

Android Notes using Finger Print Authentication

¹R. Jaya Prakash, ²T.Devi

¹UG Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai

²Assistant Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai

¹jp9494171454@gmail.com, ²devi.janu@gmail.com

Article Info

Volume 83

Page Number: 3242-3245

Publication Issue:

May - June 2020

Abstract

In this current digital world every people are using various smart devices in their daily life. From the different types of smart devices mobile phones are the important one. In olden days mobile phones are used only for communication. Now phones are used for various purposes such as to store personal data, funds transfer etc. So, in smart devices security is very important. Different types of security concepts are used in the mobile phones. Pattern identification and pin number is the example of security services. These security patterns are used in mobile phones with touch screen facility. These security concepts are easily hacked by the third parties. In this article proposed a new security system using finger print recognition to open the content in the mobile phone. Using this new application the users can able to create new notes, delete existing notes and open an existing notes. This method is more secure compared with existing security methods because each user have unique fingerprint id.

Article History

Article Received: 19 August 2019

Revised: 27 November 2019

Accepted: 29 January 2020

Publication: 12 May 2020

Keywords: Security, Fingerprint, Smart Device, Touch Screen, Android

1. Introduction

Due to the development of communication technology various smart devices are introduced in the market. Initially phones are used to make a connection between two members. Now mobile phones are not only used for communication. Mobile phones are used to send and receive mails from anywhere in the world, sharing photos, audio messages, video messages etc. Mostly amount transactions also done with the help of various mobile applications. In this situation security method is very important. Otherwise unauthorized persons easily hack personal details, pin number and password from our own device. In smart devices various types of security systems are already available. But in this security system is developed by using fingerprint identification. In this proposed application used in smart devices with touch facility to authorized the particular user. This app only

implement on Android based smart devices. In this application fingerprint is used for authorize the user. This application has some specific advantages. The main advantage of this proposed application is it is executed fast and easy to use by common people also. This application provides more secure and uniquely identify the specific people. It provides secure feeling during on line transaction.

The main benefit of this new application is it is the easiest and simplest way to identify the authorized user. In existing security applications uses the pin number, pattern and password to secure the contents. Touch input is easy way to protect the content from the hackers compared with other security methods such as pin or password. Most of the time, users forgot their password because password contains letters, symbols, characters and numbers. To retrieve the password is difficult process. Peoples are feeling difficult to enter the password into the small mobile

phone screen. Finger print technique overcomes these problems. A fingerprint image is varying from one person to another person. The unwanted peoples are not able to guess any one fingerprint.

This article is organized as follows. Section 2 explains about existing authentication methods used in mobile phone. Section 3 deals with the proposed application framework and its process flow. Section 4 discussed about the results of this proposed application. Section 5 deals with the conclusion of this application.

2. Literature Survey

Thom Does et al., said that finger print identification was standard authentication method on smart devices with touch facility. Finger print identification API was comes with Android 6.0 operating system. Using this API the application constructor to provide the security of data and issues the authorization such as on line money transactions. In this paper the authors were used two security techniques. The first technique change the existing software part to issue the proper authorized solution. In the second technique the authors change Inter-Process Communication facility. This was activating by using fingerprint authorization [1].

Paulson P Kuriakose et al., says about how mobiles devices were secured using different techniques. He said that mobile devices were secured by using pattern, pin number and password system. In authorization task using biometric details is a developing technology. Biometric security system is accepted by most of the android mobile manufacturers. Android based finger print API was showed new level of authentication process. Using this finger print app the mobile phone was unlocked with a single touch [2].

Young-Hoo Jo, et al., describes that most of the mobile manufacturing companies uses fingerprint security system in their products. This authentication is not only used for unlocking the phone it also provides more security while on line payment. In this article the authors discussed about the problems of current smart devices with fingerprint security by examine the services. The mobile phones are attacked in two ways. In the first way the unwanted applications can get the fingerprint picture of the user from their smart device. In the second type of attack, the hacker collect the fingerprint characters by decrypted a file from the encrypted form. In this article suggests a few solutions to avoid these attacks [3].

Octavi an Dospinescu et al. said that fingerprint identification contains many uses in the modern world because it is one of the unique biometric ids. In this papers the authors presented the various preprocessing techniques applied in fingerprint identification. In next part they developed a application for fingerprint identification which combined with Source AFIS

library. The proposed application name is called as BioFinger. This application used to fingerprint identification using the help of camera in mobile phones and presented their collected result [4].

Suchita Rane1, et al., explained about the existing security techniques like password protection, pattern and pin number. They proposed a new system for avoid factory reset attack. This factor attack erased all the contents and settings in the device. Using this factory attack the unauthorized persons are easily access the smart devices. In this article uses a new technique o avoid factory reset attack via bio authentication concept. A smart device with fingerprint security concept is more secure compared with other techniques like password, pin, number, security questions, pattern etc. [5]. Chandrasekhar Bhagavatula et al., explained face recognition and fingerprint identification were mainly used to unlock the mobile phone. According this article the authors conducted a survey regarding fingerprint recognition in Android mobiles. In this survey 198 peoples are participated. Based upon this survey the authors found facial recognition and fingerprint identification was the easiest way to unlock the Android based phones. But in the dark areas face identification was not useful. Most of the peoples preferred finger print authentication security over face identification or pin number. Fingerprint authorization was favored by most of the people. The final result of this survey recommends fingerprint identification is more secure and easy to use compared with other security techniques [6].

3. Proposed Method

Every people in the word have unique fingerprint id, both peoples are not have the similar fingerprint. This proposed application is mainly used to unlock the notes by using finger print identification. This applications will be used in Android based mobile devices with touch sensing facility. It provides more security compared with other security concepts. Before going to open any content from the mobile phone, the user provides their fingerprint. The given finger print is matched with stored finger print. If the current fingerprint matched with stored fingerprint the application going to be unlock. The comparison of finger print based in the minutiae points. The minutiae points of the finger print are represented in the following fig. 1. The location and number of minutiae points are vary from one person to another person

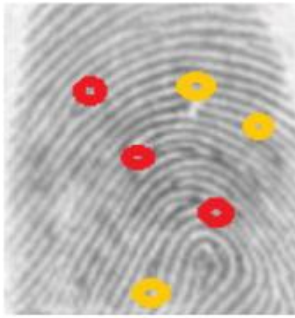


Figure1: Minutiae points

In our proposed application consists of four modules. Finger Print Authorization is the first modules of our proposed application. Using this module the user has enters their fingerprint into the system to get the access control to the notes stored in the system. : The user i.e. owner has to scan his finger to get access to the notes. The following fig 2 shows how the users scan their fingerprint to open the notes.

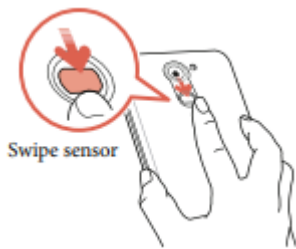


Figure 2: Scan Fingerprint

After scan the fingerprint from the user, the minutiae points are extracted using image processing algorithms. Then this extracted minutiae points are compared with stored finger print minutiae points. The match is found the user can bale to open the stored note from the database. The following fig 3 shows the process flow architecture of our proposed application.

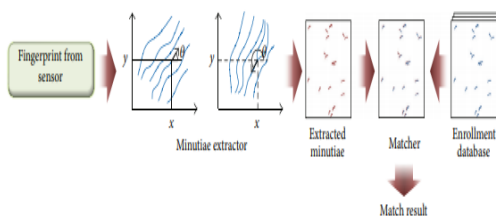


Figure :3 Mobile Fingerprint Architecture

Add notes module is used to add new notes and stored in the database. The edit notes module is used to edit already existing notes. Delete notes module is used to delete the existing notes from the database. This application is executed only on Android based mobile devices with touch screen facility. Android is the best operating system used to develop mobile

applications. This operating system is open source. So, the most of the peoples are used operating system to develop smart applications and develop new things. This security system application is very simple but using this application the notes are more secure compared with other security concepts. The main purpose of this proposed application is the phone possessor only access the notes stored in the mobile devices. This application is used as personal notes or private record or significant explanation. It is used to keep the critical notes away from unauthorized person. If the mobile device cannot have this Biometric facility, this application is not able to use. This application frontend is developed by using Android Studio concepts and the database activities are created by using SQLite.

4. Results and Discussions

Android 6.0 operating system only introduced bio metric authentication. This authentication is a new security system. That security system gives the permission to the mobile phone users to provide their proof with the single touch sense. This application mainly used in unlock mobile screen and login for online transactions. This same concept is used in our proposed application also. This proposed application provides the security for important notes in our mobile devices. The following screen shot shows the initial stage of our proposed application.

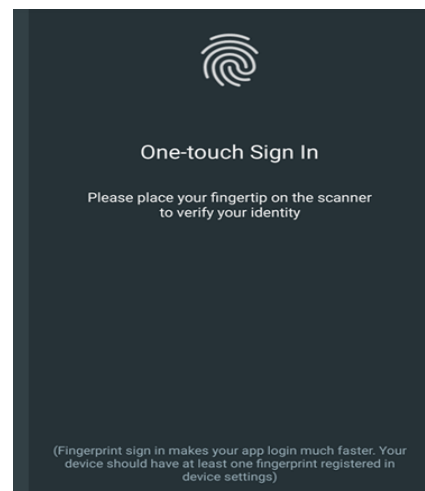


Figure 4: First Screen of Proposed Application

The first stage of our application is unlocking the screen. For this process the user can provide the finger print through mobile phone camera. If the current fingerprint is matched with stored fingerprint the specified notes will be open. Otherwise the person consider as an unauthorized person. Unauthorized persons are not able to open any content from the phone.

5. Conclusion

Different types of mobile phones are available in the market from cheapest to expensive price. Mobile content theft is increased day by day. Due to this reason more security is needed for mobile devices to store important and sensitive data. This proposed application is used to secure important documents and contents in the mobile phone by using finger print identification. Fingerprint identification is unique. The main benefit of fingerprint authorization is this id cannot able to misplace anywhere. Using fingerprint authorization online payment is also more secure than other security systems. This application verifies the user identity with registered fingerprint otherwise the specified content can't be opened. This application is processed in the Android based mobile phone without internet connectivity. To develop this application Android tool kits are used. The database creation and storing the data has done by using SQLite. Using this application the user can store any number of notes, delete unwanted notes and edit existing notes. This security technique is working based upon number of minutiae points in the fingerprints. Minutiae points are extracted by using image processing techniques.

References

- [1] Thom Does & Mike Maarse(2016), "Subverting Android 6.0 fingerprint authentication", University of Amsterdam MSc System and Network Engineering.
- [2] Paulson P Kuriakose, Ambili K(2017) , "Secured Android Application Using Biometric Authentication", International Journal of Innovative Research in Computer and Communication Engineering, Print: 2320-9798, Vol. 5, No. 4, pp. 7715-7719.
- [3] Young-Hoo Jo, Seong-Yun Jeon, Jong-Hyuk Im & Mun-Kyu Lee(2016), "Security Analysis and Improvement of Fingerprint Authentication for Smartphones", Mobile Information Systems pp. 1-11.
- [4] Octavian Dospinescu and Ilinca Liși (2016)," The Recognition of Fingerprints on Mobile Applications – an Android Case Study", Journal of Eastern Europe Research in Business and Research Article.
- [5] Suchita Rane & Narendra Shekokar(2015), " Security for Android Mobile Phones using Biometric Authentication against Factory Reset", International Journal of Science and Research, ISSN : 2319-7064, Vol. 4, No. 12,pp. 608-612.
- [6] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, Marios Savvides," Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption", pp 1-10.
- [7] S. Nirmala Sugirtha Rajini, T Bhuvaneswari & S.P Rajagopalan(2012), "Service based architecture in healthcare domain using fingerprint image identification", European Journal of Scientific Research, Vol. 85,No. 1, pp.105-109.
- [8] S.Nirmala Sugirtha Rajini(2015), " Access Control in Healthcare Information Management Systems Using Biometric Authentication", International Journal of Applied Environmental Sciences, Vol.10, No.1, pp.143-148.