Securing Mobile Cloud Using Finger Print Authentication

IehabALRassan, HananAlShaher

Department of Computer Science,King Saud University,Riyadh, Saudi Arabia

ABSTRACT

Mobile cloud computing becomes part of mobile users daily life transactions. Mobile devices with Internet capabilities have increased the use of mobile clouding computing. Due to hardware limitations in mobile devices, these devices can't install and run applications require heavy CPU processing or extensive memory. Cloud computing allows mobile users to synchronize their data with remote storage and utilize applications require heavy CPU processing or extensive memory such as Microsoft Office or Adobe Photoshop, as they run in a desktop computer.

The combination of cloud computing and mobile computing introduces mobile cloud computing, which also present new issues of security threats such as unauthorized access to resources exist in mobile cloud. Protecting mobile cloud computing from illegitimate access becomes an important concern to mobile users. This paper proposes and implements a new user authentication mechanism of mobile cloud computing using fingerprint recognition system. Fingerprint images of mobile users can be captured and processed using mobile phone camera to access mobile cloud computing . The implementation of the proposed solution in different mobile operating systems and devices show security enhancement in mobile cloud computing with accepted performance level.

KEYWORDS

Mobile cloud computing, Wireless Network, Mobile Network, Mobile devices, Cloud computing, Finger print authentication

1. INTRODUCTION

The ability to access data and applications from anywhere and at any time with low cost arethe most important benefits of mobile cloud computing. The primary security issue on mobile cloud computing is protecting remote data and applications from illegitimate access. While authorized users can access the data, the cloud provider can also do so. There is also the possibility of unauthorized access, which is access by third parties such as hackers. Therefore, the security issue in mobile cloud computing becomes one of the top areas for research [1, 2]. In tradition, cloud computingusers can avoid the security risk by just encrypting the data before it is sent and stored in the cloud. However, this is not the case with the mobile users, because encryption technology is not suitable for mobile devices due to the encryption process, which requires high workload and high CPU processing[2].In this paper a new mechanism is proposed and implemented to authenticatemobile cloud computing by using fingerprint recognition as part of the security solution. Improving the mechanism of protecting access to the mobile cloud leads to improving the security overall, which at least protects the mobile cloud from unauthorized access. This section starts with an introduction to mobile cloud computing and describes the concept of mobile cloud computing. The rest of the paper is organized as follows: section2 provides a literature review about security solutions on mobile cloud. In section3 and 4 respectively, present the proposed approach as design and experimental results. At the end, conclusion is given in section5.

DOI : 10.5121/ijnsa.2013.5604

1.1. The Mobile Revolution

Portability is an added value to computer devices that almost everyone looks for, either at work or at home, along with the preservation of processing power and local data storage. That is illustrated by the growing number of laptops users rather than PCs users and that's why the functionality of mobile phone has been changed.

Initially, the basic function of mobile phoneswasto make conversation calls. Nowadays,this becomes a trivial function sincemost of mobile usersneed to browse the Internet and do their online transactions while they are in the move. Thus, the form and the function of mobile phones have been changed. Indeed, functionality of the mobile phone closely resembles that of a personal computer; therefore,people cannot ignore the mobile world and the daily impact of transactional activity of mobile technology. This appears obviously in the increasing of number of users of mobile phones, which provide Internet access and built-in computing applications [3, 4, 5].

Mobile users can eliminate some of the constraints of the traditional computing environment, such as power, space, cost, and time, by combining pre-existing technologies to create an environment and call it cloud computing. Also, if we can make the core technology in new environment, we can create virtualization to allow more flexibility, in which the same physical resources are shared virtually with multi OS. As a result, we well take the advance in processors and storage, reducing the cost of service and increasing the speed. This adds new value that any company is looking for in services. And that leads to say the cloud is a more compelling solution and the evolution of the Internet in the near future will be toward cloud computing [6, 7, 4].

Accessing the Internet through mobile devices has become an everyday event for most of mobile users, and these devices allow users to synchronize data from or to their PCs. However, due to hardware limitations, these devices can't install and run software such as Microsoft Office or Adobe Photoshop. As an alternative, cloud computing allows users to overcome these limitations and becomes the future of mobile computing [3].

Indeed, accessing the cloud with a mobile device has created a new concept called mobile cloud computing (MCC). Data will be available not only at home or at the office, but it can easily be accessed from the cloud with a mobile device and manage your data from anywhere. Mobile devices take data out of homes and offices and put them in our pockets [3].

If clients of mobile cloud computing have an Internet connection, they can accomplish their work simply. Anyway, with all of the advantages provided by mobile cloud computing, security still remains an important issue [5].

2. LITERATURE REVIEW

In the cloud computing environment, users use an authentication system to utilize the cloud servicesthrough a Web-based user interface, either a web browser or a mobile application, or a web service application programming interface (API). Authentication on the cloud is necessary to provide secure access to the cloud services by authorized users only. At present, authentication is done in different methods, such as a simple text password [12].

In the next subsections, a review of some existing authentication systems, which are based on client-server architecture. These existing authentication systems are provided by cloud computing providers, third-party providers, and as literature.

2.1 Literature

There are several proposed strong user authentication provided by researchers to improve mobile cloud security. Omri et al. in [5] introduced an application that uses handwriting recognition as an authentication system to secure access in mobile cloud. In this way, the user is identified by password and unique handwriting style. This application, which used the mobile phone as a biometric-capture device, also used Hadoop (Apache Hadoop is an open-source software that provides applications both reliability and data motion) to establish the connection between mobile user and the cloud via Internet. It has been implemented into two ways. The main difference is in the implementation mode, one as web page and the other as mobile application.

In [13], suggested using quick response code (QR code) for a user authentication system in the mobile cloud. In this system, the user ID, password, and the user's image are converted into QR code. In the multilevel authentication system proposed in [12], this authentication system generates and authenticates the password at multiple levels to access the cloud services. Access to the cloud is allowed if authentication is successful in all levels.

- First level of authentication is the organization level. This level reads the organization password; if unauthenticated they are going to terminate. If it is authenticated, then it enters a second-level authentication.
- Second level of authentication is the team level. This level reads the team password; once authentication is done, it then enters a user-level authentication.
- Last level is the user level. This level reads the user password to provide the user privileges and permission.

In [11], a strong user authentication system was proposed for cloud computing; this system verifies user authenticity via password, smartcard, and out of band authentication. In 2011, Chen, et al. [10] proposed an extension of Yang and Chang [14]. Chen adds a password protection-based mechanism with dynamic ID to provide authentication to ensure user legality.

As seen in this section, there are a few proposed systems in the literature for mobile cloud, but for regular cloud there are many proposed schemes that are good for improving security in regular cloud, but in the mobile cloud it's so hard for users because of its lack of usability.

The balance between security and usability must be found [9], just as when trying to apply the authentication system from a traditional client server to cloud computing. It can be applied, but it has a high risk because the infrastructure in the cloud is shared among users and managed by the cloud providers.

2.2.Cloud computing providers

Cloud providers are divided into three parts, depending on the type of the service provided:

1.Software as a Service (SaaS)—the users can access an application remotely via the Internet.
2.Platform as a Service (PaaS)—users can create an application to meet their needs and then deploy it on the cloud.
3.Infrastructure as a Service (IaaS)—users can rent servers, networking components, hardware, and storage.
Indeed, when reviewing most cloud providers, perhaps all- have the same authentication system based on user ID or email and password, whether the service provided is critical or not.

2.3. Third Party

Some companies prepare authentication systems as a service to access the cloud. Any services provided by companies other than the cloud provider are called third-party providers. Recently, many of mobile device fingerprint hardware solutions are provided by companies such as Grabba, S.I.C. Biometrics, and Fulcrum biometrics. Other companies provide software with strong authentication system using input either from external hardware or from the software itself. Also, there are many companies providing solutions such as web services and software development kits (SDK) for developers to create and integrate an authentication system to help the end users. But in this research we focus on products forwarded to the end users as a ready product to use.
As seen in the literature review, the lack of existing mobile user authentication systems is the main motivation to improve the mobile cloud security through strengthen the authentication system.

2.4. Related works

A few researchers have studied how to extract a fingerprint image from digital camera. [15, 16] have shown that is possible to extract a fingerprint by using a low-cost webcam when applying different preprocessing and image enhancements approaches. [17] suggested a preprocessing approach for fingerprint recognition.

In [18], they present fingerprint image preprocessing approaches based on a whole-hand image captured by digital camera. This method starts with locating a key point location from the hand contour image. Then the middle finger is segmented from the hand image to extract fingerprint from it.

In [19], they used a monochrome digital camera and, to reduce the noise in the fingerprint image, they used a low-pass filter, then feature extraction is based on block mean value and block coherence analysis. In [20], they use a strong view difference image rejection method to convert the 3D to a 2D image, and then use the core point detection algorithm to obtain the minutiae points.

Feature extraction based on region growing method, frequency information and color distribution information is used in [21], and then, to do orientation estimation, they apply the iterative robust regression method.

In [22], the segmentation is done by skin color detection and then enhanced by using the short-time Fourier transform analysis; after that the core point is detected.

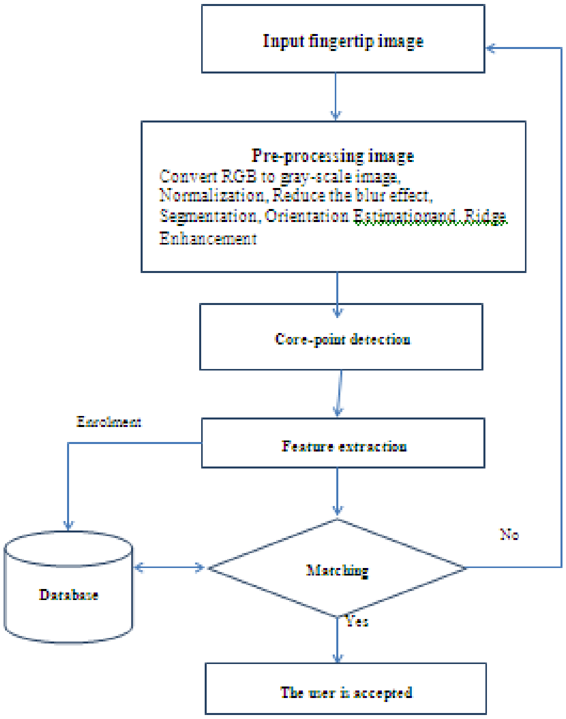

Input fingertip image
Pre-processing image
Convert RGB to gray-scale image, Normalization, Reduce the blur effect, Segmentation, Orientation Estimationand Ridge Enhancement
Core-point detection
Enrolment
Feature extraction
Database
Matching
No
Yes
The user is accepted

Fig.1. The Proposed Design Soltion

3.THE DESIGNED APPROACH

In this section, the proposed authentication mechanism using fingerprint recognition to secure access in mobile cloud is explained. Recently, there have a few works about using a digital camera or a webcam as a sensor, but in literature only. Embedding a special fingerprint sensor or adding external hardware as a fingerprint reader will be costly and will influence the mobile simplicity. Utilizing the existing camera in a mobile phone to capture fingerprint images as a biometric sensor is inexpensive to implement. The proposed solution is using a fingerprint recognition system to obtain the fingertip image through the mobile phone camera.

The aim is to convert fingertip image obtained by mobile phone camera to fingerprint image and extract ridge structure from it to be as similar as possible with the ridge structure gained from fingerprint sensor. Of course, mobile camera can't convert the image to be like the output image obtained and processed by using fingerprint sensor, but at least this process aim to export an acceptable output. Figure 1 shows the proposed design soltion and how it works.

Save or store fingerprint image on mobile device is not requirement, due each time user want access the cloud capture a new fingerprint image and login, as simple as. The whole approach was hosted on cloud to take all benefit from it (all processes and storage was there). As a developer account on a cloud provider has all privileges to create and maintain customize database as well as their applications. The database provided with Platform as a Service (PaaS) from cloud provider.

3.1.The proposed algorithm

Initially, in the enrollment phase the user presents the fingertip to the mobile phone camera to obtain a fingerprint sample and extracted features by pre-processing the sample. Then, it is stored in a database for comparison to verify the identity of the user. After take a fingerprint image as input on login form, preprocessing image function working to extract features then matching function start to match between these features with features were stored in database. If matching succeeded, then user accepted otherwise user rejected. The similarity score (S) is the result of the comparison between the extracted features and features stored in a database.

```
If (S is low value) then
    Little similarity
If (S is high value) then
    High similarity
```

After that, the decision will be based on the similarity score (S), which is compared to a predefined threshold (T).

```
If (S > T) then
    The user is accepted
Else if (S < T)
    The user is rejected [23].
```

4.EXPERIMENTAL RESULTS AND DISCUSSION

The tests were separated into two parts:

- Functionality
- Performance

4.1 Evaluation Functionality

This section evaluates each function in the pre-processing class. All functions (convert to gray-scale, filtering, etc.) gave positive test results. Figure 2 summarizes the output from various functions, including (a) the original image, (b) convert to gray-scale, (c) edge enhancement, (d) filtering, (e) binarization, (f) thinning, (g) map direction, and (h) minutiae extraction.

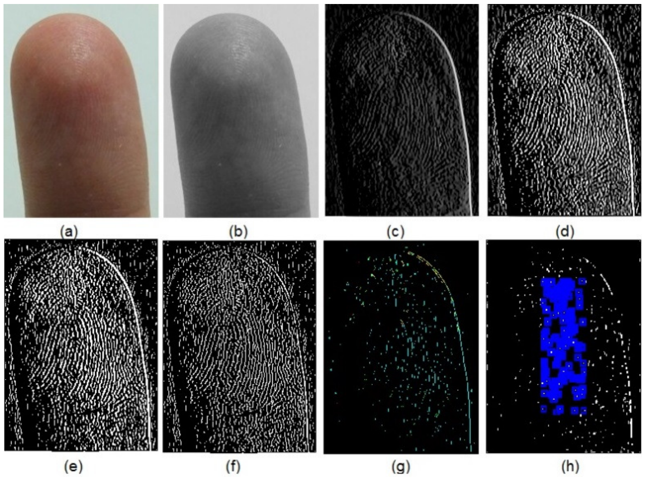


Figure 2: Functions - Output for Galaxy Note

4.2.Evaluation Performance

In this section, the process time is calculated for each function to test if the performance rate is acceptable according to the rates established by the National Institute of Standards and Technology (NIST). Figures 3,4 and5show the process time from testing the fingerprint images for the Sony Xperia S and the Samsung Galaxy S3 devices.

4.3.Conclusions from the test results

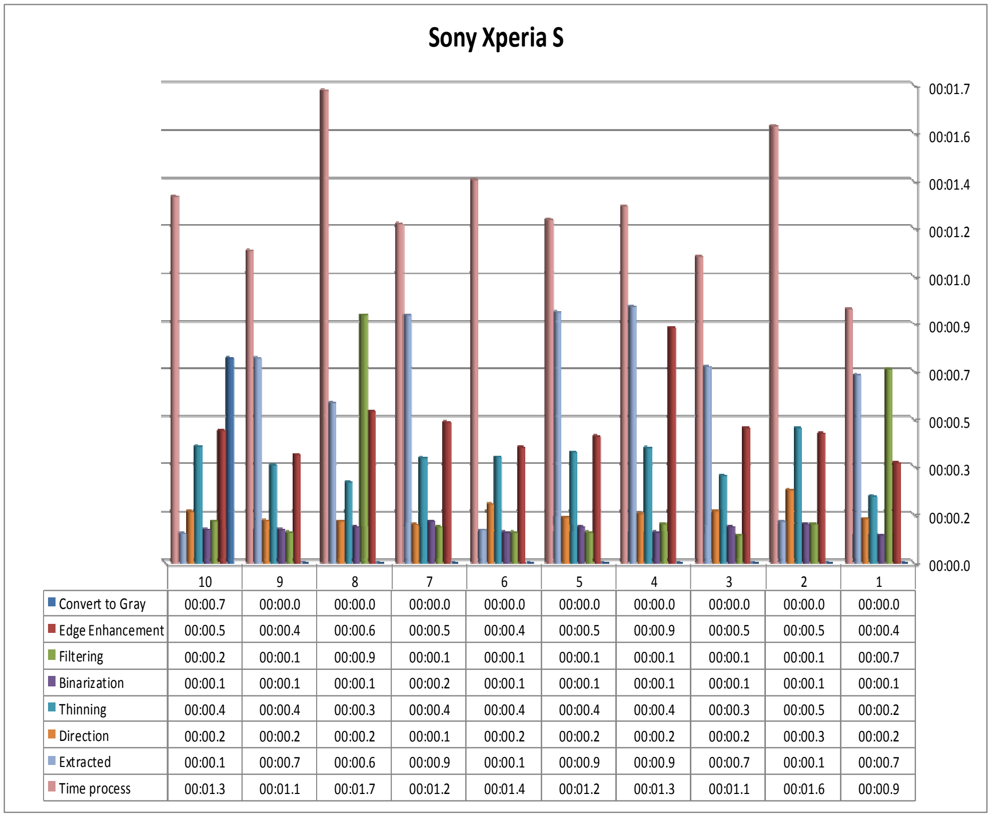
From the results presented, the following conclusions can be noticed:

- The proposed solution is not only to secure unauthorized access, but also to protect databases from injection attacks due to the absence of string input from users. The fingerprint image is the only input from the user in accordance with the interface design. No other input is permitted from the user to enter the system.
- The interface in this solution is based on HTML5, which is a cross-platform and has been tested on different mobile platforms.
- With the addition of some filters to segment the method in this solution, it will be able to work with web cameras.
- When work on fingerprint images as parabolic curves (parabola), it is easy to extract a static and accurate center point.
- Different company mobile devices that's mean different quality, resolution and size of images. In testing take this in account to prove the proposed solution should work successful with it.

Figure 3 shows the experiment results of the fingerprint image taken with the Sony Xperia S device, which recorded 0.9 seconds as the maximum time and 0.4 seconds as the average.

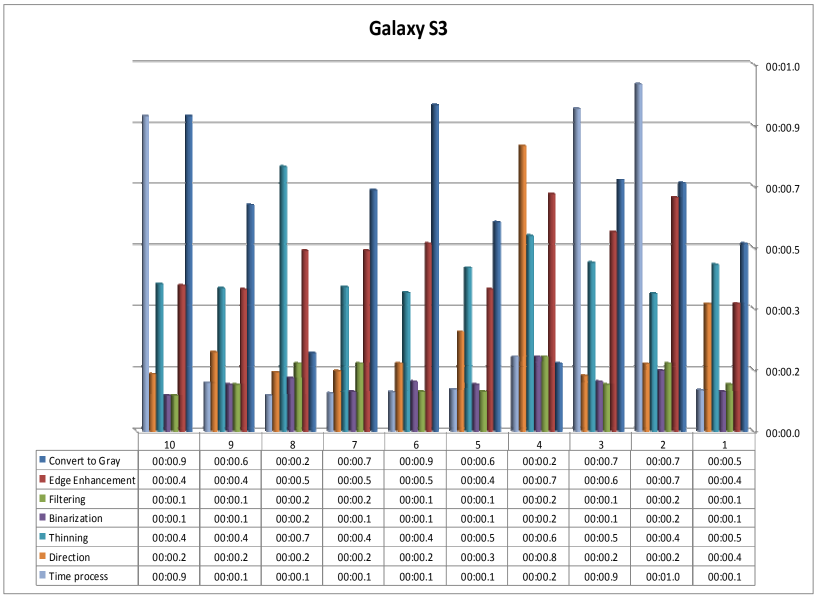
Figure 4 illustrates the process time for an image taken with a Samsung Galaxy S3 device; the maximum time is 2.4 seconds and the average is 0.5 seconds.

Another example is the BlackBerry Z in Figure 5, with approximately 4 seconds as a maximum time and 0.8 seconds as the average recorded time.



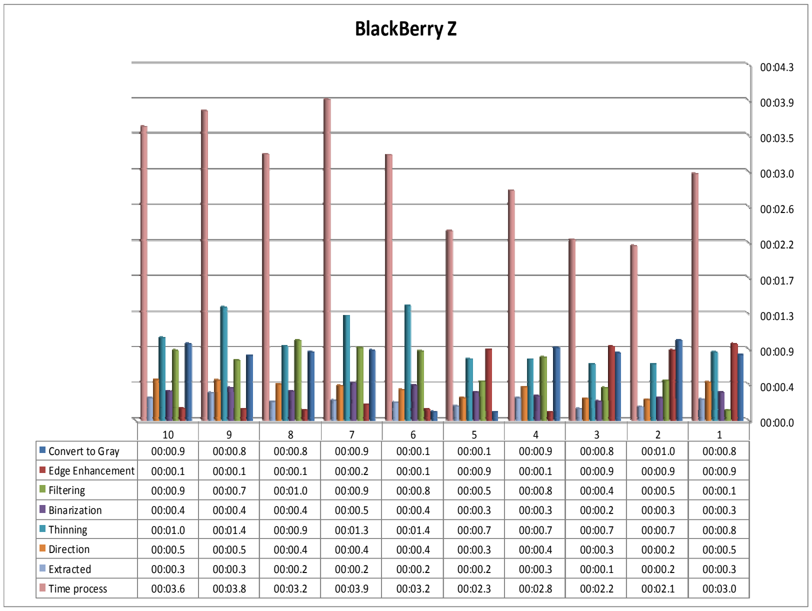
	10	9	8	7	6	5	4	3	2	1
Convert to Gray	00:00.7	00:00.0	00:00.0	00:00.0	00:00.0	00:00.0	00:00.0	00:00.0	00:00.0	00:00.0
Edge Enhancement	00:00.5	00:00.4	00:00.6	00:00.5	00:00.4	00:00.5	00:00.9	00:00.5	00:00.5	00:00.4
Filtering	00:00.2	00:00.1	00:00.9	00:00.1	00:00.1	00:00.1	00:00.1	00:00.1	00:00.1	00:00.7
Binarization	00:00.1	00:00.1	00:00.1	00:00.2	00:00.1	00:00.1	00:00.1	00:00.1	00:00.1	00:00.1
Thinning	00:00.4	00:00.4	00:00.3	00:00.4	00:00.4	00:00.4	00:00.4	00:00.3	00:00.5	00:00.2
Direction	00:00.2	00:00.2	00:00.2	00:00.1	00:00.2	00:00.2	00:00.2	00:00.2	00:00.3	00:00.2
Extracted	00:00.1	00:00.7	00:00.6	00:00.9	00:00.1	00:00.9	00:00.9	00:00.7	00:00.1	00:00.7
Time process	00:01.3	00:01.1	00:01.7	00:01.2	00:01.4	00:01.2	00:01.3	00:01.1	00:01.6	00:00.9

Figure 3: Time process for Sony Xperia S images



	10	9	8	7	6	5	4	3	2	1
Convert to Gray	00:00.9	00:00.6	00:00.2	00:00.7	00:00.9	00:00.6	00:00.2	00:00.7	00:00.7	00:00.5
Edge Enhancement	00:00.4	00:00.4	00:00.5	00:00.5	00:00.5	00:00.4	00:00.7	00:00.6	00:00.7	00:00.4
Filtering	00:00.1	00:00.1	00:00.2	00:00.2	00:00.1	00:00.1	00:00.2	00:00.1	00:00.2	00:00.1
Binarization	00:00.1	00:00.1	00:00.2	00:00.1	00:00.1	00:00.1	00:00.2	00:00.1	00:00.2	00:00.1
Thinning	00:00.4	00:00.4	00:00.7	00:00.4	00:00.4	00:00.5	00:00.6	00:00.5	00:00.4	00:00.5
Direction	00:00.2	00:00.2	00:00.2	00:00.2	00:00.2	00:00.3	00:00.8	00:00.2	00:00.2	00:00.4
Time process	00:00.9	00:00.1	00:00.1	00:00.1	00:00.1	00:00.1	00:00.2	00:00.9	00:01.0	00:00.1

Figure 4: Time process for Samsung Galaxy S3



	10	9	8	7	6	5	4	3	2	1
Convert to Gray	00:00.9	00:00.8	00:00.8	00:00.9	00:00.1	00:00.1	00:00.9	00:00.8	00:01.0	00:00.8
Edge Enhancement	00:00.1	00:00.1	00:00.1	00:00.2	00:00.1	00:00.9	00:00.1	00:00.9	00:00.9	00:00.9
Filtering	00:00.9	00:00.7	00:01.0	00:00.9	00:00.8	00:00.5	00:00.8	00:00.4	00:00.5	00:00.1
Binarization	00:00.4	00:00.4	00:00.4	00:00.5	00:00.4	00:00.3	00:00.3	00:00.2	00:00.3	00:00.3
Thinning	00:01.0	00:01.4	00:00.9	00:01.3	00:01.4	00:00.7	00:00.7	00:00.7	00:00.7	00:00.8
Direction	00:00.5	00:00.5	00:00.4	00:00.4	00:00.4	00:00.3	00:00.4	00:00.3	00:00.2	00:00.5
Extracted	00:00.3	00:00.3	00:00.2	00:00.2	00:00.2	00:00.2	00:00.3	00:00.1	00:00.2	00:00.3
Time process	00:03.6	00:03.8	00:03.2	00:03.9	00:03.2	00:02.3	00:02.8	00:02.2	00:02.1	00:03.0

Figure 5: Time process for BlackBerry Z

4.4 Discussion

The fingerprint images used in testing have a resolution of 72 dots per inch (dpi) which is less than fingerprint images resolution (300 dpi) that captured from fingerprint sensors. From the experiment results, it is evident that the range for the total processing time to pre-process a fingerprint image takes between 1 and 12 seconds. Table 1 summarizes the range of process times for each function in the pre-processing class. An acceptable enrollment time should be equal to or less than two minutes, which means that the enrollment process must be completed in 120 seconds. When the total process time is subtracted from the acceptable enrollment time, there are 108 seconds remaining for enrollment. Figures 6 and 7 show the enrollment process times in the proposed approach and how the proposed approach achieved acceptable rates.

Table 1: Summary of Process Time

Function	Range of time process	Average time
Convert to Gray	0.1 - 1	0.6s
Edge Enhancement	0.1 – 1.2	0.5s
Filtering	0.1 - 1	0.4s
Binarization	0.1 – 0.9	0.3s
Thinning	0.1 – 1.4	0.4s
Direction	0.1 – 0.9	0.2s
Extracted	0.1 – 1	0.5s
Total Time process	0.7 – 11.9	1.9s

Figure 6 shows the process time of enrolment for six different mobile devices, and nearly all are very similar. In addition, Figure 7 illustrates that 0.2 seconds is the minimum time, 19 seconds is the maximum, and 0.4 seconds is the average. This means that the proposed approach achieved 19 seconds, with 108 seconds being the maximum acceptable time.

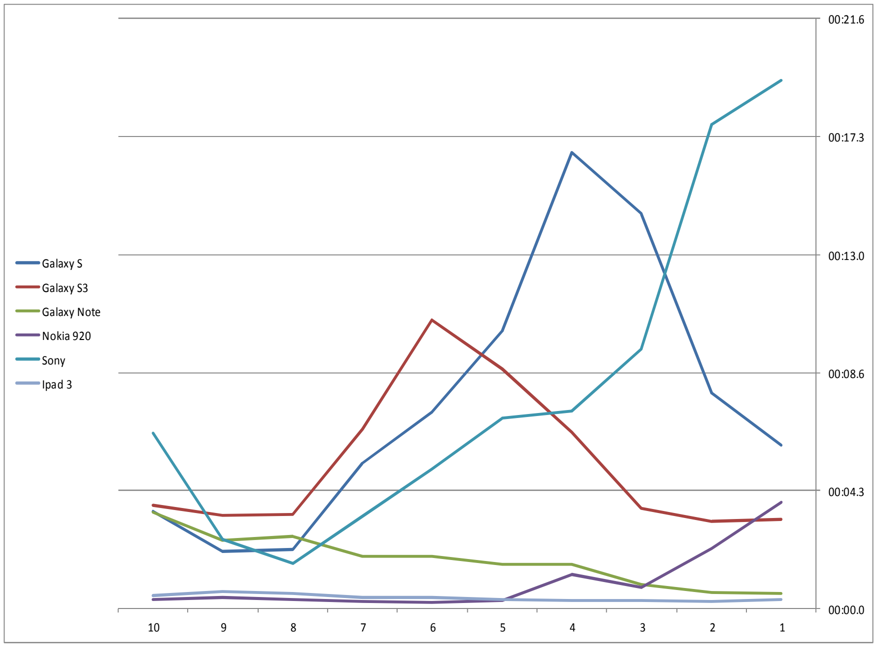
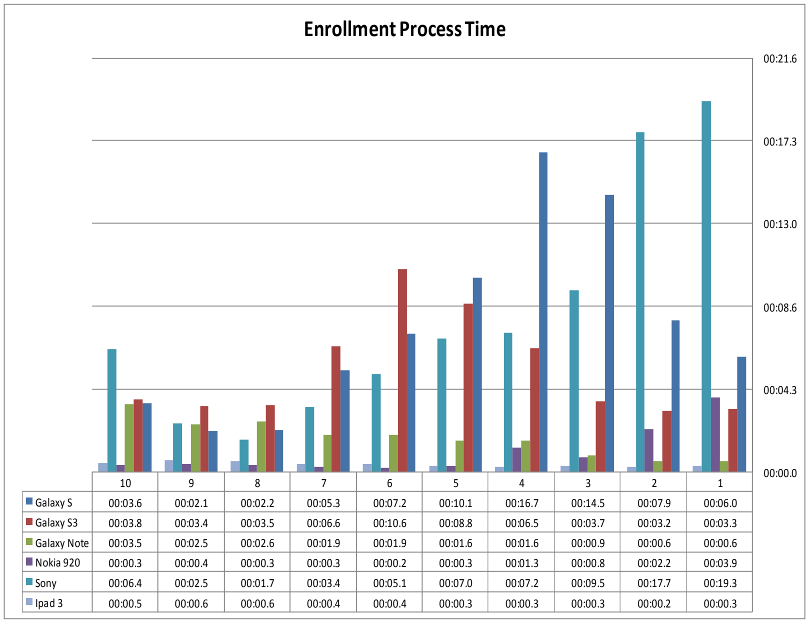


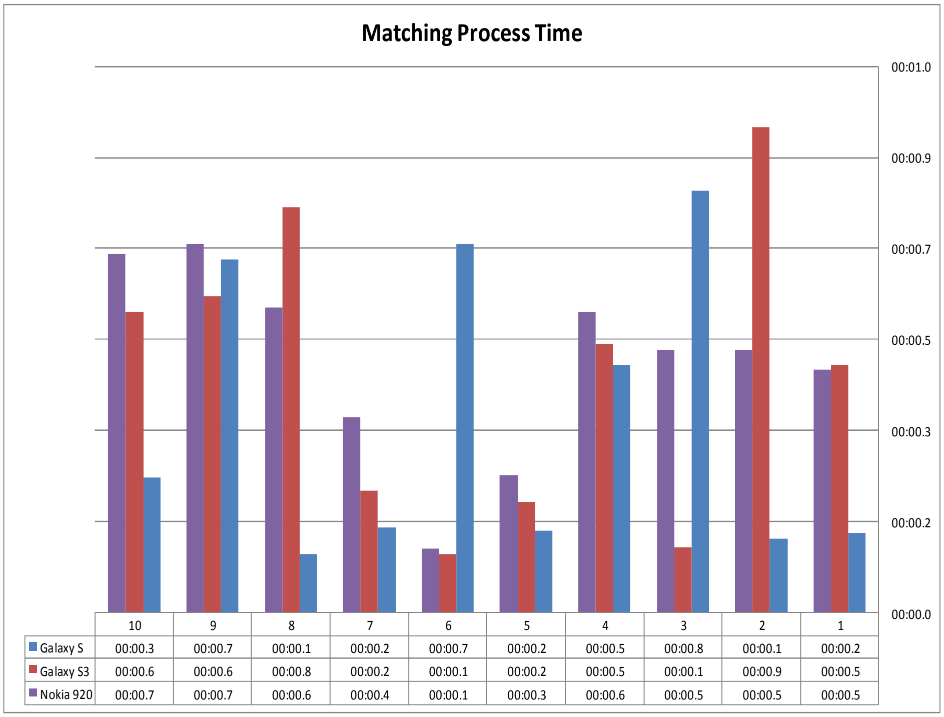
Figure 6: The time of Enrollment Process



	10	9	8	7	6	5	4	3	2	1
Galaxy S	00:03.6	00:02.1	00:02.2	00:05.3	00:07.2	00:10.1	00:16.7	00:14.5	00:07.9	00:06.0
Galaxy S3	00:03.8	00:03.4	00:03.5	00:06.6	00:10.6	00:08.8	00:06.5	00:03.7	00:03.2	00:03.3
Galaxy Note	00:03.5	00:02.5	00:02.6	00:01.9	00:01.9	00:01.6	00:01.6	00:00.9	00:00.6	00:00.6
Nokia 920	00:00.3	00:00.4	00:00.3	00:00.3	00:00.2	00:00.3	00:01.3	00:00.8	00:02.2	00:03.9
Sony	00:06.4	00:02.5	00:01.7	00:03.4	00:05.1	00:07.0	00:07.2	00:09.5	00:17.7	00:19.3
Ipad 3	00:00.5	00:00.6	00:00.6	00:00.4	00:00.4	00:00.3	00:00.3	00:00.3	00:00.2	00:00.3

Figure7: Enrollment Process Time

Creating a reference of the fingerprint images has an impact on matching results. The matching results will be more reliable if an accurate and static reference is created. This study found that by working with fingerprint images as parabolic curves, a static center point is obtained. This is in contrast to extracting a core point by using different algorithms. Further, the matching process time is shown in Figure 8 for three mobile devices. The average time is 0.4 seconds, which is an accepted rate.



	10	9	8	7	6	5	4	3	2	1
🟦 Galaxy S	00:00.3	00:00.7	00:00.1	00:00.2	00:00.7	00:00.2	00:00.5	00:00.8	00:00.1	00:00.2
🟥 Galaxy S3	00:00.6	00:00.6	00:00.8	00:00.2	00:00.1	00:00.2	00:00.5	00:00.1	00:00.9	00:00.5
🟪 Nokia 920	00:00.7	00:00.7	00:00.6	00:00.4	00:00.1	00:00.3	00:00.6	00:00.5	00:00.5	00:00.5

Figure 8: Matching Process Time

5. CONCLUSION

The combination of the cloud computing and mobile computing creates mobile cloud computing and also introduce security threats such as unauthorized users access. The focus in this researchis on the mobile cloud and protecting mobile cloud resources from illegitimate access. Biometric recognition will be used in the near future in mobile devices. The proposed solution for authenticating mobile cloud users using the existing mobile device camera as a fingerprint sensor to obtain a fingerprint image, and then process it and recognize it. Results show that the proposed solution has added value to keep performance at an accepted level.

For future work, accessing log file will be used to help identifying unauthorized attempts to access data by third parties–the cloud provider or any intruders. Based on these logs, cloud security policies will be modified and re-configured.

REFERENCES

[1] X. Li, "Cloud Computing: Introduction, Application and Security from Industry Perspectives," International Journal of Computer Science and Network Security, vol. 11, pp. 224-228, 2011.

[2] X. Yu and Q. Wen, "Design of Security Solution to Mobile Cloud Storage," Knowledge Discovery and Data Mining, pp. 255-263, 2012.

[3] J. Rittinghouse, Cloud computing: implementation, management, and security: CRC, 2009.

[4] M. Ali, "Can a Mobile Cloud Be More Trustworthy than a Traditional Cloud?," Security and Privacy in Mobile Information and Communication Systems, pp. 125-135, 2012.

[5] F. Omri, R. Hamila, S. Foufou, and M. Jarraya, "Cloud-Ready Biometric System for Mobile Security Access," Networked Digital Technologies, pp. 192-200, 2012.

[6] J. Hurwitz, R. Bloor, M. Kaufman, and F. Halper, Cloud computing for dummies vol. 1: For Dummies, 2009.

[7] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security and privacy: an enterprise perspective on risks and compliance: O'Reilly Media, Incorporated, 2009.

[9] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing, 2011.

[10] T. H. Chen, H. Yeh, and W. K. Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," in Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on, 2011, pp. 155-159.

[11] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," in Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, 2011, pp. 110-115.

[12] H. Dinesha and V. Agrawal, "Multi-level authentication technique for accessing cloud services," in Computing, Communication and Applications (ICCCA), 2012 International Conference on, 2012, pp. 1-4.

[13] D. S. Oh, B. H. Kim, and J. K. Lee, "A Study on Authentication System Using QR Code for Mobile Cloud Computing Environment," Future Information Technology, pp. 500-507, 2011.

[14] J. H. Yang and C. C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," Computers & Security, vol. 28, pp. 138-143, 2009.

[15] R. Mueller and R. Sanchez-Reillo, "An Approach to Biometric Identity Management Using Low Cost Equipment," in Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on, 2009, pp. 1096-1100.

[16] B. Y. Hiew, A. B. J. Teoh, and O. S. Yin, "A secure digital camera based fingerprint verification system," Journal of Visual Communication and Image Representation, vol. 21, pp. 219-231, 2010.

[17] B. Hiew, A. B. J. Teoh, and D. C. L. Ngo, "Preprocessing of fingerprint images captured with a digital camera," in Control, Automation, Robotics and Vision, 2006. ICARCV'06. 9th International Conference on, 2006, pp. 1-6.

[18] P. Yu, D. Xu, H. Li, and H. Zhou, "Fingerprint image preprocessing based on whole-hand image captured by digital camera," in Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on, 2009, pp. 1-4.

[19] Y. Song, C. Lee, and J. Kim, "A new scheme for touchless fingerprint recognition system," in Intelligent Signal Processing and Communication Systems, 2004. ISPACS 2004. Proceedings of 2004 International Symposium on, 2004, pp. 524-527.

[20] C. Lee, S. Lee, and J. Kim, "A study of touchless fingerprint recognition system," Structural, Syntactic, and Statistical Pattern Recognition, pp. 358-365, 2006.

[21] C. Lee, S. Lee, J. Kim, and S. J. Kim, "Preprocessing of a fingerprint image captured with a mobile camera," Advances in Biometrics, pp. 348-355, 2005.

[22] B. Hiew, A. B. J. Teoh, and D. C. L. Ngo, "Automatic digital camera based fingerprint image preprocessing," in Computer Graphics, Imaging and Visualisation, 2006 International Conference on, 2006, pp. 182-189.

[23] M. O. Derawi, B. Yang, and C. Busch, "Fingerprint Recognition with Embedded Cameras on Mobile Phones," Security and Privacy in Mobile Information and Communication Systems, pp. 136-147, 2012.