iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4160

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Graphical Password Authentication System for Mobile Application

Prof. Ms. Jagruti Wagh[1], Neha Kshirsagar[2], Ms. Janhavi Mahadik[3], Ms. Samiksha Mahalle[4], Ms. Maheshwari Pachpute[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*Student, Marathwada Mitra Mandal's College of Engineering ,Pune*

Abstract: ***Smart mobiles are essential devices in our life today. Various Applications on the device can be accessed with it. Moreover, if the mobile device is unlocked, it is also easy for sophisticated attackers to steal the owners sensitive information, such as identity, account and phone calls to overcome from this drawback we are giving security for android application using graphical password. In this paper we are representing graphical security to mobile applications by giving grid of images which are changing randomly at every login phase. Not only added the random graphic pattern authentication method indeed increase the personal secret information being stolen difficulty and complexity, it provides more security level than the traditional graphic pattern authentication in keypad lock screen as well.***

I. INTRODUCTION

Nowadays mobile devices has became a part of our lives. We can store our important data on mobile application but if security is not provided to mobile devices the attackers can easily access our important confidential data, so to avoid this, authentication using graphical password plays a very important role. There are various techniques of authentication such as textual, graphical, bimetric, inter operation but textual passwords are easy to guess for attackers and if complex password is set, the user can forget it whereas biometric is very expensive to apply. So graphical password system is invented for authentication. It is easy to remember as human can remember images or pictures more easily than text. And hence they are not easily guessable to hackers. Authentication is a binding of an identity to a subject and a graphical password is an authentication system that works by having the user to select from grid of images in a specific sequence. The rest of paper is organized as follows in Section II there is information about current techniques of graphical password authentication. Section III includes proposed work and GUI. Section IV contain comparison with other methods and finally section V contains conclusion and then references.

II. RELATED WORK

A. Recognition Scheme

In recognition technique set of images is provided and the user select images sequentially as he choose during registration.
Algorithms which uses Recognition based technique for example

1) Dhamija and Perrig technique: In this user has to pick pictures from set of pictures and have to identify those sequentially.
2) WIW scheme: In this technique has introduced several varients for each pass object and each varient is assigned with a unique code. During authentication user has to recognise preselected images along with alphanumeric code.
3) Triangle scheme technique: Here during authentication user has to select preselected icons & has to click inside convex hull bounded by pass-objects.

B. Recall Based Scheme

In recall based scheme there are two techniques I) Pure recall II) cude recall

1) Pure Recall Technique: In pure recall based authentication system, user has to reproduce or draw something as their password without producing any hint at the time of Registration phase. There are some algorithms based on pure recall based technique as follows

a) *Passdoodle:* In this , user has to draw hand written designs or text on a stylus sensitive touch screen When login to the system, user has to draw the same pass doodle which was already drawn at the registration phase.

b) *Draw A Secret (DAS):* In this,User has to draw password on a two dimensional grid touches on a stylus sensitive touch screen. When the user is available to login to the system, user has to draw the same shape and also strokes that touch on the grid must be the same which has been already drawn at the registration phase, then the user is authenticated.

c) *Qualitative DAS (QDAS):* it is an enhancement of DAS method created by encoding each stroke.

d) *Syukri Algorithm:* This technique involves two stages namely, registration and verification. In the registration stage, user is

asked to draw a signature using mouse and the system extract signature either by enlarge or scale down the signature and rotates if needed. This information stored in the database.

C. Cude Recall Technique

In cude recall based authentication system, user has to reproduce or draw something as their password with producing any hint at the time of Registration phase.There are some algorithms based on cude recall based technique as follows

1) *Blonder:* Pre-determined image is presented to the user on a visual display and then the user is supposed to tap regions by pointing to one or more predefined locations on the image.
2) *Pass Point:* In this case the image could be any natural picture or painting as well as rich enough so as to have several possible click points.

D. Image Sequence Scheme

In this technique the user uploads desired images from personal di-rectory. Advantage of this methodology is that, images uploaded from personal directory are easily memorized and these images are not visible to other users. These images are only visible to authorized user.

Sequence of images is stored in database. At the time of login user selects uploaded images in same sequence as the sequence of images was selected during registration phase. If sequence of selected images is incorrect then user will unable to login.Some types of methods used in this are

1) Image pass
2) face pass

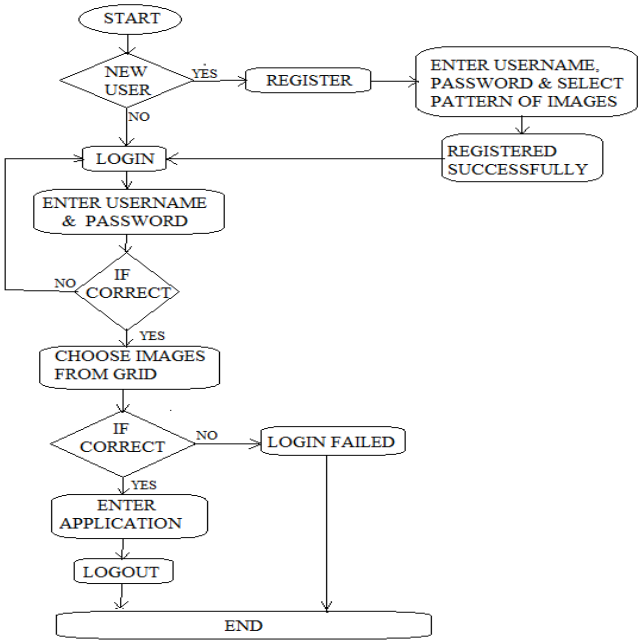
III. PROPOSED WORK AND TOOL

A. Registration Phase

When one starts the application,they will be provided options i.e login and Registration,if it is registration user has to complete the registration phase which includes username, password ,email id, mobile number as shown in figure 2. After registration user has to select password using images.

B. Login Phase

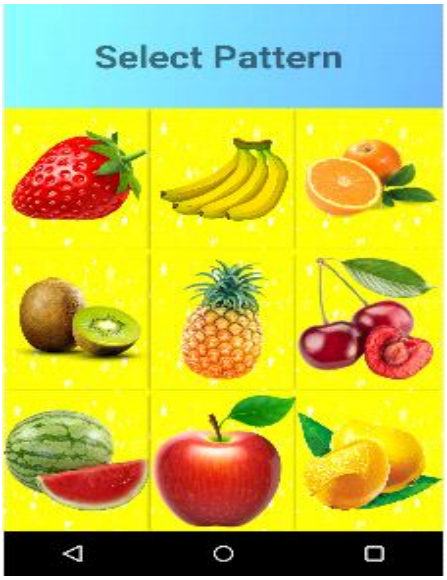
During login phase user has enter username and password he entered at login time. After verication he will be provided with grid of 3*3 images then user has to select correct password sequentially as he selected in registration phase but the images will shuffle every time of login. After entering password system will check and if password is correct then user will enter in application.



1) Activity Diagram

2 .Registration form

3. Login



4. Select Images sequentially

IV. COMPARISON WITH OTHER TECHNIQUES

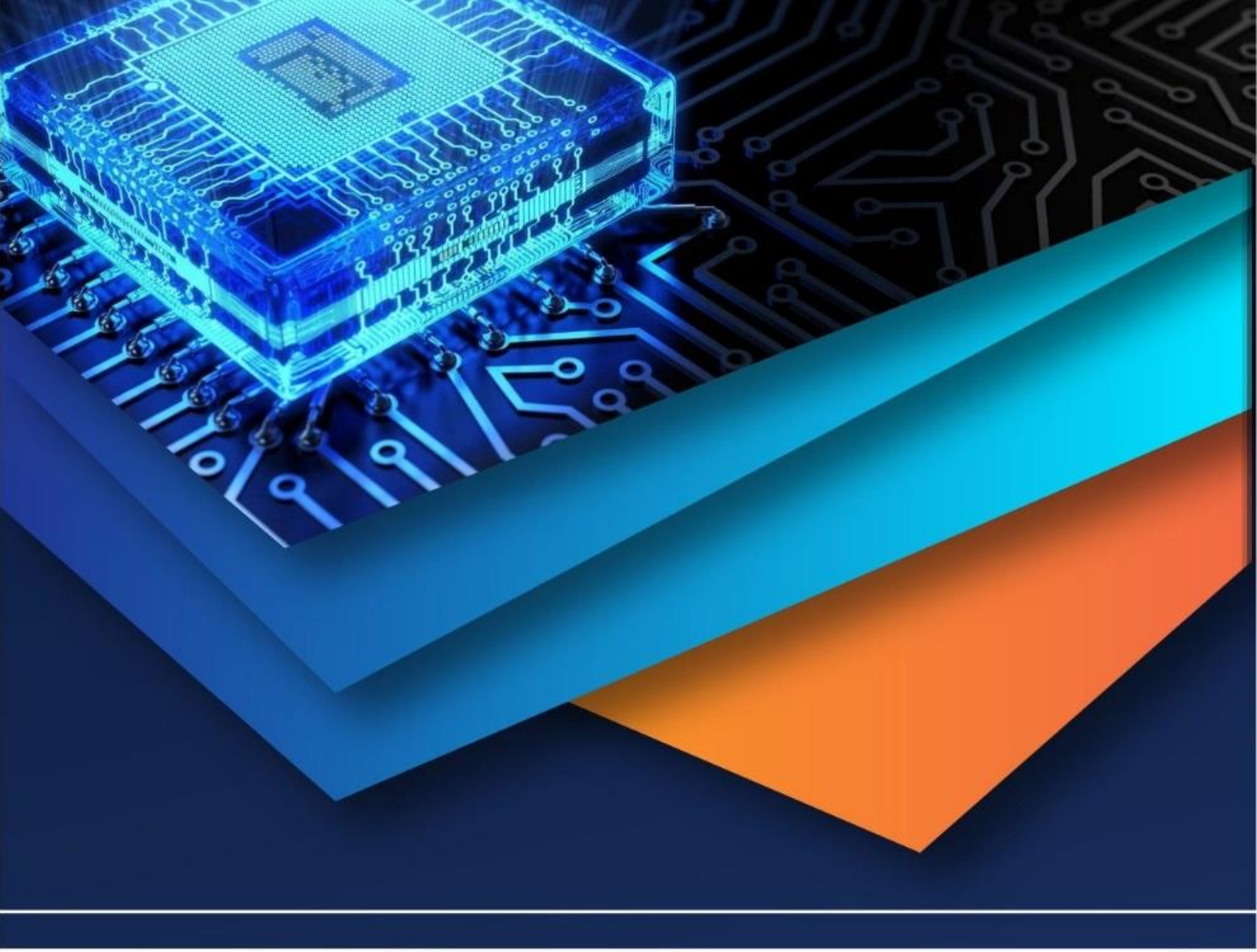
A. Using this technique problem of sholder surfing can be avoided because in this technique the images shuffle at each login time, whereas in other techniques there can be be proble of sholder surfing.

B. Here in this technique it is easy to remember password as it is image based. And human can remember images easily. Whereas in texual method user can forget the hard password set by him.

C. It is not costly because it doesn't incluse any extra sensors otherthan touch screen.

REFERENCES

[1] "Design and Analysis of a Graphical Password Scheme" Haichang Gao,Xiyang Liu,Sidong Wang and Honggang Liu,2009.
[2] "A Graphical Password Authentication System", Ahmad Almulhem,2011.
[3] "Graphical Password: Pass-Images Edge Detection",Housam Khalifa Bashier, Lau Siong Hoe , Pang Ying Han,2013.
[4] "Graphical Password Authentication",ShraddhaGurav,Lina Gawade,Prathamey Rane,Nilesh Khochare,2014.
[5] "Graphical Password-Based User Authentication With Free-Form Doodles",Marcos Martinez-Diaz, Julian Fierrez, and Javier Galbally,2015.
[6] "Enhancement of Password Authentication System Using Graphical Images"Amol bhand, Vaibhav desale, Swati shirke, Suvarna pansambal shirke,2016.
[7] "Graphical Password Authentication Cloud securing scheme",ShraddhaM. Gurav, Leena gawade , prathamey rane, Nilesh khochare,2014.
[8] "Introduction to computer securityS",Matt Bishop,Sathyanarayana S.Venkatramanayya, Pearson Education.
[9] "Pattern Recognition and imagr analysis", Earl gose, Richard johnsonbaugh, Steve jost,Easton Economy Edition.
[10] "Random Graphic User Password Authentication Scheme in Mobile Devices"Sung-Shiou Shen, Tsai-Hua Kang, Shen-Ho Lin, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY