ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Three Step Authentication Technique To Safeguard The Data Present In An Android Device.

Ritesh Kumar, Deb Jyothi, and Revathy S*.

Sathyabama University, Chennai, Tamil Nadu,India

ABSTRACT

In today's world, with the rise in technology, data security has become a rising issue. With the most conventional way of password authentication in android devices, shoulder surfing and other hacking techniques has become vulnerable. Also, the introduction of biometric fingerprint as well as the high complexity of these techniques, these are not yet popular in the mass. So, we propose in this paper, three step authentication technique that can be used as a step by step verification to access data in android devices. In this technique we have used the combination of three common data types that a human being access and can remember in an easy manner. They are Images, Text, and Colors.

Keywords: authentication, safeguard, data.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

With the rise of the usage of mobile devices, number of mobile manufacture came into existence to unleash their technologies to the world. Among these, Android is the most used and popular platform to the masses. So it is quite normal for the people to store their personalized data in these devices. But these rise of android devices has also lead to the rise of hacking techniques to manipulate the data present in these devices without an authorized access.

Data security is the main motive of this paper. With the rise in the vulnerability of personalized data security in the android devices, it is essential to build a new systematic authentication scheme which can safeguard the device from unwanted access. Although, fingerprint scanners and iris recognition scanners has been introduced in few devices, but due to the high complexity and hardware problems faced with these techniques, these are still in a modifying stage.

In this paper, we are trying to build a new technique of authentication for android devices. This is a three step authentication method in which we have planned to use the combination of images, text and colors. User need to select a specific image, text and color codes during the registration phase. According to the user's input during the registration phase, he need to select the correct image from a grid of image in the first step, in the second step, the correct textual password need to be entered from a grid of text and in the third step, the specified color codes need to be entered. Only after all the three steps gets authenticated, the user will be allowed to access the device.

RELATED WORK

Some of the works are discussed in this section. Many commonly used techniques to lock an android device have been initiated till date. The default system provided in every smartphone is to slide the home screen to open the device. It cannot be considered as a security mechanism as the user need not have to authenticate the device singularity in these techniques [1].

Pattern, pin and password locks are the most commonly used authentication technique used by users in recent times. User should either create a numeric pin or a pattern or an alphanumeric password during the registration. And during the unlocking of the device, the same should be replicated in the locked screen to unlock the device [1].

With recent growing of biometric authentication system, fingerprint as well as iris recognition scanner has been tried to be implemented in many android devices. But with the high complexity faced and hardware delays leads to a negative impact of this technique to the user [1].

In reference to SwapnilWaghmare, MadhumitaChatterjee and Satish L Varma's paper on "Authentication System for Android Smartphones", a new technique is introduced as a registration and login phase. In the registration phase, the user need to provide with the user details such as mobile number, email id along with a secured password. In the login phase, that is when the user tries to authenticate the device for data access, he needs to type the password previously registered during the registration phase. The user will get three chances to verify, after that a random number will be send to the user's mobile number or email id using which he can access the device and change the password. If he fails to verify the random number as well, within three attempt, the data stored in the device gets backed up to the phone's memory and if the internet is accessible, then the backed up data will be sent to the registered email id. This technique is proposed with the idea to save the data from unauthorized access [2]. But usage of only textual password is too vulnerable for shoulder surfing [2].

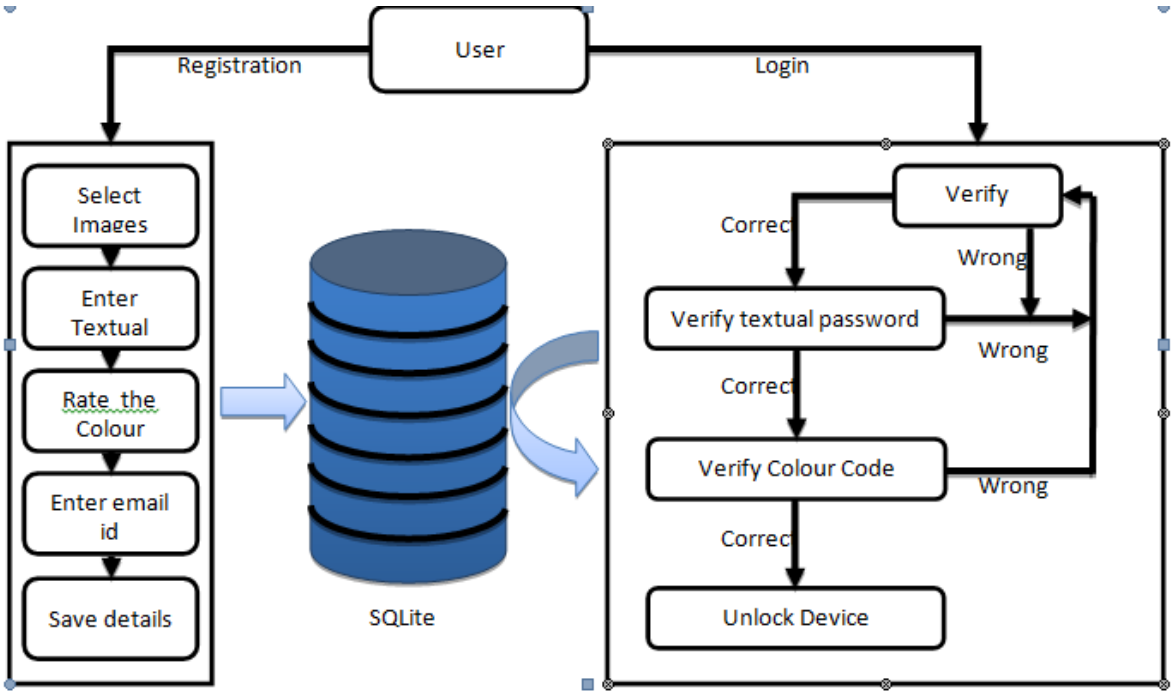
In reference to PulkitTandon and Geogen George based paper on "Next Level User Authentication in Android", a multi-step authentication technique is proposed. In this, a series of techniques starting from voice speech recognition, pattern based, pixel identification technique are tied together to form a strong and secured authentication. It was a complete new idea but with complication, as both the voice and pixel identification techniques are based on hardware which can malfunction and lead to dissatisfactory result [3].

ISSN: 0975-8585

In reference to M. Sreelatha, M. Shashi, M. Anirudh, MD. Sultan Ahamerand V. Manoj Kumar based paper on "Authentication schemes for session using color and images", a new session based authentication technique was introduced which combines the images, text and color. But this method was implemented in a web based service [4]. In the registration phase, the user is asked to select an image, a textual password and color codes for some particular sets of color. In the login phase, firstly a grid of images is displayed among which the user needs to select the preselected image of the registration phase. Once the user selects the correct image, the next authentication step gets displayed, that is a grid of alphanumeric characters. In the grid, the user needs to select the alphabets of the password which is provided during the registration phase. If the password selected via the grid is correct, then a band of few colors will be displayed. In this, we need to type the color codes of the specified color. If all the three steps get authenticated correctly, then the web service is allowed to access in it [4].

Proposed Work:

Architecture:



Workflow diagram

The above diagram shows the architecture of the proposed technique and its workflow of how the user can first register his personalized password and then how he can unlock it.

Registration Phase:

In the registration phase, the user need to select a particular images which will act as the key image to unlock the first step of verification in the unlocking process. This image can be selected from a set of images provided in the registration phase.

Secondly, a textual password must be provided by the user which will be the second authentication key in the login process. This password can be any 4 digit password including any alphanumeric character excluding any symbols.

Thirdly, a set of color will be provided to the user. User have to rate the color with their own choice in the range of 0-9. This part is connected to the last step of verification where a set of color will be provided to the user and the user have to specify the correct color code based on the rating they provided during

registration phase. An email id needs to be given by the user mandatorily. In case if the user forgets the password, a n email to change the password and unlock the device can be forwarded to it.

All the details provided by the user in this phase are stored in the SQLite database and can be retrieved back from it during the unlocking/login phase.

Login/Unlocking Phase:

In the login phase, when the user will try to access the device, he will come across a three step verification process. Firstly an image grid of a set of images, secondly a text grid of all the alphanumeric character and in the last step, a collection of color blocks.

In the first step, a collection of images is displayed to the user. Among the images displayed, one image will be present which has been selected by the user during the registration phase. If the user selects that particular key image, he will directed to the next step of verification or else the user will be asked to select the correct image to access the device.

Once the user gets through to the second step, he will displayed with a grid of 6*6 matrixes containing all the alpha numeric character starting from A to Z and 0-9. In this step, the user needs to type the textual password he has specified during the registration phase using the grid. The grid will have a randomized display of characters. If the user fails to insert the correct password, he will be redirected to first step of verification, which is the image grid. Else the user is passed to the next and the last step.

In the last step, the user will be provided with a series of 3 color blocks with each having a textbox beneath it. During the registration phase, the user has rated a set of color with random codes for each color. Based on that coding, the specified color displayed now need to be rated correctly, only then the user will be granted access to the device. If failed, the user will be redirected to the first step of this login.

Also the user is provided with a forgot password option, which will send a link to the user's email to change the password.

Implementation:

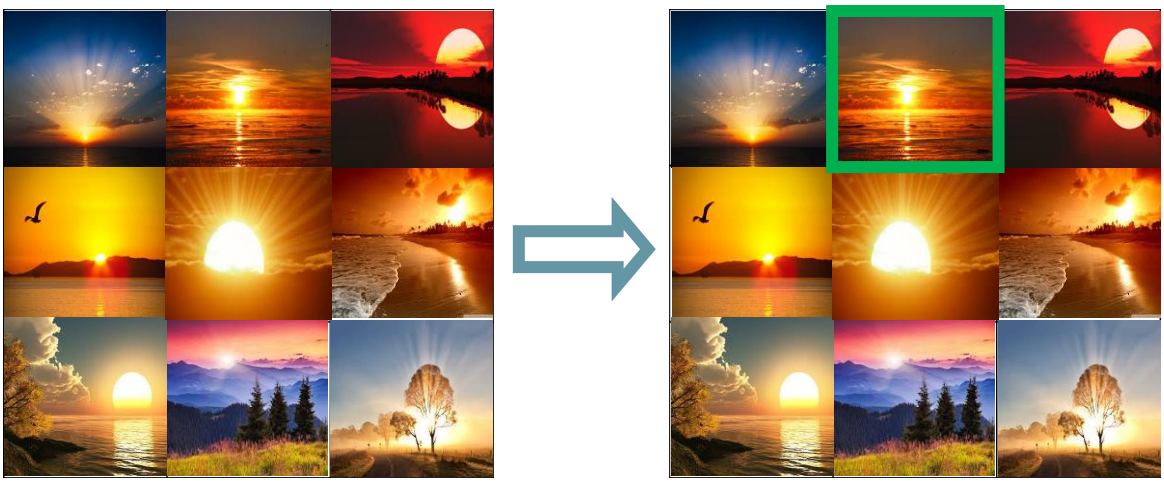
Image verification:

In this, we have taken image button for each of the images present during the registration phase. Each image button has been set with some integer values. When the user selects a image during the registration phase, the integer value corresponding to the image get stored in a verification variable. During login phase, when the user selects any image, the integer value of that image gets crosschecked with the verification variable. If it matches with it, then the next step gets redirected or else the user is asked to select the correct image.

Text verification:

In this step, grid of 6*6 matrices of alphanumeric numbers is taken as buttons. Each characters can be represented using its ASCII value. During the registration phase, the 4 digits of the textual password is converted to their respective ASCII values and added. This added value is then stored in a verification variable. In the login phase, when the user presses the button of each of the textual password, the sum of it is compared with the verification variable. If it matches, the next and the last step get displayed. Or else, the user is send back to the image grid in the first step.

ISSN: 0975-8585

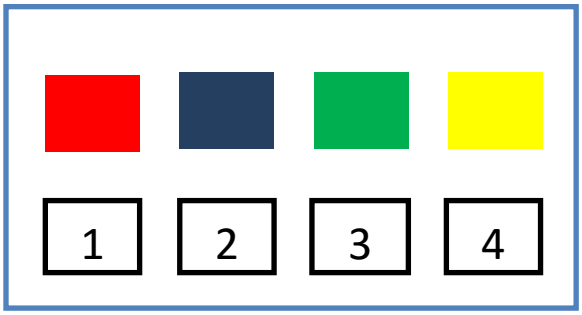


Q	W	E	R	T	1
Y	U	2	I	O	5
P	0	A	S	D	F
3	G	H	J	6	L
K	4	X	Z	V	C
8	V	B	N	M	9

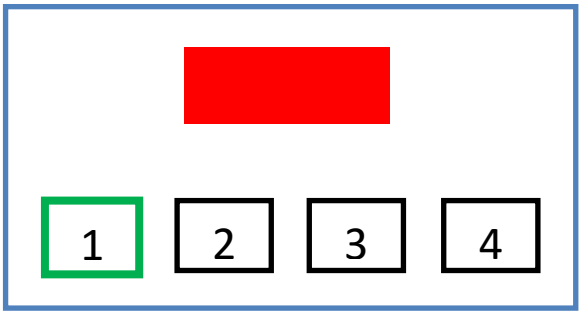
Color code verification:

To implement this part, we collected a set of image button of different color codes like green, blue, black etc. Now in the registration phase, when user rates the color with their choice, each rating of colors is being stored in the variable specified with the color. In the login phase, when user is provided with a color block among all the colors, the user typed color rating gets compared with the variables value specified during the registration phase. Once it gets verified the user gets access to the device.

Registration Phase



Login Phase



CONCLUSION

With the three step authentication, it will be difficult for the hackers to track down all the password patterns used in it by different users. Previously, a lot of technique has been initiated to authenticate an android device, but a three step technique to do so is a new approach. Although some complexity may arise

for the users to remember all the selected keys/passwords but in a long run, this technique may get acquainted with the common people. Also, three verification step is hard to crack by a hacker. This application is suitable for the users with high confidential data stored in their android devices. With further research, the technique can be made user friendly and effective in the upcoming future.

REFERENCES

[1] Kwang Il Shin, JiSoo Park, Jae Yong Lee, Jong Hyuk Park. "Design and Implementation of Improved Authentication System for Android Smartphone Users",26th IEEE International Conference on Advanced Information Networking and Applications Workshops 2012.

[2] Swapnil Waghmare, Madhumita Chatterjee and Satish L Varma. International Journal of Computer Applications 2014;87(5):19-24.

[3] PulkitTandon, Geogen George. International Journal of Engineering Development and Research 2014;2(1):847-851.

[4] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer and V Manoj Kumar. International Journal of Network Security and Its Applications 2011; 3(3):111-119.