Volume 2, Issue 4 April 2016 ISSN NO: 2454 - 7514

# North Asian International Research Journal Consortium

*North Asian International Research Journal*

*Of*

*Science, Engineering and Information Technology*

IRJIF IMPACT FACTOR: 3.01


# Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi, Urdu all research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

## Editorial Board



**Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,**
**Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com**

# "GRAPHICAL PASSWORD AUTHENTICATION USING CLOUD"

**ADITYA M. POKHARKAR[#1], KIRAN S. BHAJANAWALE [*2], SACHIN AALAM [#3]**
Department of Information Tech. NMIET, Talegaon, Pune. India

***Abstract* — *This paper represents an integrated evaluation of the Persuasive Cued Click-Points [1], [2] graphical password scheme, including usability and protection evaluations, and implementation considerations. An important usability goal for knowledge-based authentication application is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. We use motivation to influence user choice in click-based graphical passwords, encouraging users to select more random and different, and hence more difficult to guess click-points and password. There are 6 levels for lock. In that 1st level contain one image, 2nd contain two images and so on up to 6th level which contain 6 images each with different cued click point. User uses this level as per his security issue. User will select different images which he likes and select cued click points for each image, this data will save to phone as well as cloud also. The device will unlock only with correct cued points of each image. If the device get formatted then the images and cued click points data will be downloaded from cloud automatically. A possible strategy for increasing security is to enforce a minimum number of click-points, but allow users to choose the length and difficulty level of their password, similar to minimum text password lengths. The system would continue to show next images with each click, and users would determine at which point to stop clicking and press the login button. Although most users would likely choose the minimum number of click points, those concerned with security and confident about memorability could select a longer password. If some unauthorized person try to access the device then the device will capture the photo from front camera as well as send the location using GPS [4] to the email address of authorized person.***

***Keywords* — *authentication, graphical passwords, usable security, empirical Studies.***

## INTRODUCTION

The problems of knowledge-based security system, typically text-based passwords, are well known. Users often create memorable passwords security that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember and take more time to put. A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication systems allow user choice while influencing users towards stronger passwords and effective security. In our system, the task of creating weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path-of-least-resistance. Rather than increasing the burden on users, it is easier to follow the systems suggestions for a secure password a feature lacking in most schemes. Click-based authentication techniques include pass points, cued click points and persuasive cued click points. In pass point's method, users have to select click points on a single image. In Cued click point method, users can select click points up to n image i.e., in each level it takes a

single click point on a single image. In Persuasive cued click points (PCCP) [1],[2] it selects one click point on one image using persuasive technology. In the case of security, the click based graphical authentication suffered with hotspot and shoulder surfing problems.

## I. EXISTING METHODLOGY

### A. *Pin Lock.*

### B. *Pattern Lock*

### C. *Face Lock.*

### A. *Pin Lock.*

Pin Lock [5][6] is based on the 0-9 numbers. With these numbers with different combinations user can use it as a pin password. The correct pin will unlock the device.

### B. *Pattern Lock*

Pattern lock [5][6], is based on existing research on graphical passwords and requires the user to form a pattern on the screen by drawing lines in order to unlock the device. Its interface consists of 9 nodes in a 3x3 grid formation. Users start by touching one of the dots to make it the start point and swipe their fingers to add dots and form a pattern.

### C. *Face Lock.*

It uses face [5] [6] detecting software and front camera of the device to unlock the phone or the device. It uses the grid layout to detect the face shape and match it to the original one to unlock.

## II. SCOPE

Android application using drop-box API to upload and download Images to set password, password set activity using Image X-Y Coordinates Use this lock for any particular application installed on mobile. Unlock the application by choosing correct coordinates from random images

## III. MOTIVATION

Present locking [5] [6]systems are not so secure in now a days due to common pin, patterns, and characters. Face lock is not working well in low light areas. Also if device get formatted then unauthorized user can easily misuses the data. Therefore it is need to develop new locking system that provide more security to smart phones. The new system will provide well locking system while device is in use and with the help of cloud also provide security when it get formatted. It also help to track the location of phone

## IV. ISSUES IN EXISTING SYSTEM

1. Pin Lock:- For easy to remember the pin users uses the phone number, birth date or car/ bike number as a pin, due to this the pin does not remain as a secret. And if user put hard and long pin as a password then it may get happen the user get forget it very easily.
2. Pattern Lock: - The Patterns gets very common most of users have same pattern for their smart phones so anyone can easily access and misuses the personal data.

3. Face Lock:-Unable to detect the face of person in low light also it gets unlocked by people having same face structure.

## V. PROPOSED SYSTEM

Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information In Pass Points, passwords consist of a sequence of

five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks points in the correct order from cloud, within a system-defined tolerance square of the original click-points. We are also preventing shoulder attack by using random number generation method. We are also adding the GPS [4] [6] co-ordinates of the images with it. This provides the cloud authentication to user.

## VI. BENEFITS OF PROPOSED SYSTEM

1) Not easy to copy password.
2) Different levels of lock
3) Use of cloud.
4) Image computing.
5) GPS Based tracking.

## VII. RELATED WORK

### *1. Detection of Cued Points*

The Detection of exact cued click point by user is not possible every time so it will track the user by using + -35 x and + - y coordinates ratio near from cued click points.

### *2. GPS*

GPS stands for Global Positioning System. [4] Global Positioning System (GPS) is networks of satellites that continuously transmit coded information, which makes it possible to correct identify locations on earth by measuring distance from the satellites. The purpose of using GPS module in the system is, it continuously transmits serial data like position of an individual wearing sensor, in terms of latitude and longitude, date, time and speed values to processing unit.

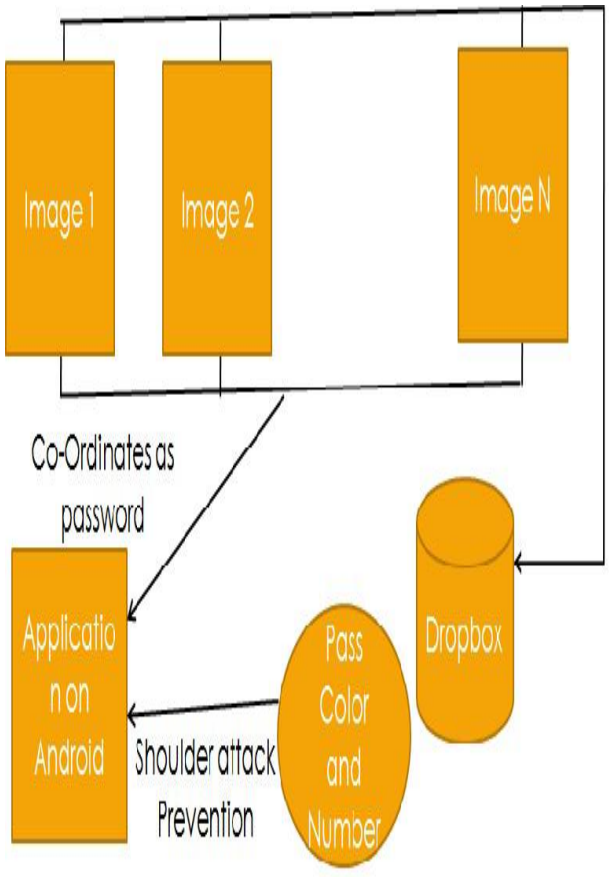
### *3. Use of Cloud*

The use of cloud [3] is main feature of this system. In the case of device lost the cloud will detect the device with the help of IMEI number and install the security mechanism on device automatically.

### *4. Capturing the Image*

In the case of device lost if unauthorized try to unlock the locking system and he/she uses all chances then the image get capture by the camera of the device and send it to the authorized user's mail-id.

## VIII. METHODOLOGY



## IX. SYSTEM ARCHITECTURE

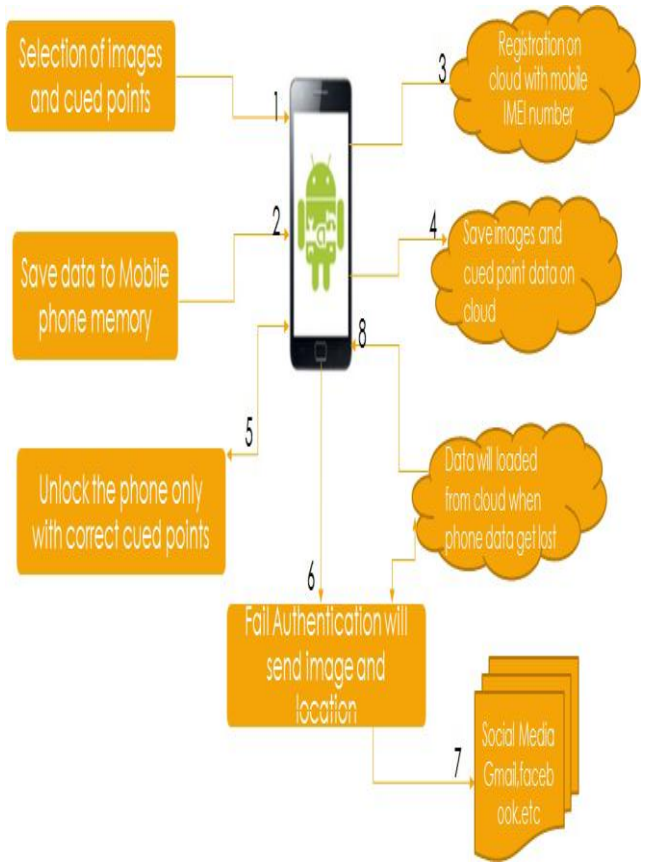



**Fig 2: System Architecture.**

## X. CONCLUSION

We have shown that it is possible to allow user choice while still increasing the effective password space. Furthermore, tools such as PCCPs [1][2] viewport (used during password creation) cannot be exploited during an attack. Users could be further deterred (at some cost in usability) from selecting obvious click-points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport with every shuffle past a certain threshold. The approaches discussed in this paper present a middle-ground between insecure but memorable user-chosen passwords and secure system-generated random passwords that are difficult to remember. A common security goal in password-based authentication systems is to maximize the effective password space. This impacts usability when user choice is involved

## ACKNOWLEDGMENT

Each project big or small is successful largely due to the effort of a numerous wonderful people who have always given their precious advice or lent a helping hand. I sincerely appreciate the inspiration; support and guidance of all those people who have been instrumental in making this project a success.

We would also like to thank all the faculty members of NMIET for their critical advice and guidance without which this project would not have been possible.

## REFERENCES

[1] S. Chiasson, C. Deschamps, M. Hlywa, G. Chan, E. Stobert,and R. Biddle, MVP: A web-based framework for user studiesin authentication (poster), in Symposium on Usable Privacy and Security (SOUPS), 2010.

[2] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van" Oorschot, Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," School of Computer Science, Carleton University,

[3] Shraddha M. Gurav and Leena S. Gawade Computer Department Mumbai University, RMCET.

"Graphical Password Authentication Cloud securing scheme."

[4] S. Manoharan Department Of Computer. sci, university , Auckland. "On GPS Tracking of Mobile Device. april 2009."

[5] Kwang II Shin and JI Soo Park Department of Computer sci and technology And engineering Seoul National University Of Science And Technology, Seoul korea. "Design And Implementation of Improve Authentication System for Android Smart Phone User"

[6] Android Security Overview, Android open source projec http://s ource.android.com/ tech/security/index.html

# Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

**Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301 Jammu & Kashmir, India**
**Cell: 09086405302, 09906662570,**
**Ph No: 01933212815**
**Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com**
**Website: www.nairjc.com**