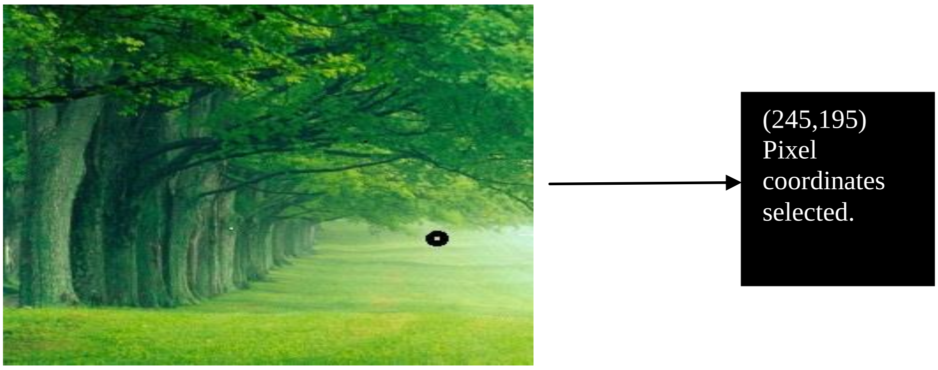


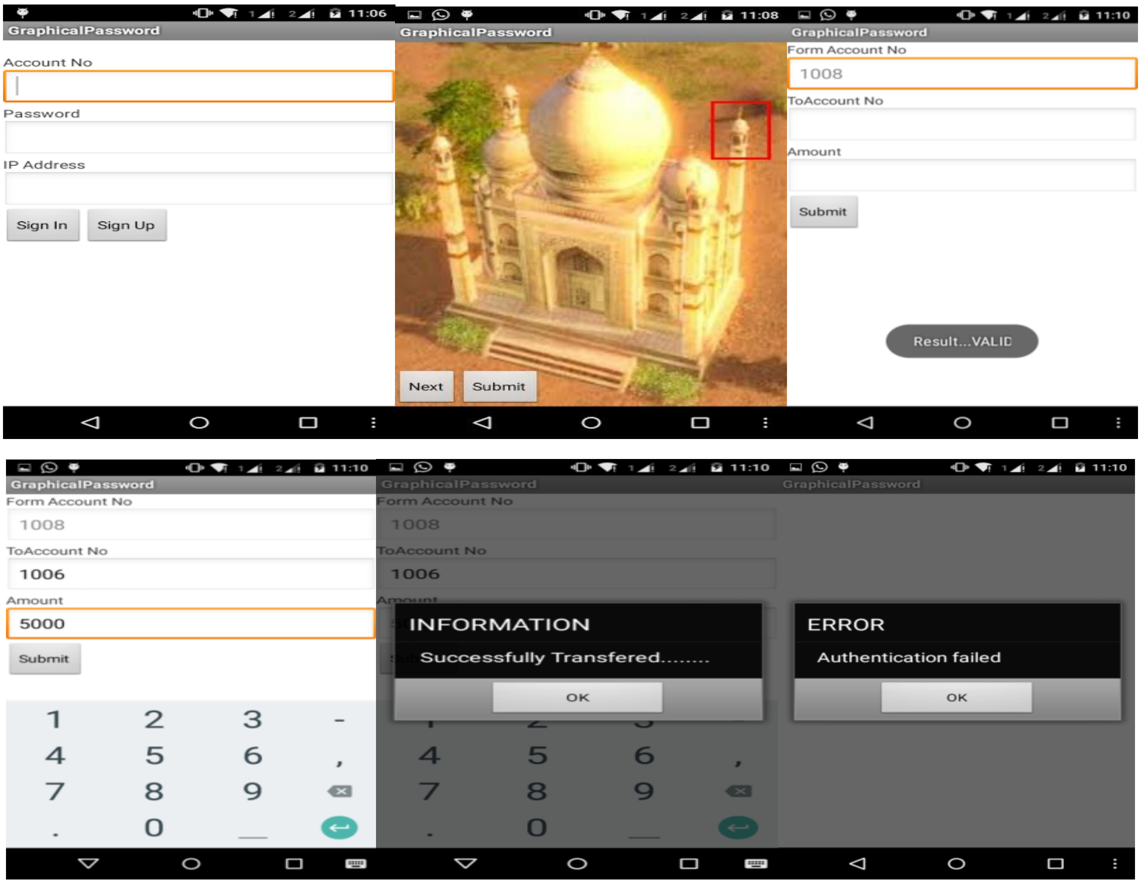
Fig.5. User selection

- **Validation:**

For accessing the services, user have to pass through authentication process. In the authentication, on the basis of encipher; process will be on track at the server-side. Set of imageries which will be provided to user are based on the upshot of calculation. If the cipher and image matches then the user is legal otherwise illegal.

V. IMPLEMENTATION

- Install the APK file in user mobile.
- Open the application.
- Clack sign up. Enter the minutiae and reminisce the IP address **172.245.132.132**.
- Click Submit. An image will be displayed.
- Drag and select some portion of the image and then click "SUBMIT" to endorse the selection and then "NEXT".
- Subsequent image will be exposed.
- Reprise the technique. If the user does not want to select anything in this image and then click “next” without clicking submit to skip the image.
- Once two images and its portions are selected, the user will be registered.
- A message will be shown as ‘Your Account No is “… ”’ and the user can use it for transaction.
- Click logout to exit the application.
- Now user ought to again enter the details and click sign in.
- The two images which the user selected during sign up will be displayed and the user has to select the identical slices of the images as before. Valid login will yield the funds transfer page and the transfer from field will be automatically filled with the user’s account number. Authentication failed error memorandum will be revealed for invalid user.
- Give the details. Initially while registering each account will have 100000 as balance. So the amount will be detected from the bal of account 1008 (from above screenshot) and credited to the account 1006.



Account No

Password

IP Address

Form Account No: 1008

ToAccount No

Amount

Result...VALID

Form Account No: 1008

ToAccount No: 1006

Amount: 5000

INFORMATION

Successfully Transfered........

ERROR

Authentication failed

Fig .6. Screen shots

VI. COMPARISON

[6]The graphical password is offering more protection to the internet services than the textual password. The table 2 shows the number of correct submission made by the users.

Table 2: Correct submission made by the users when using alphanumeric password and graphical password

Number of users	Alphanumeric password	Graphical password
5	3	4
10	7	10

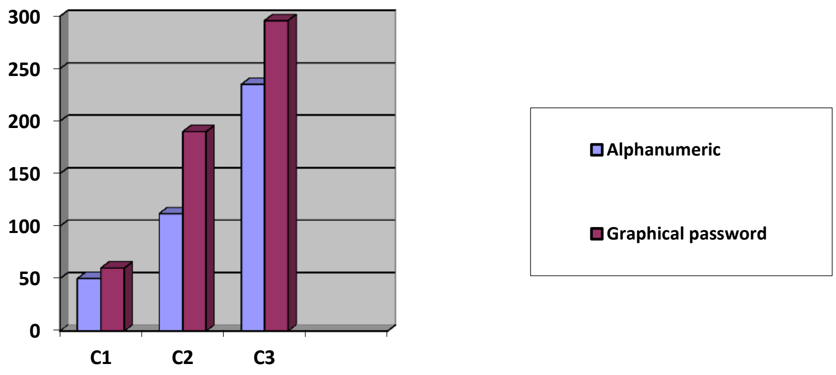


Fig .7. Chart compares alphanumeric and graphical password.

The chart represents the comparison between the alphanumeric password and graphical password. The x axes represent the number of correct submission made and y axes represent the number of users. It shows clearly that graphical password is more protective and easy for the user's remembrance. The textual password is predicted by various software and it does not need human interactions.[7] The graphical password needs human interactions.[8] Hence it prevents the access of unauthorized users.

VII. CONCLUSION

Thus Graphical Password authentication can be given by taking cloud as a platform. The new scheme solves the many problems of the existing stems like guessing attacks and shoulder surfacing attacks etc. It can also be useful for user in security point of view. Our future work is to make the application to be compatible with all types of operating system and to implement this with all types of operating systems and to implement this application for protecting all kinds of internet services.

REFERENCES

[1] Security Analysis of Graphical Passwords over the Alphanumeric Passwords by G.Agarwal,1Deptt.of Computer Science, IIET, Bareilly, India 2,3 Deptt. of Information Technology, IIET, Bareilly, India 27-11-2010.

[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] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceeding of 8th USENIX Security. Symposium, 1999.

[4] Captcha as graphical password- A new security primitive based on hard AI problems by Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu on IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014 891.

[5] Graphical password authentication in 2014 international conference on electronic system, signal processing and computer technologies.

[6] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. Journal of HCI, vol. 63, pp. 102–127, Jul. 2005.

[7] A Survey on Recognition-Based Graphical User Authentication Algorithm. Farnaz Towhidi Centre for Advanced Software Engineering, ((IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, December 4,2009 ISSN 1947-5500)

[8] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords"International Journal of Network Security, Vol.7, No.2, PP.273–292, Sept. 2008.

[9] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys(CSUR) journal, vol. 44, no. 4,Aug 2012,New York, USA.

[10] Authentication for Session Password Using Colour and Images by jai patel,SNJB's COE Computer Engineering Department, University Of Pune Ganeshkhind,Pune. (ICRTET) No 2, 2013.