Effectiveness of Iphone's Touch ID: KSA Case Study

Ahmad A. Al-Daraiseh
IS dept. King Saud University
Riyadh, Saudi Arabia

Diana Al Omari
IS dept. King Saud University
Riyadh, Saudi Arabia

Hadeel Al Hamid
IS dept. King Saud University
Riyadh, Saudi Arabia

Nada Hamad
IS dept. King Saud University
Riyadh, Saudi Arabia

Rawan Althemali
IS dept. King Saud University
Riyadh, Saudi Arabia

***Abstract*—A new trend of incorporating Touch ID sensors in mobile devices is appearing. Last year, Apple released a new model of its famous iPhone (5s). One of the most anticipated and hailed features of the new device was its Touch ID. Apple advertised that the new technology will increase the security of its device, and it will also be used in different applications as a proof of identity. To make the issue more controversial, Apple announced a new financial service (Apple Pay) that allows iPhone 6 users to use their iPhone as a replacement to credit cards. The minute the new technology was introduced; many questions appeared that needed immediate answers. Users were concerned about how it will work? Is it easy to use? Is it really safe? And whether it will be effective in protecting their private data or not? In this paper we provide a comprehensive study of this feature. We discuss the advantages and disadvantages of using it. Then we analyze and share the results of a survey that we conducted to measure the effectiveness of such feature in the Kingdom of Saudi Arabia (KSA). In this study, we only focus on users from KSA, because if the device fails to protect mobile's data, severe consequences might happen. Due to cultural believes in KSA, releasing mobile contents to unauthorized people could lead to crimes. Survey analysis revealed somewhat controversial results, while 76% of all participants believe that this technology will improve the device security, only 33% use it to lock/unlock their devices, and even a smaller percentage use it to make purchases.**

***Keywords*—IPhone 5s; IPhone 6; IPhone 6 plus; Fingerprint; Touch ID**

I. INTRODUCTION

Nowadays, one of the main concerns in the mobile computing industry is the mobile security. Smartphones and other mobile devices can store and process a large amount of data in different formats. The majority of such data is private and confidential. Moreover, Hardware and software advances in this field made mobile devices an essential part of almost every activity we carry on in our lives. Storing large amount of data about such activities made mobile device a target for all types of attacks.

Attackers used vulnerabilities in communication protocols (such as, GSM, WIFI, and Bluetooth), Hardware, and software to attack mobile devices. Therefore, securing such devices from all types of attacks became a priority to all manufacturers and software developers. One of the modern security methods used in securing Smartphones against unauthorized users is the fingerprint technology. It was originally introduced to the mobile industry by Apple Company in its iPhone 5s device, and was re-used again in the new mobile editions iPhone 6, and iPhone 6 plus.

Fingerprint is the most widely used biometric to identify different individuals. It is impossible to find two persons with an identical fingerprint pattern. Also, fingerprint patterns never change during an individual's life span, which make them ideal means for identification purposes. [1]

The concept was introduced for the first time by the Chinese who invented a new technique called fingerprint to identify people. The idea received more attention in Europe during the 17th and 18th centuries, were European scientists began their interest in the human skin especially friction ridge skin. Later, in the 19th century England published many books about fingerprint. In the 20th century exactly in 1902 fingerprint evidence has started to be used in the courts of England. In 1903, New York developed the first system that uses fingerprinting for criminal purposes. Then in the year of 1921, Federal Bureau of Infestation (FBI) used fingerprinting as an identification method and built special section for that. In 1992, identification section was rebuilt as the Criminal Justice Information Services division (CJIS). [2]

Since the 80's of the last century, the usage of computing devices increased rapidly. Such devices stored and processed very sensitive data. Immediately, scientists realized the need for a strong authentication mechanism to protect those devices from an unauthorized user. While passwords and smart cards are good means for authentication, a human fingerprint might be the most unique and hardest to fake or break [3].

The important questions now are, to what extent can this technology help securing mobile devices? Do users have any concerns when using it? Will it be used openly or selectively? These questions and others will be discussed later in the

analysis section.

The rest of the paper is organized as follows: in section 2, related work is discussed. In section 3, the methodology is presented. In section 4, a comprehensive analysis is provided. Finally in section 5, conclusions are drawn.

II. Related Work

Steve Gold [4] wrote on how the future of payment authentication will be through biometric means. He explained that multiple agencies will be involved and that any standardization effort needs to consider all of them. Steve stated that using such technology will simplify the authentication process. He concluded that in order to protect users' privacy there shouldn't be a central database for biometrics, and network tracking of such devices shouldn't be allowed.

Stephen Tipton et al. [5] investigated the iOS security issues. The authors pointed out that the scanned biometric data could be recorded by Apple, in addition to problems related to faking fingerprints and usability issues. They concluded few measures Apple took to protect such data; for example, keeping the data away from app developers, turning tracking off ability, providing the iClould Key Chain which uses different PIN, and the utilization of strong encryption to prevent any group from accessing such data.

Shri et al. [6] did a study on the usability of Smartphone fingerprinting. The Authors did a task oriented experiment to see whether PIN authentication or fingerprint Authentication was more usable. Their results indicate that Fingerprint authentication was more appealing and that it could reduce the number of Smartphones that was left unsecured without a PIN.

N. Yildirim and A. Varol [7] investigated the different biometric features that could be utilized to protect mobile devices; for example, face, voice, and fingerprint. They also listed different methods and applications of such features. They concluded that fingerprint authentication will be used heavily and in different applications.

Ming Gao et al. [8] focused on the benefits the fingerprinting technology in Smartphones will bring, and challenges it will face. They concluded that this technology will be the mainstream in the future.

S. SaintGermain [9] discussed a new law in California that required a warrant to search any Smartphone. This law is considered a victory for privacy activists. The author concludes that by law, the victim shouldn't be forced to unlock his own Smartphone, and hence, the police need to be able pass the biometric authentication, even with a search warrant, by other means.

Hugh and Lorie [10] claim that using fingerprint as an authentication mechanism may reduce the system's security. The authors did a little experiment. They prepared two groups of people and asked them to create passwords to protect an e-banking account. One of the groups was only allowed to choose passwords, the other one was allowed to use fingerprints as well as passwords. By examining the length and the strength of the passwords they had chosen, the results showed that the group that was given the fingerprint option created less secure passwords than the other group. That led the authors to say that the group who had (password-with-fingerprint) account felt more secure, which made them create less secure passwords. In conclusion, using the fingerprint authentication shouldn't seduce us to select weak passwords.

Tarika and Bhawna [11] indicate that fingerprint authentication shouldn't be used. Their reasoning is that, we leave our fingerprint everywhere, and that it is very easy to reproduce such fingerprints. Hence, using them is not safe.

J. Hu [12] discussed different methods for the protection of fingerprint templates. Specifically, he considered biometric key generation, fuzzy schemes and noninvertible transforms. He concluded that the first two methods don't require the storage of a template, and the third one easily produces cancellable fingerprint templates.

It is very clear from all of the above that there are mixed opinions regarding this technology. Given the peculiar nature of Saudi Community, this research aims at finding out in which direction KSA's users will go? And how deep they will utilize the technology?

III. Methodology

In order to produce a comprehensive study of iPhone's fingerprint technology, a large amount of information was gathered and analyzed from different resources; such as, papers, newspapers, and electronic articles. After that, a survey was published to see whether Saudi people can trust this technology for securing their sensitive data or not. The reason why only Saudi participants were selected is that we wanted to see how the most private and protected society accepted the technology. The results will be discussed in the analysis section.

The main challenge was the lack of resources especially that the fingerprinting in Smartphones is new. Only few articles discussed the technology. Also, most of the conclusions were opinions rather than facts.

IV. Analysis

Apple Company, one of the largest well-known companies in the computing and Smartphone industry, has released the new version of smart phones "iPhone 5s" with a new feature added to it. The purpose of this new feature as Apple states is to improve the security of mobile phones, make it easier to their customers to protect their phones, and use it as a way to verify and accept orders done by users from the iTunes Store, and in iPhone 6, use the phone to replace credit cards.

Using this technology, iPhone mobile users can secure and lock their phones by a touch of their finger, as simple as that. So, before actually getting into the privacy details of this feature, let's give a general view over it by talking about this feature and how it works.

Currently, the technology exists in the latest releases of the iPhone (s5 and 6), some iPad versions, and other Smartphones from different manufacturers. In order to activate this feature on your device, all you have to do is to put your fingerprint on the button and through this touch; your fingerprint will be

saved through an embedded sensor. It is important to mention here that this button is made of hard glass material in order to protect it. It is also used as a lens to generate a clear picture of your fingerprint. The more you it's used on your mobile, the better the scanner will recognize your fingerprint [13].

The using of fingerprint was expanded in iPhone 6 to include purchasing products by using fingerprint as a way to pay. Apple realized how hard it is to carry and manage multiple credit cards. They also realized the danger that threatens our safety when carrying them. "Apple Pay" is a new service introduced by Apple. It is a way to pay by phone using fingerprints and NFC technology. Apple has promised a high level of security so that all transactions are confidential, and no one can track what we buy using this service. The service is now working in the United States and had a strong commencement. Apple made agreements with a large number of shops and officially began the service in October 2014 using the iPhone 6 and 6 Plus devices only. More than 220000 shops and popular restaurants in America will support this service [14]

The following sections discuss this feature from different security perspectives.

A. Safety and usability

Firstly, regarding the security and the safety of the saved fingerprints, Apple's senior vice president of hardware engineering, Dan Rico illustrated how the company's technique used to save the fingerprint information is very secure, Apple utilized one of its security techniques called "Secure Enclave".

Generally speaking, secure enclave is like a vault where information can be stored and this information cannot be accessed without the touch ID of the user. Also, the fingerprint will be saved after it has been encrypted. As Mr. Dan emphasized, the fingerprint will never ever be used in other software nor it will be saved on the company's servers.

This was regarding where the fingerprints will be saved, but actually in our daily activities, our fingerprints can be anywhere. Wherever we put our hands, our fingerprints will be. So what if someone tries to simulate our fingerprint? Will he be able to open our mobile? The answer is definitely "NO" because according to Apple Company, the sensor senses the shapes on our fingerprint from specific layers of the skin that only works on a live finger.

Secondly, regarding the usability of this iPhone 5s' fingerprint feature, is it easy to use? Absolutely yes. A user only needs to register his/her fingerprint for the first time, then start using it each time he/she wants to unlock the phone. When a user wants to unlock the phone, he/she has two options: either enter the PIN or push the home button by one of registered fingers. Both methods produce the same result. So what's the difference and why would someone use the fingerprint feature? Actually, the answer of this question will be in the next section, where a list of advantages and disadvantages of this feature will be shown. [15]

B. Advantages and disadvantages

Just like any other new technology, iPhone's touch ID has some advantages and some disadvantages. Advantages will be listed first:

- The first and most important advantage of this feature is its uniqueness. And hence it gives us a peace of mind that no one else will be able to unlock our devices. Based on this we can also assume that our data is more protected.
- Fingerprint recognition is fast. The device unlocks almost instantaneously.
- Ease of use. The phone will unlock by putting the owner's finger over the Home button.
- Convenient. Unlocking the phone doesn't require much attention, and hence users can be doing other tasks as they unlock the phone.
- Universal. iPhone's fingerprint recognition system allows the user to enrol multiple fingers which let the user use any other finger to unlock the phone if one of his fingers is injured.
- Long lasting. A person's fingerprint does not disappear by aging, but as people get older they usually lose their collagen which makes it harder to recognize their fingerprint. [16]
- Another advantage is that when the owner wants to buy music or any other material from the iTunes store, he doesn't need to enter the password, he can only use his fingerprint and this will be as a verification of his identity. [17]

On the other hand, the following are weaknesses or disadvantages of this technology:

- Fingerprints can be easily recreated. Tarika [11] indicated that fake fingerprints can be used to unlock the device.
- Overconfidence. Using the fingerprint option makes us feel more secure and hence we tend to choose weak passwords as a backup. As suggested by [10].
- Fears of wrong storage or usage. Many researchers and users expressed their fears and lack of trust. Losing such information can lead to severe consequences.
- Sensor's sensitivity. Dirty or oily skin might affect the accuracy of the sensor. Also, fingerprint recognition is affected by what the finger is exposed to of injuries or burns.

C. Reliability

Is it reliable or not? Can people rely on it as they did with the PIN? The Touch ID is very reliable and durable. Although, some people have found that sometimes the sensor may not respond to their fingerprint if the hand is wet or has a high temperature. It does work for the majority of people with no issues.

D. People's perspective toward fingerprint feature

Generally speaking, some people like this feature and find

it as an interesting new feature to protect their mobiles, and even if there is a password, they would like to use it as a way of following the technology without thinking about any privacy concerns. But actually, these are the minority, whereas the majority of people have high concerns regarding the real aim of such feature. Why to have our fingerprints saved at a specific place even if no one can share or use it. As long as the password is still there, why does Apple Company and others release such feature? Moreover, with all of Apple's efforts to convince people that their fingerprints information will be secured and not saved on their servers, people still have high fears of Apple's other objectives of this feature and whether Apple will share any of their analytical information about the Touch ID system to Apple or any other party [18].

E. People's fears and concerns

Most of people's concerns are centred on privacy and identity tracking. One main concern is that Apple stores the users' fingerprints in its servers, creating a huge database of users' biometric information for people from all around the world. If it happens, it will pose a huge threat to all users, especially if this data is handed to governments of different countries. These fears have increased dramatically after the United States' National Security Agency (NSA) spying scandal was uncovered. NSA collected personal information of citizens and residents in USA through a program called PRISM. Regarding this matter, Apple confirmed that it will not store the fingerprints in its servers and they will not be synchronized with iCloud even. Instead, it will be stored only on the encrypted chip A7. Also, it will not be stored as an image, but instead it will be stored as fingerprint data. It is worth mentioning that Apple calls the technique as (Touch ID) not (finger scan) which is an accurate description of what it does, so it doesn't scan the fingerprint but it reads features that distinguish one person from another. So, it divided the fingerprint into three parts (whorl, loop, arch) and then picked up the finer details such as the path of the blood veins. [19]

Another concern is about the recreation of one's fingerprint. These fears have increased even more since the media published a story about a German hacker who was able to hack iphone5s Touch ID and unlock the device using fake finger from a fingerprint's photo. [20]

People are also concerned that a thief is forced to cut off the victim's finger to be able to unlock the phone. Such concerns may seem exaggerated, but we can't ignore that it already happened. In 2005, a car thief in Malaysia cut off part of the owner finger to steal a car, Mercedes S-Class, which was protected by fingerprint recognition system. Regarding this, Apple confirmed that it has developed the technology, so that fingerprint recognition happens by scanning the finger skin dermal layer, which requires the finger to be alive and in its natural state. After all, the real concern would be "do thieves know that?" [21]

In the next section, results of the conducted survey will be explained in detail.

F. Survey results:

According to the survey, the majority are using iPhone for more than 3 years. And most of them are using iPhone 5s.

A survey was used to see the prevalence of this new feature amongst Saudis, whether they have liked it or not? And what are their fears and concerns about it? The survey was filled by 2230 persons living in different Saudi Arabia regions. Our sample consists of 780 females and 1450 males. The majority of all participants held a bachelor degree and between 25 to 34 years old. Thus, they are overwhelmingly young. Most of the participants in the sample are from Riyadh region. The demographic questions answers are in table 1, 2 and 3.

TABLE I. PARTICIPANT REGION

Region	Number	Percent
Riyadh region	1310	59%
Mekkah region	300	13%
Eastern region	180	8%
Qassim region	140	6%
Asir region	90	4%
Medina region	70	3%
Al Jawf region	40	2%
Northern Border region	30	1%
Jazan region	20	1%
Tabuk region	20	1%
Al Bahah region	10	1%
Hail region	10	1%
Najran region	10	1%

TABLE II. PARTICIPANT AGE

Age	Number	Percent
18-24	600	27%
25-34	1060	48%
35-44	450	20%
45-54	90	4%
55+	30	1%

TABLE III. PARTICIPANT EDUCATION

Education	Number	Percent
No high school degree	40	2%
High school degree only	460	21%
Bachelor degree	1560	70%
Master degree or higher	170	8%

Also, by asking the participants if they use the same mobile device password PIN for their online account, 21% answered "Yes", 46% answered "No" while 29%answered "Sometimes".

Regarding the usage of the fingerprint feature, the results were somewhat controversial, although 55% of all users think that password PIN is not secure enough, and 76% agree that the use of biometric can improve the mobile security, only 33% use fingerprint to unlock their iphone device, while 17% use it sometimes. Besides that, only 16% use the fingerprint to buy from iTunes usually, and 5% use it sometimes, while 77% do not use it at all. The questions along their answers in details are found in table 4.

When asked the participants if they have concerns about using the fingerprint feature, 31% answered "Yes" while 67% answered "No". Then, people who answered "Yes" were asked about their concerns. The majority of all concerns were from breach of privacy. By comparing the answers based on the range of ages, we found that the majority of people in the ages between 18 to 44 were concerned from a breach of privacy, while the major concerns for the people who are in the ages between 45 to 54, are releasing their fingerprint's details to governmental agencies. The comparison details can be seen in figure 1.

When asked "What makes you comfortable with protecting your iPhone?" 49% answered "Having strong password", 34% answered "Using biometrics", 23% answered "Having antivirus" and 17% answered "Having security software" as showed in figure2.

Finally, participants were asked about the most important things in their phones, 88% of all females which is the majority answered "personal photos" and 63% of males answered "personal photos" and "personal information" as seen in figure 3. The questions and their answers in details are shown in table 5.

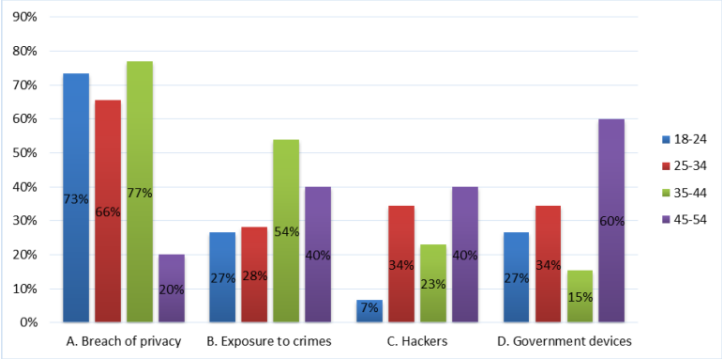

Fig. 1. participant concernes

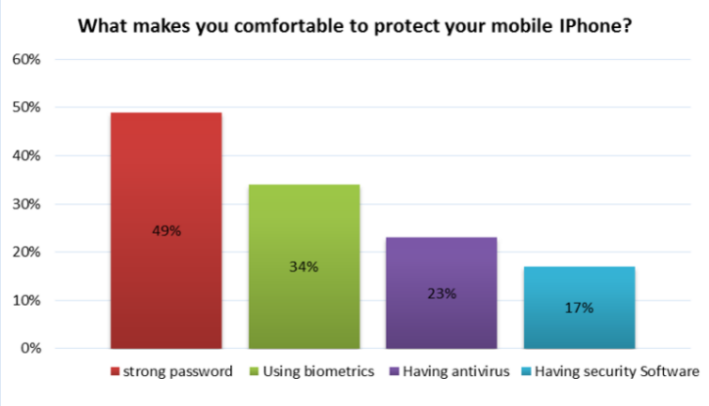

Fig. 2. protection methods results

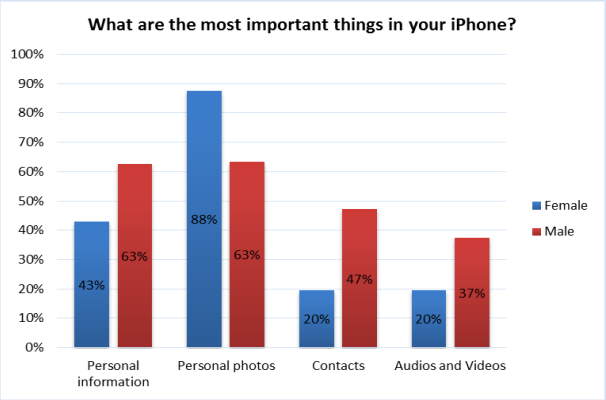

Fig. 3. participant important mobile content

TABLE IV. SUMMARY OF THE IMPRESSIONS OF FINGERPRINTS

No	Question	Responses				Total
		Yes	No	Sometimes	No answer	
1	Do you own an iPhone?	1950	180		91	2230
2	How long have you been using it? a. One year b. Two years c. More than 3 years	380 270 1400			180	2230
3	Which iPhone model do you have? a. iPhone 5s b. iPhone 6 c. iPhone 6 plus d. other	1630 80 40 480				2230
4	Do you use the same mobile password PIN for your online account?	490	1030	670	40	2230
5	Is the password “PIN” secure enough?	960	1230		40	2230
6	Do you think using biometrics improves the mobile security?	1690	490		50	2230
7	Do you use the fingerprint feature to unlock your device?	720	1080	380	41	2230
8	Do you use the fingerprint feature to buy from iTunes?	350	1710	110	51	2230
9	Do you face any difficulties while using it?	310	1420	380	120	2230
10	Do you have any concerns related to the fingerprint feature?	690	1490		50	2230

TABLE V. SUMMARY OF SECURITY ISSUES

No	Question	Responses	Total
1	Which of the following makes you comfortable protecting your iPhone?		
	a. Having antivirus	280	
	b. Having security Software	200	
	c. Having strong password is good enough	790	2290
	d. Using biometrics	480	
	e. All	60	
	f. A & B	50	
	g. C & D	150	
	h. A & B & C	20	
	i. No answer	80	
2	What are the most important things in your iPhone?		
	a. Personal information	230	
	b. Contacts	110	
	c. Personal photos	340	
	d. Audios and Videos	70	1430
	e. All	40	
	f. A & C	280	
	g. A &D	40	
	h. A &B &C	10	
	i. No answer	310	

V. CONCLUSIONS

In conclusion, there is no doubt that using Touch ID in Smartphones is an attractive and somewhat secure feature. Apple and other mobile manufacturers are racing to include in their products and find more ways to utilize it.

Different communities have mixed views regarding this technology. Some of them think that it is the most secure and convenient feature, while others think it not secure and can be used for tracking purposes.

In this paper, we covered this feature from all aspects. We discussed the pros and cons of this technology and the different views of users and researchers.

In KSA, the survey results show that people extremely care about their mobile data. Although ostensibly, the majority believes that the Touch ID will improve the security of their phones, only a small percentage fully trusts it.

ACKNOWLEDGMENT

At the end of this paper, we would like of course to thank Allah who supports us in doing everything in our lives and of course in completing this paper specially. Also, we would like to thank Dr. Ahmad Darayseh - Our instructor in the Security course - for his support and help in suggesting this interesting topic for us and also giving us many advices and ideas. Last but not least, we would like to thank our families and friends and everyone supported us with any idea and helps us in completing this paper.

REFERENCES

[1] T. Trimpe."Fingerprint Basics" [Online]. Available:http://sciencespot.net/Media/FrnsScience/fingerprintbasicscard.pdf

[2] The International Association of Identification in partnership with NIJ, The Fingerprint Sourcebook, Washington, DC 20531, The Department of Justice's National Institute of Justice (NIJ),2011.

[3] Jansen Wayne, Daniellou Ronan, Cilleros Nicolas, "Fingerprint Identification and Mobile Handheld Devices: *An Overview and Implementation."National Institute of Standards and Technology,* March 2006, 18 pages

[4] Steve Gold. (2013, Nov-Dec) "Meeting the Biometrics Payment Security Challenge". *Biometric Technology Today,* [Online] Vol. 2013, Issue 10, pp. 5–8.Available:http://www.sciencedirect.com/science/article/pii/S0969476513701759 [Nov. 12, 2014]

[5] Stephen J. Tipton, Daniel J. White II, Christopher Sershon, and Young B. Choi. (2014, May) "iOS Security and Privacy: Authentication Methods, Permissions, and Potential Pitfalls with Touch ID" , *International Journal of Computer and Information Technology*, [Online] Vol. 03 – Issue 03. Available: http://www.ijcit.com/archives/volume3/issue3/Paper030302.pdf [Nov. 12, 2014]

[6] Shri Karthikeyan, Sophia Feng, Ashwini Rao, Norman Sadeh. "Smartphone Fingerprint Authentication versus PINs: A Usability Study" in CMU-CyLab-14-012, July 31, 2014.

[7] N. Yıldırım, A.Varol. (May. 2014) "Mobile Biometric Security Systems for Today and Future", *2nd International Symposium on Digital Forensics and Security.* [Online] ISDFS'14. Available: http://asafvarol.com/makaleler/NilayYAsafV8691.pdf [Nov. 15, 2014]

[8] Ming Gao, Xihong Hu, Bo Cao and Dianxin Li. "Fingerprint Sensors in Mobile Devices", in Industrial Electronics and Applications (ICIEA), 2014 IEEE 9th Conference, 2014, pp. 1437 – 1440.

[9] SaintGermain, Sonthonax Bolivar. (September 19, 2014) "Is the Battle Over for Smart-Phones?" Available: SSRN: http://ssrn.com/abstract=2498707 or http://dx.doi.org/10.2139/ssrn.2498707

[10] Hugh Wimberly, Lorie M.Liebrock, "Using Fingerprint Authentication to Reduce System Security: An Empirical Study ", IEEE Symposium on Security and Privacy, 2012, Pp.32-46.

[11] Tarika Bhutani, Bhawna Bhutani. (Oct. 2013) "No To Fingerprint Security System", *International Journal of Computer Science and Management Research.* [Online] Vol. 2 Issue 10. Available:http://www.ijcsmr.org/vol2issue10/paper532.pdf [Nov. 12, 2014]

[12] J. Hu," Mobile Fingerprint Template Protection: Progress and Open issues", third IEEE Conference on Industrial Electronics and Applications, Singapore, RMIT University, 2008.

[13] Matt Reeder. "iPhone 5S fingerprint scanner explained: 10 questions about Apple's new smartphone feature answered." *Financial Post* (Sept. 13, 2013), sec. FP Tech Desk.

[14] Apple. (2014, October 16). Apple Pay Set to Transform Mobile Payments [Online]. Available: http://www.apple.com/apple-pay/

[15] Dave Tach. "How Apple will keep your fingerprints safe in the iPhone 5S". Internet: http://www.polygon.com/2013/9/17/4741030/apple-a7-iphone5s-fingerprints-secure-enclave, Sep 17, 2013 [Mar. 17, 2014]

[16] J.Angeline Rubella, B.Santhosh Kumar,"Fingerprint Based License Checking for Auto-Mobiles", IEEE-Forth International Conference on Advanced Computing (ICOAC), MIT, Anna University, China, December, 2012.

[17] Andrea Peterson and Hayley Tsukayama. "Fingerprint scanner for iPhone 5s raises privacy, security concerns." *The Washington Post* (Sept. 21, 2013), sec.PostTv.

[18] Dan Farber. "Sen. Franken questions privacy of iPhone 5S fingerprint scanner." Internet: http://news.cnet.com/8301-13579_3-57603947-37/sen-franken-questions-privacy-of-iphone-5s-fingerprint-scanner/. Sept.20, 2013 [Mar. 12, 2014]

[19] Stephen Braun, Anne Flaherty,Jack Gillum , Matt Apuzo.(Jun. 15. 2013).PRISM is just part of much larger,Scarier Government Surveillance program..[Online].Available:http://businessinsider.com/prism-is-just-the-start-of-nsa-spying-2013-6.

[20] Charles Arthur. (Sept. 23, 2013).iphone 5s fingerprint sensor haked by Germany's Chaos Computer Club. [Online] .Available:http://theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

[21] Jonathan Kent. (Mar.31, 2005).Malaysia car thieves steal finger.[online].Available:http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm