ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

Graphical Password Strategy

[1] Veeramani Ramasamy, [2] Ambica Gupta, [3] Aakriti Rai
[1] M.E., Assistant Professor of Department of Information Technology, SRM University, Ramapuram, Chennai
[2] [3] Third Year Students Department of Information Technology, SRM University, Ramapuram, Chennai

Abstract;- **This paper is based on graphical password to protect user data or unauthorized access of information. The pattern are some set of graphical images which randomly changes its position every time you try to login. The user has to provide his details for registration and then has to draw a pattern as a password. The user has to select an application while registration itself and can have multiple accounts for every single application. The pattern is a 4X4 Grid consisting of multiple graphical images, the user has to drag or draw at least over 4 images for the application to consider his pattern lock. The Application auto generates a Unique Id for every User who wants to register. After the user has successfully registered he is redirected to the Login page where he has to provide his Id and Pattern Password from which the selected application by the user during the registration opens up.**

Keywords;- **Graphical password, Graphical images, 4x4 Grid pattern.**

I. INTRODUCTION

Password have been widely used to authenticate users to remote servers in web and other applications. Text passwords have been used for a long time. Graphical passwords, introduced by Blonder in 1996, are an alternative to text passwords. In a graphical password, a user interacts with one or more images to create or enter a password. Graphical passwords are intended to capitalize on the promise of better memorability and improved security against guessing attacks. Graphical passwords are particularly suitable for keyboard less devices such as Android and iPhones where on in putting a text password is cumbersome. For example, Windows 8 recently released by Microsoft supports graphical password logon. With increasingly popularity of Smart phones and slate computers, we expect to see a wider deployment of graphical passwords in Web applications. The project allows user to input a pattern password and only user knows how the pattern looks like as a whole. On matching the pattern, system unlock the security and opens up the specified application. Every time user logs on to the system the pattern password randomly changes its position. Now, if user chooses the correct pattern to make the original pattern, the system authenticates and allows to access the application. Else the user is not granted access.

.

II. MODULES AND THEIR DESCRIPTION

This application comprises of four Modules:

1. Registration: User first need to register into the system simply by filling up the details such as Name, Email id and Phone number.

2. Pattern Lock: After filling up the details, user can now set a pattern of his/her choice for security purpose.
3. Login: After successful registration, user can now login into the system by matching up the pattern.
4. Application Access: If the security pattern is matched, system grants the access to use the specified application.

III EXISTING SYSTEM AND PROPOSED SYSTEM

Problem with current scenario

Some two persons proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the pre-selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

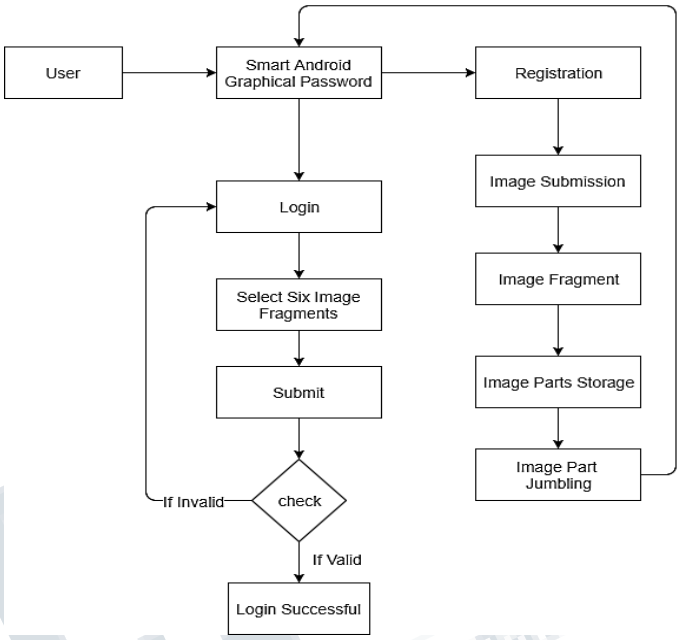
traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious.

Other two persons developed a graphical password technique that deals with the shoulder-surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess, both suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.

Proposed System:

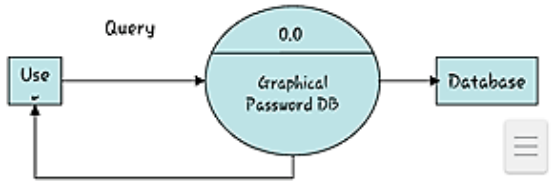
Graphical password application allows the user to set a pattern password for using other applications. The patterns are some set of graphical images which randomly change its position every time you try to login. The user has to provide his/her details for registration and then has to draw a pattern as a password by drawing it twice. The user has to select an application while registration itself and can have multiple accounts for every single application. The pattern is a 4x4 grid consisting of graphical images, the user has to drag or draw at least over 4 images for the application to consider his/her pattern lock. The Application autogenerates a Unique Id for every User who wants to register. After the user has successfully register he is redirected to the Login page where he/she has to provide his/her Id and Pattern Password and the application selected by the user during the registration opens up.

IV. SYSTEM ARCHITECTURE



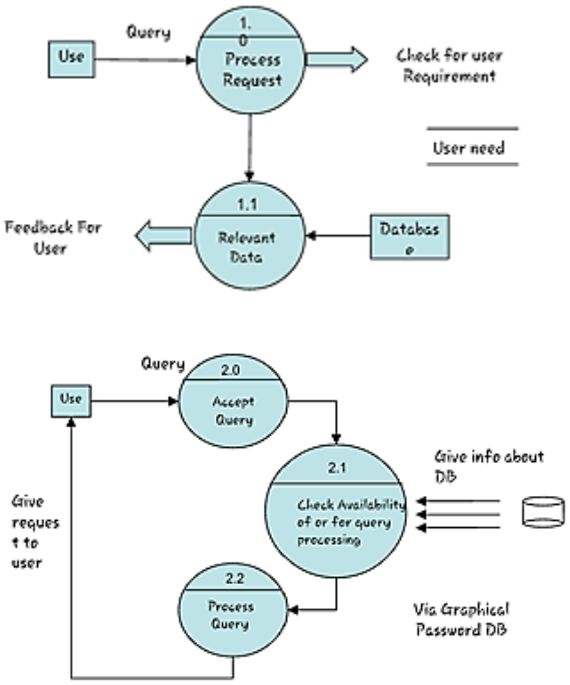
V. DATA FLOW DIAGRAMS

A data flow diagram is a graphical tool used to describe an analyzed movement of data through a system. These are the central tool the bases from which the other components are developed. The transformation of data input to output through processed, may be described logically and independently of physical components associated with the system. These are known as the Logical data flow diagrams. A full description of a system actually consists of a set of data flow diagrams.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017



VI. CONCLUSION AND FUTURE WORK

The main aim of developing this application is to secure every smart phone device from external threads which we never know when they accessed our smartphone read or share our private data, messages, images, etc. as the doesn't have any locking facility from snooping.
This application secure all your personal files, data, etc. once the device is locked using this security application.

REFERENCES

[1] en.wikipedia.org

[2] Dr. Mcchester Odoh And Dr. Ihedigbo Chinedum E. Implementing 3D Graphical Password Schemes. e-ISSN :2278-2834,p-ISSN:2278-8735.Volume 9,Issue 6, Ver.II (Nov-Dec.2014),PP 09-17

[3] Yuxin Meng. DESIGNING Click-Draw Based Graphical Password Scheme for Better Authentication.2012 IEEE Seventh International Conference on Networking, Architecture, and Storage.