ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Secured Android Application Using Biometric Authentication

Paulson P Kuriakose, Ambili K

P.G Scholar, Dept. of Computer Science and Engineering, Cochin College of Engineering, Kerala, India

Assistant Professor, Dept. of Computer Science and Engineering, CCET, Kerala Technical University, Kerala, India

ABSTRACT: Android Mobile devices are secured using various mechanisms like pattern, pin, and password. Biometric Authentication is an upcoming technology accepted by various android mobile manufactures for better security and with change in technology, time this mechanisms are vulnerable to various attacks like factory reset. Android Fingerprint APIs are bringing user authentication to a whole new level, making it fast and secure. Unlocking a phone with a single touch is one of the favourite features in Marshmallow and really wish there were more apps out there using touch identification. Fingerprint recognition itself is not new, but the OS-level support for it in Android has been much anticipated. In the near future, it's going to eliminate the need to integrate specific fingerprint SDKs from device manufacturers like Samsung, which, without a doubt, would be a great relief for app developers and users.

KEYWORDS: Android, Biometrics, Authentication, Security, Privacy

I. INTRODUCTION

Mobile phones vary from simple to smart phones, from cheap to the most expensive phones. Mobile devices are not only used for communication but also for storing sensitive data and credential information like username password, bank details, personal details and such information can be misused when mobile device gets stolen or lost [6]. With increase in mobile theft, security plays an important role. When proper security is provided to the device sensitive data can be deleted remotely after device gets stolen or make device useless for thief which will discourage mobile theft. Biometric Authentication is a technology adapted by many mobile manufactures for mobile security [1], [4]. Biometric authentication means authenticating a person based on their biological characteristics such as fingerprint, face, iris, voice, and retina. Biometric fingerprint recognition is used in majority of the smart phone's. The advantage of fingerprint biometric authentication over other biometric authentication is the uniqueness, high performance. All the people in the world have their own unique fingerprint, two persons cannot have same fingerprint not even the twins. A standalone biometric security is unreliable because of device vulnerabilities.

With support for fingerprint sensors becoming a native part of Android as of the Marshmallow release and fingerprint sensors rapidly becoming standard fare in flagship phones as a result it's easy to get spoiled by the ease of unlocking something with a touch of your finger. This release offers new APIs to let you authenticate users by using their fingerprint scans on supported devices, Use these APIs in conjunction with the Android Keystore system. Your app can authenticate users based on how recently they last unlocked their device. This feature frees users from having to remember additional app-specific passwords, and avoids the need for you to implement your own authentication user interface. Your app should use this feature in conjunction with a public or secret key implementation for user authentication.

Biometric security implementations are believed to prevent intrusions and theft against mobile cellular devices. Essentially, a biometric system is used for identification or verification based on physiological and biological factors. Generally speaking, criminal acts are motivated by various reasons. A victim can either be deprived of their cell phone by some form of theft, or be vulnerable to losing sensitive information through a breach in security. More cell phones are being stolen every day because there is a market which demands the supply; some refer to this as a black market which establishes an incentive for theft. Fingerprint recognition may seem to be a bit more secure because a fingerprint

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

is extremely unique and difficult to mimic. One study used fingerprint authentication for digital signing based on the X.509 certificate infrastructure. A unique feature to this research was the fact that users were able to download third party algorithms to customize protocols. Additionally, this research was conducted using an external USB optical fingerprint sensor and the US National Institute of Standards and Technology Biometric Image Software. A different fingerprint authentication method was discussed in another article involving an optical fingerprint reader as well. The belief in this research was that 2D code provides a more effective security protocol and QR codes are more reliable and secure. The information gathered is detailed to basic ridge patterns and specific characteristics. Both of these research articles presented a different method to the same type of biometric authentication system. According to a biometric evaluation study, penetration attempts were made against a fingerprint authentication system using an artificial fingerprint. The results showed an illegal authentication success rate of 81%. It seems that if an owner's fingerprint can be obtained and re-created with plastic and gelatin, a breach may take place and any

II. RELATED WORK

Kataria, Adhyaru, Sharma, Zaveri [1] have briefly explained biometric authentication process and different types of authentication techniques including its strength and limitations. Fingerprint authentication have high uniqueness, permanence, performance and medium universality, measurability, acceptability, circumvention which states that it is best among other biometric authentication like hand geometry, iris, retina, face, ear, voice, signature etc.

Ritu, Sonam, Vinita, Vishakha [2] have proposed an algorithm to generate pseudo random numbers. The algorithm has large cycle and values are uniformly distributed. The algorithm takes a seed value (X0) as input further using formula given below it is used to generate a set of random numbers. Donny, Liza, Lei [3] has proposed a system to discourage mobile theft and prevent theft of sensitive information. The mobile phone having biometric authentication will only charge when it gets connected to phone charger which consist biometric authentication that act as a dongle. Such system will discourage mobile theft since the thief has to steal both phone and charger without charger the phone will be useless. When phone gets stolen due of biometric authentication the owner of phone get time to erase the sensitive data remotely. Vendors should provide a unique mechanism to delete data remotely since apps which are used to delete data remotely may sometimes be vulnerable to viruses [9]. As we saw from earlier studies, vulnerabilities do exist in biometric security systems as well as the standard PIN or password-based security methods. That said, fingerprint recognition seems to be a better alternative compared to other biometric methods for security. Reason being, voice and face recognition can easily be spoofed using a photo or voice recording]. Additionally, other methods proposed such as location tracking and user recognition can be too intrusive on human privacy. In order to have a better understanding of just how unique fingerprints are, let us go over some basic facts and information

III. PROPOSED SYSTEM

Device start by fingerprint biometric authentication and only one fingerprint will be register. The device consist no memory card slot since no proper external storage encryption is provided in android devices allowing no provision to introduce the data wipe software in mobile device [10]. Our proposed system consists of three phases. The first phase is about storing the biometric fingerprint for the first time and updating the factors. Second phase is about mechanism to store it in keystore. Third phase is mechanism to login.

User should register fingerprint 10 times in system for system accuracy for first time in shop when device is purchased. To update any of the listed factors the user has to start device by passing fingerprint biometric authentication [11] and select finger print manager in settings. For updating fingerprint the user should provide correct back-up code which allows deleting the existing fingerprint. To register for new fingerprint user should provide generated authentication code which is obtain by using multi window feature of mobile device. Generate authentication code option is selected from settings to generate authentication code, user have to make use of key which user enters while registration for first time (in case of first time update) or while obtaining the generated authenticated code during previous update (in case of nth time update) and provide in other window. When correct authentication code is provided system allow user to register for new fingerprint 10 times.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

It's a quick and convenient way of authenticating the user's identity. While a traditional PIN, pattern or password is an effective security feature, there's no denying that requiring the user to input a password does add some friction to the user experience. Touching your fingertip to a sensor is far easier than entering a PIN, pattern or password, making fingerprint authentication an effective way of striking a balance between keeping your users safe and providing a frictionless user experience. You can't forget a fingerprint! Most of us have a long list of passwords we need to remember on a day-to-day basis. Plus, if you follow best practices for creating secure passwords (never use the same password more than once; always use a combination of symbols, numbers, plus upper and lower case characters) then chances are these passwords aren't particularly easy to remember! Fingerprint authentication can provide your users with all the security of a password, without actually adding to the list of passwords they need to remember on a day-to-day basis.

No more struggling with mobile keyboards. Not only are long, complex passwords difficult to remember, they're also difficult to type on the smaller screen of a mobile device. Even if your app only requests the user's password once per session, navigating the awkward mobile keyboard can make this feel like one time too many. Also, consider that many mobile users interact with their apps on the go – and no-one wants to be messing around trying to type out a long, complex password when they're stood up on a busy commuter bus! Fingerprint authentication gives users a way of confirming their identity without them having to go anywhere near the mobile keyboard.

No more annoying password recovery or reset. There's never a good time to forget your password, but forgetting a password for a mobile app can be particularly painful as users tend to interact with mobile apps on the go. If you're out and about then the last thing you want to do is sit down and navigate an app's password recovery or reset procedure. By adding fingerprint authentication to your app, you can ensure that your users never have to see your app's password recovery or reset screens again.Your fingerprint is unique and impossible to guess. Even if your users follow best practices for creating a secure password, there's no guarantee that someone won't be able to guess their password anyway, or even manipulate the user's device into leaking their password via tools such as spyware. While nothing is ever 100% secure, a fingerprint cannot be guessed or stolen in the same way a password can.

IV. PSEUDO CODE

Step 1: focus on checking that the device has the hardware, software and settings required to support fingerprint authentication
Step 2: create the key, cipher and Crypto Object that we'll use to perform the actual authentication.
Step 3: The user has granted your app permission to access the fingerprint sensor.
Step 4: Fingerprints can only be registered once the user has secured their lock screen with either a PIN, pattern or password, so you'll need to ensure the lock screen is secure before proceeding.
Step 5: The user has registered at least one fingerprint on their device.
Step 6: If any of the above requirements aren't met, then your app should gracefully disable all features that rely on fingerprint authentication and explain why the user cannot access these features.
Step 7: go to step 3.
Step 8: End.

V. SIMULATION RESULTS

The following figures showing the performance evaluation of the application with different concerns like memory, network usage, graphical performance, processor usage etc. When you develop Android apps, always pay attention to how much random-access memory (RAM) your app uses. Although the Dalvik and ART runtimes perform routine garbage collection (GC), you still need to understand when and where your app allocates and releases memory. To provide a stable user experience where the Android operating system can quickly switch between apps, make sure that your app does not unnecessarily consume memory when the user is not interacting with it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

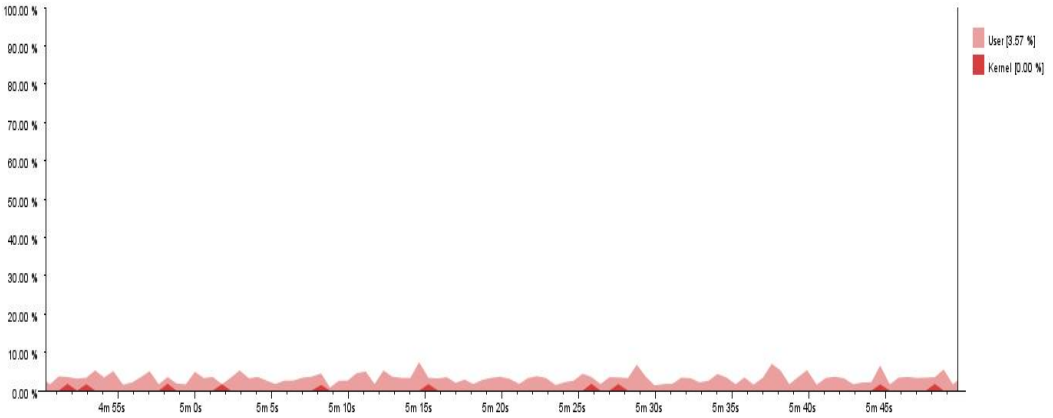

Fig 6.2 Application Memory Usage

Tracking memory allocations can give you a better understanding of where your memory-hogging objects are allocated. You can use Allocation Tracker to look at specific memory uses and to analyze critical code paths in an app such as scrolling.

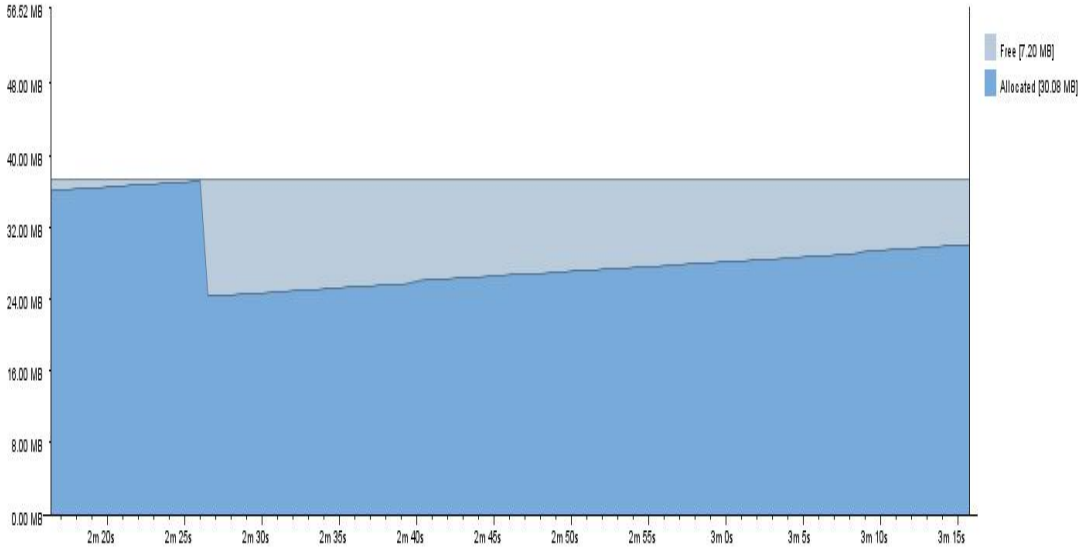

Fig 6.2 Application CPU Usage

VI. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed biometric authentication system performs better with the total memory and cpu usage. Most cell phones use a password, PIN, or visual pattern to secure the phone. With these types of security methods being used, there is much vulnerability. Another alternative is biometric authentication. Biometric security systems have been researched for many years. Some mobile manufacturers have implemented fingerprint scanners into their phones. Since theft of cell phones is becoming more common every day, there is a real need for a security system that not only protects the data, but the phone itself. It is proposed through this research that a biometric security system be the alternative to knowledge-based and password-based authentication.So we can utilize the systems

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

biometric authentication feature towards our application for better security and confidential data processing. This will not be a burden to integrate and not easy to stolen like traditional authentication factors like user id and password. and also it will not consumes much memory. so it would be a nice feature , the application with biometric authentication.

REFERENCES

[1] Kataria, Adhyaru, Sharma, Zaveri, "A survey of automated biometric authentication techniques" In Proceedings of the IEEE Nirma University International Conference on Engineering (NUiCONE), pp. 1-6, 2013.
[2] Ritu, Sonam, Vinita, Vishakha, "VRS algorithm A Novel Approach to Generate Pseudo Random Numbers" In Proceedings of the IEEE International Advance Computing Conference (IACC), pp. 7-10, 2014.
[3] Donny, Liza, Lei, "Preventing Cell Phone Intrusion and Theft using Biometrics" In Proceedings of the IEEE Security and Privacy Workshops (SPW), pp. 173-180,2013.
[4] Charles Severance. "Anil Jain: 25 Years of Biometric Recognition" IEEE Journal Computer, pp. 8-10, 2015.
[5] Weizhi Meng, Wong, Furnell, Jianying, "Surveying the Development of Biometric User Authentication on Mobile Phones" Communications Surveys & Tutorials, IEEE, pp. 1268 – 1293, 2014.
[6] Zhiling, Yufei, "Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft" In Proceedings of the IEEE 45th Hawaii International Conference on System Sciences (HICSS), pp. 1393 – 1402, 2012.
[7] R. Schwamm, N. C. Rowe, "Effects of the factory reset on mobile devices," in The Journal of Digital Forensics, Security and Law (JDFSL), VOL 9, NO 2, pp. 205-220, 2014.
[8] L. Simon, R. Anderson, "Security analysis of android factory resets" n 3rd Mobile Security Technologies Workshop (MoST) IEEE Computer Society Security and Privacy Workshops, 2015.
[9] Laurent, Ross, "Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile AntiVirus Apps" Mobile Security Technologies (MoST) IEEE Computer Society Security and Privacy Workshops, 2015.
[10] Nseir, Hirzallah, Aqel, "Issues with Various Security Threats on Mobile Phones" In Proceedings of the IEEE Information and Communication Technology (PICICT), pp. 37 – 42, 2013.
[11] Yamazaki, Dongju Li, Isshiki, Kunieda, "SIFT-based algorithm for fingerprint authentication on smartphone"
In Proceedings of the IEEE Information and Communication Technology for Embedded Systems (ICICTES), pp. 1 – 5, 2015.
[12] Khan, Qureshi, Qadeer, "Anti-theft application for android based devices", In Proceedings of the IEEE Advance Computing Conference (IACC), pp.365 – 369, 2014.
[13] Ankur, Divyanjali, Bhardwaj, "A dissection of pseudorandom number generators", In Proceedings of the IEEE 2nd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 318 –323, 2015