International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)

ISSN: 2456-236X

Vol. **04** Issue **02** |**2020**

Random Graphical Patterns To Avoid Shoulder Surfing

Anjana Menon R[1], Dinesh Soni[2]

[1,2] *Master Student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India*

ABSTRACT

The project entitled "Random Graphical Patterns to Avoid Shoulder Surfing" is explaining a graphical pattern/password strategy. Since lineal or normal password strategyisunsafe to shoulder surfing, many shoulder surfing strategiesagainst graphical password have been introduced. The project involves a single user module. The user should register a pattern for unlocking the desired application. The pattern is a collection of fruit images in a 4x4 grid. The position of fruits changes randomly in every login. The user can unlock the application by selecting the fruit pictures from different locations in a particular sequence so that he can build the unlock pattern. Graphical passwords can be efficiently used in any android device to provide better security and memorability.

Keyword: - Shoulder Surfing, Graphical Password, Random Pattern, Android, Security, Memorability.

1. INTRODUCTION

In the information security domain, Shoulder Surfing is similar to social engineering activity in which a person is trying to get information such as sensitive information, passwords, personal identification numbers (PINs) and other credentials by looking over the victim's shoulder. Through this project, we are making an effort to avoid this kind of attacks by making use of this application.

Text passwords have been widely used to authenticate users to remote servers in the Web and another kind of applications. Graphical passwords are an alternative to text passwords. Here, a graphical pattern password is used. A user interacts with one or more images (here we are using images of fruits) to create a password. Graphical passwords provide better memorability and improved security against guessing and shoulder surfing attacks.

The project allows user to set a pattern lock for specified applications and the only user knows how the pattern looks like as a whole. Every time user logs in, the fruit picture's position changes and the pattern should be entered correctly by choosing the fruit pictures in the correct order. Now, the system allows accessing the application. Otherwise, the user is not granted access.

2. STATEMENT OF PROBLEM

The problem statement of this project would be to create a graphical password or a pattern lock that is resistant to shoulder surfing – a kind of social engineering attack.

3. SIGNIFICANCE

With the increasing popularity of keyboard-less devices like smartphones, security is also a concern. In such devices, pattern locks are already common. Patterns are most prone to shoulder surfing and it can be revealed through the smudges on the screen. Here comes the significance of this project. This android application makes use of a graphical pattern/password which can be used effectively without worrying about such kind of attacks.

4. REQUIREMENT SPECIFICATION

Requirements Specifications specifies the usage of both Hardware and Software with their corresponding versions, modules etc., which are necessary for the overall outcome of the project.

Hardware specifications include:

- i3 Processor-Based Computer
- 1GB - Ram
- 5 GB Hard Disk
- Android Device

Software specifications include:

- Windows 10
- Android Studio [4]
- SQL Server 2008 [5]

5. PROPOSED SYSTEM

- Graphical Password application allows the user to set a pattern password for using other applications.
- The pattern is some set of fruits which randomly change its position every time you try to login.
- The user has to providethe details and draw a pattern twice for registration.
- The user has to select an application during registration itself.
- The pattern is a 4X4 Grid consisting of Fruits, the user has to drag or draw at least over 4 fruits 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 and the application selected by the user during the registration opens up.

6. MODULES

A single User Module comprises of 4components:

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

Pattern Lock: After filling up the details, the user can now set a pattern of his/her choice for security purpose.

Login: After successful registration, the user can now login into the system by matching up the pattern.

Application Access: If the security pattern is matched, the system grants access to use the specified application.

7. ACTIVITY DIAGRAM

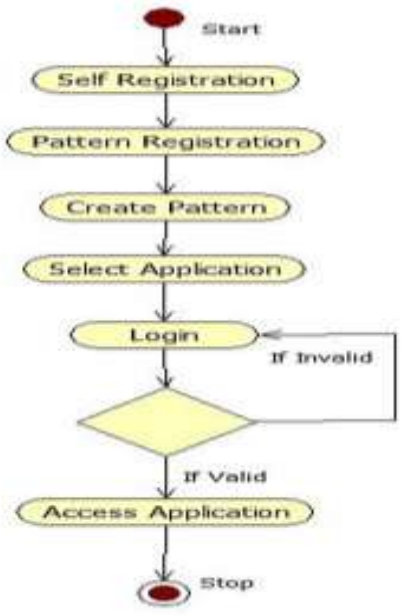

Fig – 2: Activity Diagram

In figure 2, the first process is starting the application. Then register with own details such as Name, E-mail Id and Mobile number. With these details, we need to select a particular application by clicking the radio button, which we want to secure. After this, the pattern registration page will be displayed. In this page, we need to draw a new pattern twice and click on the submit button. Now, we go to the login page again and enter the Unique Id, which generated at the time of sign up. If the entered Id and registered pattern will be matched, then we can access the application otherwise we can't.

8. FUTURE ENHANCEMENTS

In this application, we can notice an option 'credit'. As a future enhancement, we are looking forward to including a vault inside this option. It could be used as a safe folder in which we can store images, videos, voice notes, documents and also folders as a whole. So basically, this application can replace various vaults and app locks as it incorporates both app lock and secret vault.

We are also putting forward an idea to use this graphical password strategy in web applications also in order to improve memorability and also to avoid shoulder surfing.

9. CONCLUSION

To conclude, Mini-Project "Random Graphical Patterns to Avoid Shoulder Surfing" which has been developed to physically secure every smartphone device from external threats which we never know when people can access our smartphone, read or share our private data, messages, images, etc. The project introduced a position interchanging graphical pattern/password for secured locking of the desired application. All your personal files, data, etc. will be secured once the device is locked using this security application.

10. ACKNOWLEDGEMENT

Weare sincerely thankful to Jain University for providing me with the opportunity to write a research paper on this topic. We are also thankful to Mr Subarna Panda, Assistant Professor and Dr Lakshmi JVN, Associate Professor for guiding me in every single stage of this research paper and supporting throughout the process in preparing a meaningful paper. We are also thankful to Dr.N.MNachappa (Head of School-CS& IT) of Jain (Deemed-to-be University) who have helped me during the course of this research paper in different ways. Through this paper, we have learnt how the vulnerability pattern of password works and camouflage patterns usability.

11. REFERENCES

[1].Microsoft Developer Network (MSDN): http://msdn2.microsoft.com/en-us/default.aspxThis is a valuable online resource and is a must for any developer using Microsoft tools.
[2].https://code.tutsplus.com/tutorials/learn-java-for-android-development-introduction-to-java--mobile-2604
[3].https://www.javatpoint.com/android-tutorial
[4].https://www.androidauthority.com/android-studio-tutorial-beginners-637572/
[5].https://androidforums.com/threads/connect-android-to-remote-SQL-server-2008.866466/