International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

# Biometrics and Security in Smartphones

**U. Suba, R. Karthikayani**

Master of Computer Application, University College of Engineering, Anna University, BIT Campus, Tiruchirapalli, Tamil Nadu, India

## ABSTRACT

In the present scenario, among our huge life requirements, security plays a vital role in our daily life. Till now there exist some of the security system which includes Passwords, Personal identification number (PIN), Pattern screen locks, Fingerprint scanner. Since the existing system is not fully protect our device, we need some technical development. So, here I have modify the existing system by implementing a biometric reader for eyeball scanning. The significance of biometrics, specifically iball scanning which have been implemented into smartphones, primarily the iPhone5S.. The security of the technology is presented and analyzed while the security breaches and hacks are demonstrated in detail. We look at secure options in Android vs. iOS. And we also look at the future of biometrics and soon to be wearable technology. We then propose the idea of two factor authentication and a iball scanning database

**Keywords:** iPhone, Security, Touch ID, iOS, Android

## I. INTRODUCTION

Security may be applied for application, data, network, home and buildings. In this present day we have already several type of security systems like barcode, identity card which are based on various type of technology and has tedious processing, which takes a long time for decision, highly expensive, less percentage of securing, chance of hacking and destroy or altered easily.

The point of the fingerprint reader is to save time, and to force people to implement some form of security on their devices, which often store very sensitive data. It is a cooler looking alternative to inputting long strings of complex passwords every time you want to unlock your device or authorize a transaction in the App Store. Humans are lazy and we want speed over most everything. Touch ID allows just that while also supporting just as much, if not more security than a passcode.

It is a cooler looking alternative to inputting long strings of complex passwords every time you want to unlock your device or authorize a transaction in the App Store. Humans are lazy and we want speed over most everything. Touch ID allows just that while also supporting just as much, if not more security than a passcode.

## II. LITERATURE SURVEYS

Mobile devices are rapidly becoming a key computing platform, transforming how people access business and personal information.

Access to business data from mobile devices requires secure authentication, but traditional password schemes based on a mix of alphanumerics and symbols are cumbersome and unpopular, leading users to avoid accessing business data on their personal devices altogether [7]. The rich set of input sensors on mobile devices, including cameras, microphones, touch screens, and GPS, enable sophisticated multi-media interactions. Biometric authentication methods using these sensors could offer a natural alternative to password schemes, since the sensors are familiar and already used for a variety of mobiletasks.

User frustration with password-based authentication on mobile devices demonstrates that a high level of usability must be achieved for a mobile authentication technique to be accepted. As biometric recognition algorithms continue to improve, the user experience will be an increasingly critical factor in the success of such techniques.

In this paper, we explore authentication techniques on mobile devices from the users' point of view. We study three biometric authentication modalities -voice, face

and gesture, and combinations of voice with face and gesture. A typical 8-character password condition is included as a baseline.

This study is the first to measure user action times for authentication using different biometrics on a mobile device. It provides insight into user performance when using these techniques under favorable conditions. The purposes of this paper, mobile devices are considered as tablet and cell phones which run a mobile Operating System (OS). More specifically, these are Android (Google), iOS (Apple), or BlackBerry OS (RIM). While it is important to note these terms, this literature review is focused primarily on the Android OS security vulnerabilities. Polymorphic is defined as malware that transforms to be somewhat different than the one before. The automated modifications in code do not modify the malware's functionality, but they can render conventional anti-virus detection technology ineffective against them.

Biometric authentication is a well-studied area of research. Physical biometrics, such as face, voice and signature, are the most commonly used forms.
Biometrics authentication systems have been evaluated against a rich set of metrics that incorporate both performance and usability aspects User attitudes have been explored, but relatively little attention has been paid to empirical comparison of the usability of biometric authentication methods. Tole dano et. al's usability evaluation of multimodal (non mobile) biometric authentication systems is a notable exception. It proposes a testing framework for biometric usability analysis that uses ISO usability factors (i.e., effectiveness, efficiency and satisfaction) for evaluation.

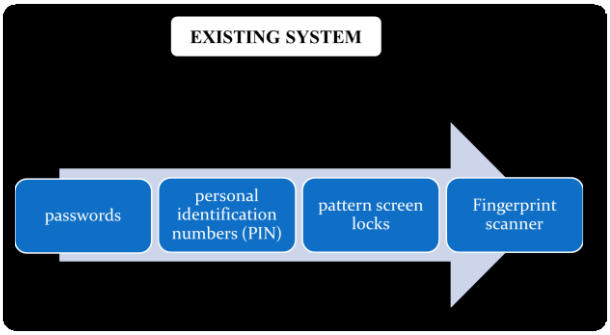
As a first approach, the investigation subject of this paperis defined as: any mobile device that contains a smartcard that is controlled by a mobile network operator (MNO).Intuitively, this is the definition of a mobile phone. This definition is too broad for us because it also coversmobile phones that are not in the focus of this paper. Theseare mainly the kind of phones that can only be used forthe phone functionality (plus text messaging and some basic other functionality), often aligned with a limited display size.Such phones are called feature phones. They sometimes have proprietary operating systems and are not extensible with additional software. Even though the applications on these phones can be attacked, e.g., Denial of Service (DoS) attacks.

This paper presents the Security Policy pattern, a design pattern that has been used in many contexts, and proved to be useful, to develop applications capable of securely loading classes off the network and executing them locally.

The Security Policy pattern can be used either on the client- or server-side. For example, in the case of a Web browser, the pattern is used on the client-side, and in the case of a global compute engine the pattern is used on the server-side. While the pattern may sound Java-centric, it can however be implemented in other languages.

Requires the existence of a framework. The security policy pattern uses theSecurityManager as its framework. Also, the security policy pattern usesthe advanced security features in Java 2 (e.g. protection domains).

## III. EXISTING SYSTEM




**Authentication:password**

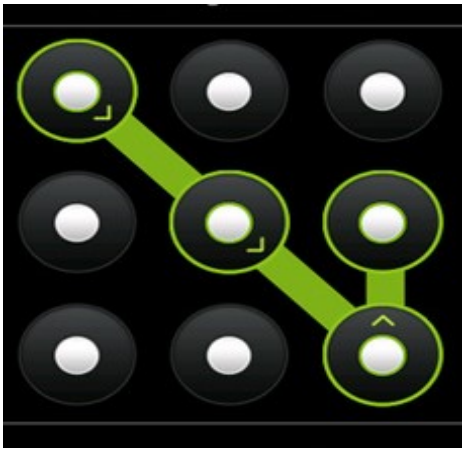
Cheapest, easiest form of authenticationWorks well with most applications Also the weakest form of access control Lazy users' passwords: *1234*, *password*, *letmein*, etc. Can be defeated using dictionary, brute force attacks Requires administrative controls to be effective, Minimum length/complexity,Password aging.Limit failed attempts. Slide unlock which has no security features, it just needed to be utilized to gain access into the phone.

A pin which is the second most secure, which increases with the amount of digits. Or you are able to choose to not have a simple pin and you can use a password as in Jelly Bean. This feature is there newest and will be thoroughly discussed through this paper. Their iball scanning, which is used to gain access to the phone.

**Autentication:Pattern lock**

Swipepathoflength 4–9 on 3 x 3 grid Easy to use, suitable for mobile devicesProblems:

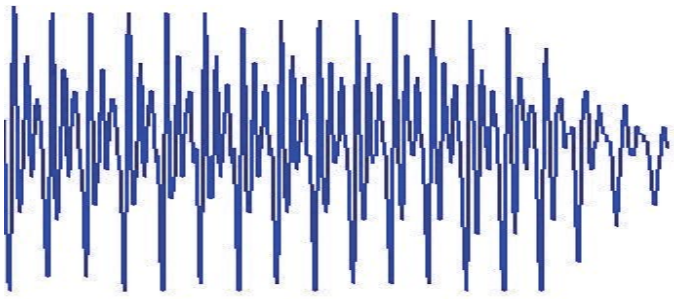
389,112 possible patterns; (456,976 possible patterns for 4-char case-insensitive alphabetic password!)
Attacker can see pattern from finger oils on screen.



**Voice**

Only three participants made positive comments, that speaker verification using a spoken number was "natural", "faster than other modes that required an additional biometric", or "easier to use than typing". Most comments were negative. Nine participants commented that they experienced"Interference between the content of the authentication method and what I needed to remember" or it was "impossibly difficult to remember things after speaking".

Participants also expressed concern about the security aspects of this approach. Five participants commented that speaking a phrase out loud "doesn't feel secure". Participants felt that voice would not be a practical method in real contexts, saying "In real life there would be noise, and interference leading to huge frustration".

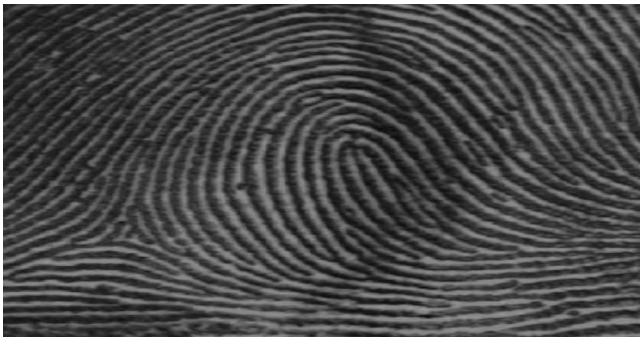


**Face**

Eleven participants made positive comments that "it was easier to remember the numbers", or "I was able to mentally 'repeat' the value, even as I was taking a picture." Four found it "easy" or "simple" to take the picture, but nine others complained that positioning the camera was "somewhat annoying", "a bit hard because of the reflection of myself I was getting" or "cumbersome to position the face". Participants commented on the lack of feedback when their face was positioned properly: "I didn't know when it worked well", or "not sure how accurately I need to place my nose in the box on the screen." Participants took action to get better pictures: "I had to find a solid background and then it worked", or "I found a better lit spot in the room". Several participants felt uncomfortable taking a picture of themselves: "I have to suspend the fact that I might not like the picture", "felt too much like I was taking a vanity photo."

***GRfinger for Fingerprint Recognition***

GRfinger Fingerprint SDK is fingerprint recognition Software Development Kit (SDK) that allows you to integrate biometrics in a wide variety of applications. It is supported by dozens of programming languages, richness of code samples, its thorough documentation and also reliable application developing in a matter of hours. We chose GRfinger as it has a readymade library that can be used by various programming languages, reliable, and it supports multiple readers.



**Apple History**

Officially founded in 1976 [1], garage-started Apple Computer went from being the laughingstock of the neighborhood in Palo Alto, California to a multinational corporation with an incredible reputation for constantly revolutionizing different industries. While it was not taken seriously its first few years, Apple has been ahead of the game while laying cornerstones along the way of technological advancement within our world. Apple's public offering of $22 per share in 1980 jumped 32% in the first day, instantly making 40 employees millionaires [2].

iPhone Evolution

In 2012 the introduction of iPhone 5 changed the physical dimensions of the glass screen that had been used for five years, making the resolution natively 16:9, which meant no more black bars when watching movies; a courteous renovation. Which leads us to today, 2013, and the first time in iPhone history of a dual device release. The iPhone 5S with its notable fingerprint reader, and the 5C which adds a splash of plastic color, undoubtedly geared towards a younger audience. Both these devices sold 9 million units their first weekend and are now available in 47 countries around thworld [3].

**Other Companies Adopting This Technology**

Apple is not the founder of fingerprint technology. In fact fingerprint readers have been implemented to security features long before the iPhone was even invented. Even Motorola had integrated a print reader in one of their smartphones in 2011, a model called the Atrix. Ironically, right after the release of iPhone 5S Motorola sent a tweet intending to put down the idea of fingerprint readers in cell phones [12]. HTC proclaimed shortly after the 5S was announced that they too would have a device with this technology.

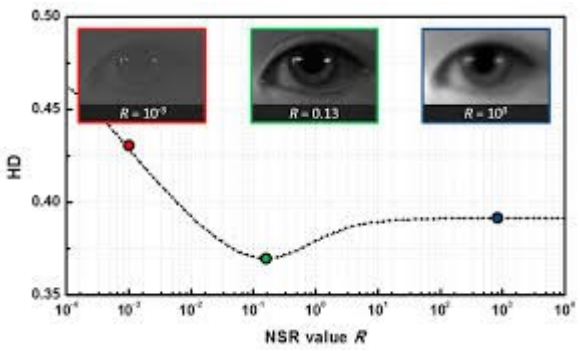
The HTC One Max's fingerprint sensor is more difficult to use and is not as well integrated to the device as the iPhone's. The sensor itself is located on the back of the device, making it hard to see when you hold it properly (screen facing you). It is located right underneath the protruding glass that covers the camera lens, and since it requires a swiping motion to activate, more than likely your finger will smudge the glass and blur your next photo.

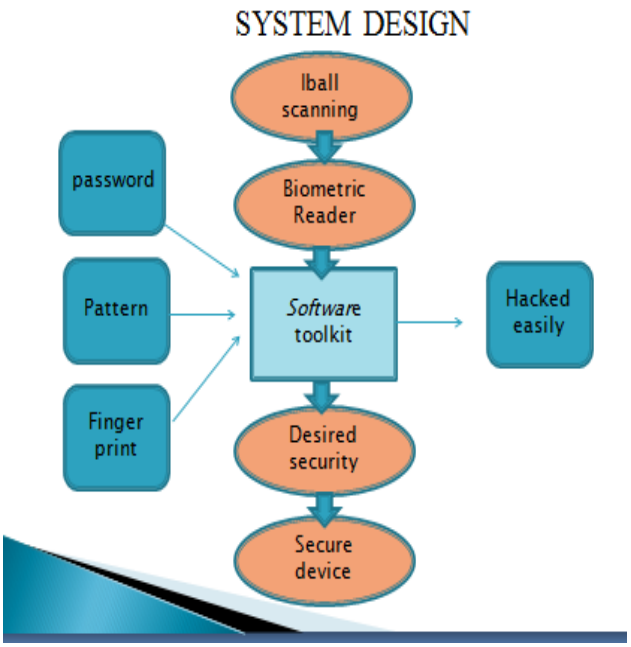
**Biometrics**

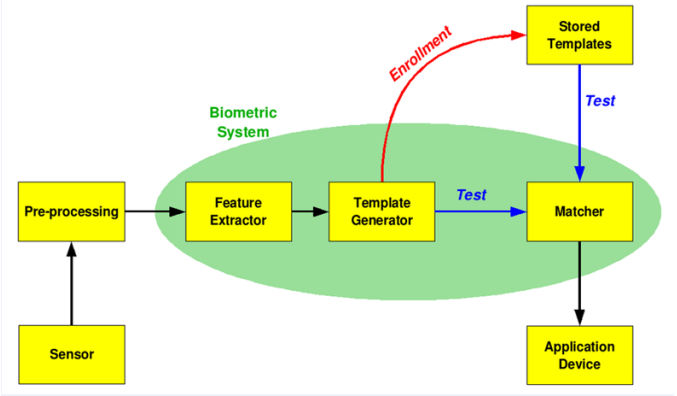
Biometric Authentication, also known as Biometrics, is a form of technology that makes use of biological traits for identification purposes. Using biometrics as a form of security has really expanded over the last few years quite rapidly. This has happened mostly for two reasons, the first of which is security and the second is convenience. Biometric identifiers are basically split up into two groups; the first is physiological. This includes fingerprints, palm prints, facial recognition, retina scanning, DNA, and iris recognition. The second form is behavioral which includes voice and typing rhythm. In computer science, most biometric authentication is used for access control. The most common example of this is using biometrics as a password, although it is not uncommon for biometrics to also be used as an identifier.

## IV. SYSTEM DESIGN

Usecasediaram:

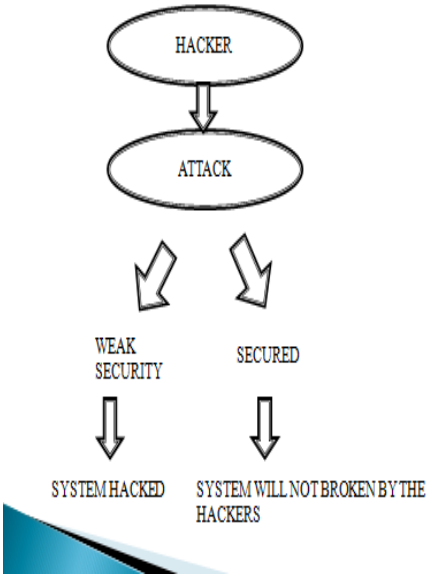


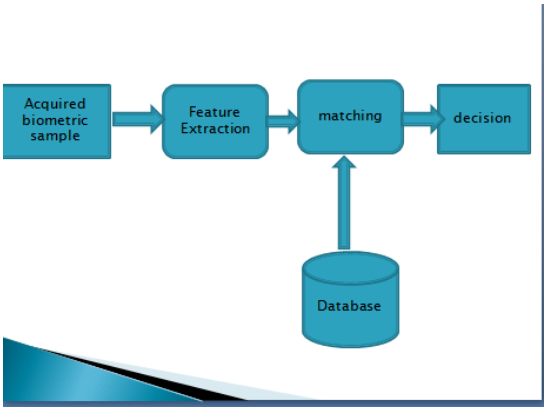


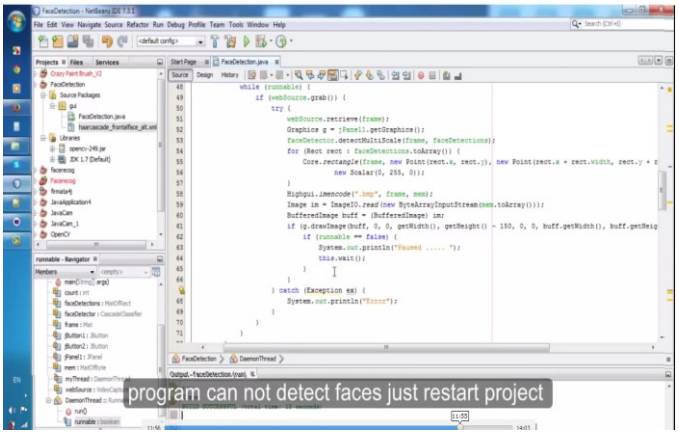

**Activity Diagram:**

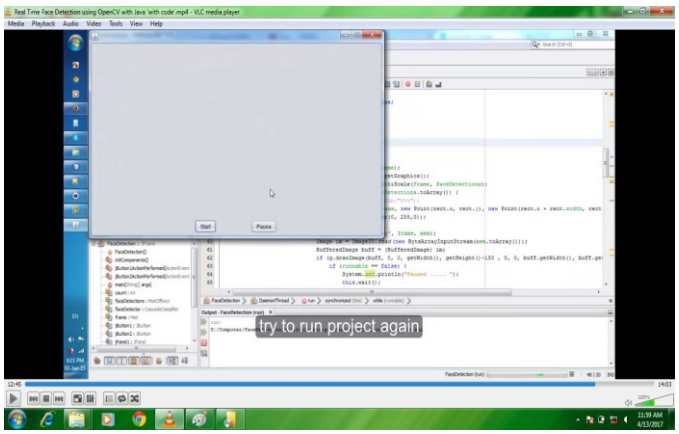
Activity diagram gives the activity involved in the working of the proposed application.

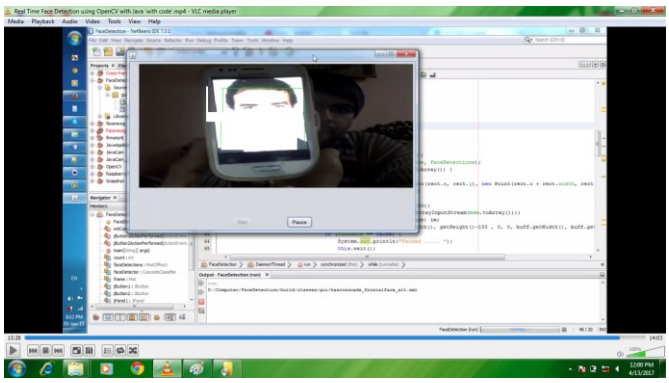



## V. OUTPUT



## VI. CONCLUSION

The proposal system (MOBAS) is based on providing user mobility and friendly, cost effective in large-scale production and processing. Captured data from sensors is sent to the PC workstation over a channel within a wireless network between the transmitter and receiver in order to provide a secure channel for the data exchange. Some changes may occur depending on the environment of implementation and accordingly minor specifications change may exist. The proposed MOBAS offers a new feature which is a mobile biometric security in smartphone " iball scanning by which the policeman can capture the personal iball scanning in some cases where he can't take a iball scanning especially in lawlessness case or anarchy case that is recently existed in some development countries in the present time. If we apply the proposed system (MOBAS) on the areas where the rate of crime increased significantly such as Egypt, Iraq and Libya in this present day, the rate of crime will be decreased and also we could stop the criminal cases that happened in the previous periods such as "Port Said Stadium Incident" in Egypt. Also MOBAS provides other features such as easy GUI for the user, low cost, sufficient results (using low cost sensors), fast and reliable transmission (identification takes around 20 seconds).

## VII. ACKNOWLEDGEMENTS

I thank Mrs.karithiyani for guiding me and supporting me till the end of the project.

## VIII. REFERENCES

[1]. The Three Tenents of Cyber Security," n.d.. [Online].Available: http://www.spi.dod.mil/ tenets.htm. [Accessed 4 November 2012].

[2]. P.H.Zope and Poonam Mote, "Multimodal Biometric system using Gabor Filter", International Journal of Advanced Trends in Computer Science and Engineering, Volume 1, No.2, May – June 2012.

[3]. Saeed Meshgini, and et al. "Face Recognition Using Gabor Filter Bank, Kernel Principle Component Analysis and Support Vector Machine", International Journal of Computer Theory and Engineering, Vol. 4, No. 5, October 2012.

[4]. P. D. Garje, and et al. "Multibiometric Identification System Based On Score Level", IOSR Journal of Electronics and Communication Engineering (IOSRJECE), Issue 6, Volume 2, pp. 07-11, Sep-Oct 2012.

[5]. Smita Kulkarni, "Improving Biometric Identification through Score Level Face Fingerprint Fusion", International Journal of Scientific & Engineering Research, Issue 6, Volume 3, June-2012 .