© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Robust Security Enhancement for Smartphone Using Biometric Fingerprint

Dr. D. Bennet
Professor, Department of computer Applications, Anna University, Narayanaguru College of Engineering, Kanyakumari, Tamil Nadu, India

ABSTRACT

The tremendous growth of Information and Communication Technology the samatphone take an important role for everyone day to day activity. In which the different level of peoples uses assortment of applications. Huge amount of users use smartphone, at the same time Security in smartphones have come to constitute a competitive platform that connects humans and the surrounding physical world. Along with the communication functions and mobility of cellular phones, smartphones have various sensors in addition to greatly enhanced performances and storage space compared with existing cellular phones. However the "unlock" process of smartphones and the need for user passwords when accessing social network services establish to be great flaw in smartphone security. Therefore, smartphone security should be enhanced through biometrics, which can make up for the shortcomings of passwords and PIN (Personal Identification Number). The proposed fingerprint recognition method to be enhanced the system performance and also to improve the smartphone security. To evaluate the proposed fingerprint recognition method is used in the smartphones, its performance was compared with existing fingerprint verification methods in terms of FAR (False Acceptance Ratio), FRR (False Rejected Ratio) and EER (Equal Error Rate).

Keywords : PIN, FRR, FAR, EER and CPS (Cyber-Physical Systems)

I. INTRODUCTION

Given the augmented significance of the relationship of existing physical systems in real space with cyberspace, or software running on the computers, the offered concept of embedded systems has been expanded to Cyber-Physical Systems (CPS). Various embedded devices compute based on the observed status of the physical system which influences the physical system itself. It is an integrated system that observes, adjusts, and controls a physical system's actions. As shown in Fig.1 the CPS concept covers a range of artificial intelligence systems such as traffic control, social network system and realtime information sharing [1]

Smartphones equipped with various sensors have recently witnessed widespread adoption. They can be considered a field where mobile CPS has been applied. The recital of mobile devices such as smartphones is improving swiftly. Along with information processing capabilities, various sensor modules such as mobile communication such as camera, accelerometer, and gravity sensor, as well as hardware capabilities such as storage space, 2nd, 3rd, and 4th generation mobile communication, WiFi, Global Positioning System(GPS), and Bluetooth enable mobile CPS through mobile devices. Unlike conventional embedded systems, which generally are immobile given the high cost of mobility, smartphone users can carry a mobile conveniently and acquire information about their surroundings using various sensors. In addition, smartphones users react to the physical

world through the smartphone regardless of time or space. Hence, smartphones are used as a convenient, competitive platform between humans and the surrounding physical world.

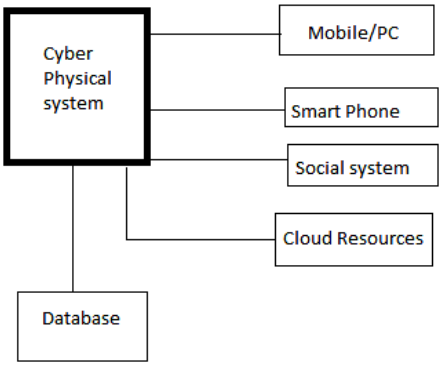

Figure 1. Cyber Physical System

II. SOCIAL NETWORKING SERVICES

Social Networking Services (SNS) users can share their thoughts, meditations, status, and cultures. Given that users can share information through SNS using a smartphone and regardless of time and space, online SNS usage through smartphones is increasing rapidly. Moreover, many SNS companies have been announcing smartphone mobile applications that allow quick and easy access to various SNSs [2]. The greatest strength of a SNS is that it allows communication with numerous other SNS users through chatting, messaging, file sharing, wikis, e-mails, voice mails, and videos. When communicating through SNS, in most cases, users only recognize others through their SNS IDs and not by their physical forms. Hence, one can impersonate another by cracking that person's account information and logging into a SNS using that information or by creating and operating an alternative SNS account in that person's name. Recently, such incidents have actually been occurring in SNSs. Most SNSs perform personal verification with a user ID and a password, both of which are easy to steal. Furthermore, when using smartphones for accessing SNSs, the respective IDs and passwords are stored in the system for automatic login. The automatic login feature ensures that users are not required to type their ID and password at each log in, as well as to avoid any inconvenience due to forgotten passwords. In the light of these issues, the password-based user authentication currently used in smartphones, as well as the security of the password-typing process, requires improvements. Recognizing this need, of late, smartphone manufacturers have been implementing biometric features such as fingerprint or facial verification,

III. SMARTPHONE SECURITY STRENGTHENING USING FINGERPRINT VERIFICATION

More services are being provided to customers thanks to the development of computer and communication technologies, which do not impose any time or location-based limits on service delivery. Given that the importance of smartphone use is increasing in real life owing to services such as SNS and Internet banking, faceless verification services are gaining importance. Currently, verification systems such as password or Personal Identification Number (PIN) are mainly used. However, these methods have problems such as users forgetting key information and easy misuse by others of data exposed externally. Several studies have focused on various solutions solving such problems. Among those solutions, biometrics has drawn much attention as an appropriate means for solving such problems as well as enhancing security [3]. For strengthening smartphone security through fingerprint verification, smartphones' "unlock" process needs to be strengthened. Smartphones are generally unlocked using passwords and patterns. When typing passwords or drawing patterns, however, they can be easily spied on or deduced. In contrast, fingerprint-based verification is safer because even if someone tries to spy on the fingerprint input process, fingerprint information cannot be leaked or deduced. Moreover, because the user simply has to touch the fingerprint sensor, the inconvenience resulted from the typing password when using SNSs is avoided.

Even smartphone manufacturers are implementing fingerprint sensors in their products or developing fingerprint sensors for smartphones for improving smartphone security. Hencethe security of the password input process, which is the weakest link in controlling user access to smartphones or SNSs, can be improved by using fingerprint verification, as shown in Figure 3. More, over, this method can be used not only for smartphone unlocking and access but also for user verification in various smartphone applications.

IV. PROPOSED FINGERPRINT VERIFICATION

A. FINGERPRINT PROCESSING

In this method the biometric measurement is extracted from the user's finger print image and is send along with the username to authenticate. The fingerprint image of the user is depicted as follows,

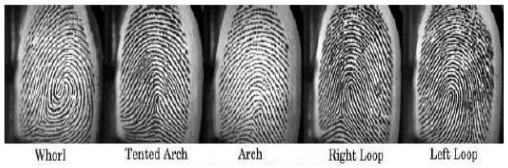

Figure 2. Fingerprint images

To improve the matching score to enhance [4] the fingerprint image for further processing.The fingerprint image is processed through image processing techniques such as Rom filter, Normalisation, Binarization, Thinning, Minutiae extraction and core detection. Once the core is detected the digest is calculated from it.The biometric measurement extracted is derived from the ridge ending and bifurcations which are shown as follows,

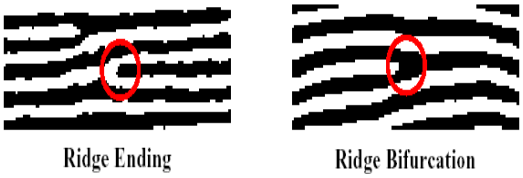

Figure 3. Biometric measurement

In this the digest that is send along with the username to register. Once the user is registered their authentication is checked at the two servers that are proposed. The block diagram to represent the process carried out in an image is as follows,

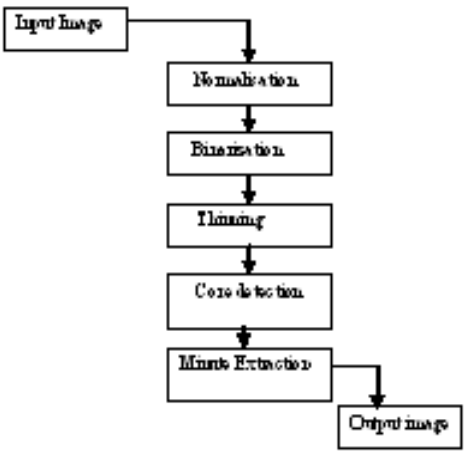

Figure 4. Block Diagram finger processing

B. ROM FILTERING

Filtering is the process of removing the noise present in the image. The image may be introduced by dirt or body oil while the fingerprint image is captured. Lot of filtering approaches is used for noise removal. Here the ROM filter concept is used. It is an accurate filter while comparing the other filters. This filtering operation depends on the state variable. The state variable is defined as the output of the classifier that acts on the difference between the current pixel and the remaining rank ordered pixel values inside a neighborhood window centered on the current pixel

C. BINARIZATION

The binarization operation takes a grayscale fingerprint image as an input and returns a binary fingerprint image is output. The image is reduced in intensity levels from the original 256 (8-bit pixels) to 2 (1-bit pixels). The difficulty in performing binirization is that all the fingerprint images do not have the same intensity threshold cannot be chosen. Therefore, a common image processing tool is used to determine threshold.

D. NORMALIZATION

Before process the input fingerprint image, we normalize the image to constant mean and variance. Normalization is done to remove the effects of sensor noise and finger pressure difference denotes the Gray value at pixel and is the estimated mean and variance of the input fingerprint Image.

$$N(i,j) = \begin{cases} M_0 + \sqrt{\frac{VAR_0 \times (I(i,j)-M)^2}{VAR}}, & \text{if } I(i,j) > M \\ M_0 - \sqrt{\frac{VAR_0 \times (I(i,j)-M)^2}{VAR}}, & \text{otherwise} \end{cases}$$

Where M_0 , VAR are the desired mean and variance values.

E. THINNING

Thinning is a morphological operation that is used to remove selected foreground pixels from binary image. Thinning reduces the widths of the ridges. A good thinning method will reduce the ridges to single-pixel width while retaining connectivity and minimizing the number of artifacts introduced due to this processing.

F. CORE DETECTION

A reliable approach for the detection of the singular points is required to classify the fingerprints conveniently. The IBBO (Iterative Block Based Orientation) *method* is the proposed practical approach to detect the singular points in fingerprints. By using this method, the core and delta points are extracted on the basis of differences in the local ridge directions between the adjacent blocks and also the minute points are extracted. Since the algorithm of the IBBO method is quite simple and efficient.

V. PROPOSED METHODOLOGY

In the existing cloud architecture is not effusive prevent the un-authorized access for the information available in cloud. The propose methodology first to verified the user identity i.e. fingerprint, is authorized allow the user to access the information in cloud otherwise could not permit the user.

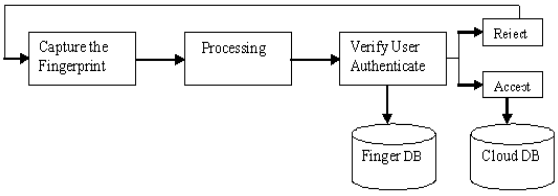

Figure 5. Proposed Architecture

To capture the fingerprint using a capture device and store the finger features in the finger database. The features are located in the cloud server at the datacenters. The user access the information from cloud server, first to verify the user is legitimate or not. Then the user is authenticated under verification process to accept otherwise reject.

VI. PERFORMANCE COMPARISON

The proposed method is compared with the existing methods to get better performance in case of effective security. In a multi-server based network [5] architecture to locate a separate server for authentication. Because the passwords and pin not fully supported for network based Cloud security, but the biometric fingerprint based authentication scheme to prevent unauthorized access and highly secured.

VII. CONCLUSION

The utilities of smartphones are to a great extent increased. The social network services, which are used for sharing personal information and status through web services, are increasing in conjunction with the increase of high-performance smartphones. Social network services are fundamentally changing not only personal life patterns but also modern political, economic, and social environments. It can replace conventional media that cannot perform its role properly by the control in countries. Hence, SNS safety procedures are extremely important. When any person accessing social network service through smartphones, password information can be leaked

during the user login process or it can be hacked if one loses their smartphone. The present methodology proposed using fingerprint verification for robust security of smartphones as well as the login process. I conclude that in a smarphones, cloud based services or any other online/offline services the biometrics based security gives better result comparethe finger database. The features are located in the cloud server at the datacenters. The user access the information from cloud server, first to verify the user is legitimate or not. Then the user is authenticated under verification process to accept otherwise reject.

VIII. REFERENCES

[1]. M. Conti, S. K. Das, C. Bisdikian et al., "Looking ahead in pervasive computing: challenges and opportunities in the era of cyberphysical convergence," Pervasive and Mobile Computing, vol. 8, no. 1, pp. 2–21, 2012.

[2]. M. Salehan and A. Negahban, "Social networking on smartphones: when mobile phones become ddictive," Computers in Human Behavior, vol. 29, no. 6, pp. 2632–2639, 2013.

[3]. S. Prabhakar and A. K. Jain, Automatic Fingerprint Recognition System, Springer, 2007.

[4]. D. Bennet and Dr.S.Arumuga Perumal, "Fingerprint: DWT, SVD Based Enhancement and Significant Contrast for Ridges and Valleys Using Fuzzy Measures" Journal Of Computer Science And Engineering, Volume 6, Issue1, March-2011.

[5]. D. Bennet and Dr.S.Arumuga Perumal, "Fingerprint Based Multi-Server Authentication System", Print ISBN: 978-1-4244-8678-6, Digital Object Identifier: 10.1109/ICECTECH. 2011.5941869. Current Version: 07 July 2011.

Dr. D. Bennet. Professor, Narayanaguru College of Engineering,, Kanyakumari Dist. He has totally 20 years of experience in teaching as well as research. He has completed his M.C.A degree from Manonmaniam Sundranar University. M.Phil Computer Science from Alagappa University, Karaikudi., and Ph. D in computer Science from Manonmaniam Sundranar University. He is a counselor in IGNOU and also staff in charge and examiner in Maduri Kamaraj University, Manonmaniam Sundranar University and Alagappa University. He has organized and attended number of National, International seminars, conferences, Workshops and also presented papers. His area of research is Network Security using Biometrics. He has also a deep knowledge in Image Processing, Data Mining, Network Security, Neural Network, Cloud computing and Multimedia Technology.
profdbennet@gmail.com.