

Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach

Mangala Belkhede*, Veena Gulhane**, Dr. Preeti Bajaj***

* Department of Computer Science and Engineering,

** Department of Computer Science and Engineering,

***Department of Electronics Engineering,

G. H. Raisoni College of Engineering, Nagpur, India.

msmadankar@gmail.com, vinagulhane@gmail.com, preetibajaj@ieee.org

Abstract—

The next generation of banking applications won't be on desktop or mainframes but on the small devices we carry every day. Secured e banking on the mobile is the latest issue for all mobile users.

In this paper authors have focused on, how biometric mechanism provides the highest security to the mobile payment. The present security issues surround the loss of personal information through the theft of the cell phone.

The use of biometrics has been virtually eliminated the possibility of someone gaining access to a third party cell phone directly. It is therefore important that the biometric identification templates are not certainly stored on the phone but will gather at run time. A man in middle attacking at WAP gateway is a great concern. So for securing the biometric identification template on the WAP gateway from client (mobile) to server (host server) RSA algorithm will provide the enhanced security at transmission level. The current paper presents the proposed biometrics mechanism to secure the mobile payment also provides the security at the wireless transmission level. Biometrically secured mobile payment system is much safe and secure and very easy to use, also no need to remember passwords and secret codes. Mobile payment is used for banking and various M-commerce applications. Here authors are using the Android mobile for taking the real time fingerprint image for login the Mobile Banking Application. The main research focus on the feature extraction from the runtime fingerprint image on the Android mobile and send to the server for authentication. A newly proposed Fuzzy Logic Based fingerprint matching algorithms will be implemented at the server side.

Keywords— Biometric security, Mobile banking, Mobile Payment, Android, M-commerce

I. INTRODUCTION

The online banking transactions are part of daily routine for an individual. The existing online banking system has several drawbacks. Firstly hacking, from the internet any one can hack the username and password and the result is third person gets access to owner account. As anyone is not with twenty four hours on the Internet, i.e. access bank website, it takes some time to know that your account get hacked and third one can get transfer the money to his own account. Secondly, every time one has to carry laptop or PC with you. So for this issue secured payment applications on mobile device i.e. M-commerce is proposed.

Today is the era of mobile, everyone having the mobile in his hands, instead of using the laptop or PC, mobile is the best option to use for the banking purpose. The next generation of banking applications won't be on desktops or mainframes but on the small mobile devices we carry every day. Secured e-banking on the mobile is the latest issue for all mobile users. M-commerce, in the context, provides a lot of services like Mobile ticketing, Mobile banking, Mobile location based services, Mobile auctions, Mobile purchasing and so on. This represents an incredible opportunity to enable mobile devices, as universal devices for mobile commerce applications.

Existing smart phones in market an open, programmable software framework is vulnerable to typical smart phone attacks. Such attack can make the phone partially or fully unusable and cause unwanted SMS/MMS billing. The statistics shows [1,2] online transactions are hacked. To

avoid the general device attack, authors have used the Android mobile for the payment application. Android has software stack based on the Linux Kernel and it contains the Android Native libraries [3]. Android is a very powerful device. As it has in-built libraries, and top level security mechanism to secure the rich application [4]. It also includes the Image processing library that can be used for the processing input images.

PDA's and cell phones these days come with fingerprint scanners for authentication and transactions. There are various methods to take the runtime fingerprint. Android has the in-built fingerprint scanner. It is also possible to install the fingerprint scanner software to the android device, and take the fingerprint at run time. Even if biometrics mobile is not available, the camera with high megapixel can take the picture and can be processed further for the secured banking in android based mobile device. Here mobile digital camera is used to capture the fingerprint image. Fingerprint is a powerful mechanism in biometric authentication. So here the payment application is secured on all the ways, i.e. it uses the secure device, biometric security mechanism to open the payment application and wireless channel security.

II. LITERATURE REVIEW

In a core banking system, there is a chance of encountering forged signature for transaction. And in the net banking system, the password of customer may be hacked and misused. Thus security is still a challenge in these applications. There are many techniques to secure the customer information and to prevent the possible forgery of signatures and password hacking [2]. Still there are some problems. Today, single factor authentication, e.g. Passwords, is no longer considered secure in the internet and banking world. Easy-to-guess passwords, such as names and age, are easily discovered by automated password-collecting programs. Two factor authentications have recently been introduced to meet the demand of organizations for providing stronger authentication options to its users. In most cases, a hardware token is given to each user for each account. The increasing number of carried tokens and the cost of the manufacturing and maintaining them is becoming a burden on both the client and organization [5]. A biometric technology makes sense for E-payment. In today's world, no one needs pockets. That stuff jingling around in their keys, credit cards, checkbooks are replaced by something closer to the body. When you need to open a door or make a purchase, technology allows anyone to do so with a fingerprint, a voice command, or a computer scan of eyeball. A new approach to the fingerprint payment technology i.e. using

biometric technology with E-payment is perfect because it won't just identify, but it will authenticate as well. Dilip Kumar and Yeonseung Ryu have suggested to use fingerprint for operating ATMs, here in state of using the card, fingerprint gets used for transaction [6]. The drawback/missing part in this paper is that it was for ATM banking and not for a handy operation with mobile or iPod dependent operation.

Secondly Dr. Suresh Sankaranarayanan has worked on biometric mobile but these mobiles are still very expensive in the market hence technology cannot be available for common man, biometric scanner is used to take the fingerprint for the authentication on mobile device [7].

The authors have tried to simplify the process by using any mobile having 3 megapixel cameras. The same concept has been explored in this paper in next few sections. Section III talks about the suggested methodology. Section IV presents proposed plan for secure payment on mobile. Section V is the concluding section.

III. METHODOLOGY

A. Biometric Authentication

Since biometrics operation is a very common application for identification. Worldwide many have worked in the similar area. Biometrics identify people by measuring some aspect of individual anatomy or physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioural characteristic (such as your handwritten signature), or something that is a mix of the two (such as your voice) [6]. Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today and are already in use [6],[8]. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the context, a biometric system may operate either in verification mode or identification mode.

1) Verification mode:

In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not. Identity verification is typically used for positive

recognition, where the aim is to prevent multiple people from using the same identity [9].

2) Identification mode:

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an Identity.

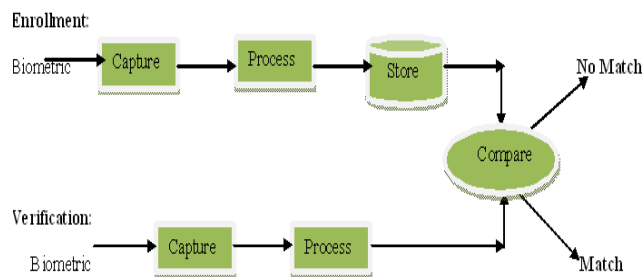


Figure 1: Biometric Enrollment and Verification Process

3) Fingerprints:

In order to be used for recognizing a person, the human trait needs to be unique and not subject to change. Fingerprints, for example, have been used for over one hundred years and, therefore, are generally well accepted as a recognition technology. Other technologies such as face, hand geometry, speaker and iris recognition are also generally accepted. Fingerprints are important. This biometric technology uses the pattern of friction ridges and valleys on an individual's fingertips. These patterns are considered unique to a specific individual. The same fingers of identical twins will also differ. A user does not need to type passwords - instead, only a touch to a fingerprint device provides almost instant access (typically less than 1 sec.). A typical enrollment identifier may include 2 finger samples (e.g., 1 KB) although smaller finger samples are also used. One of the challenges of fingerprint technology is individuals that have poorly defined (or tenuous) ridges in their fingerprints [6],[8]. Since the proposed designed application does not have mobile with scanner, a digital image captured through its 3 pixel camera is being processed for authentication of an individual. Here 3 mega pixel mobile digital cameras are to be used to capture fingerprint images. Images captured with digital camera are distortion free since these images are free from the pressure of contact. Furthermore those images are free from the problems in terms of hygienic, maintenance,

latent fingerprint problem and so forth. There are some challenging problems when developing a fingerprint recognition system that uses the digital camera. The contrast between the ridges and the valleys in fingerprint images obtained with the digital camera, the depth of the field of the camera is small thus some part of the fingerprint regions are in focus but some parts are out of focus, and lastly motion blur in the image acquired[10].

4) Feature Extraction :

A generic fingerprint authentication system consists of two parts: enrolment and verification. In enrolment, the collected raw fingerprint image is pre processed, and the features are extracted and stored. In verification the similarity between the enrolled fingerprint features and the features computed from the input fingerprint is examined. Pre-processing is an important step prior to fingerprint feature extraction. The generic process of pre-processing encompasses segmentation, enhancement, and core point detection. Here the captured fingerprint image is in RGB format is first converted to gray scale. This gray scale image is input to the normalization process. Fingerprint segmentation is necessary to eliminate the undesired background and reduce the size of the input data. As this is the image captured by digital camera it is difficult to find the minutiae, so contour technique is used to find the region of interest, and then apply the Core point detection method. Usually mobiles are having the digital camera, so to secure the mobile payment by using biometric mechanisms captured by digital camera will be more efficient.

B. Secured Transaction

Here authors prefer Android mobile for secure payment application. The mobile phone landscape changed last year with the introduction of smart phones running Android, a platform marketed by Google. Android phones are the first credible threat to the iPhone market. Not only did Google target the same consumers as iPhone, it also aimed to win the hearts and minds of mobile application developers. On the basis of market share and the number of available apps, Android is a success.

Android is an application execution environment for mobile devices. It includes an operating system, application framework, and core applications. The Android software stack is built on the *Linux kernel*, which is used for its device drivers, memory management, process management, and networking. The next level up contains the *Android native libraries*. Various system components in the upper layers use these libraries, which are written in C/C++. Incorporating

these libraries in Android applications is achieved via Java Native interfaces. William Enck and his colleagues discussed the main components of an Android application and how to use an Android-specific mechanism to protect Android applications. In general, several security mechanisms are incorporated into the Android framework. We can cluster them into three general groups: Linux mechanisms, environmental features, and Android specific mechanisms.

C. FUZZY LOGIC

Fuzzy logic is a form of many-valued logic, it deals with reasoning that is approximate rather than fixed and exact.

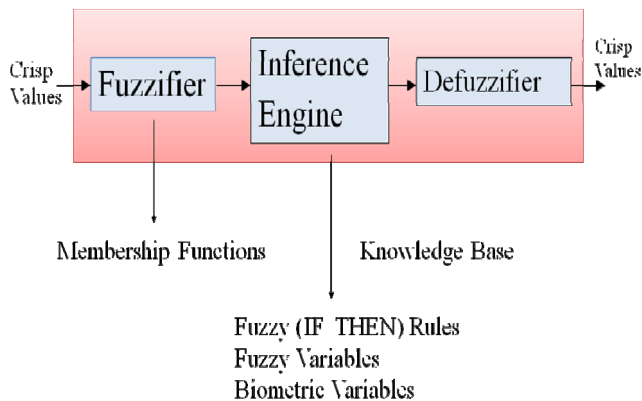


Figure 2: Structure of Fuzzy Logic Controller

A fuzzy logic controller consists of three main operations: Fuzzification, Inference Engine and Defuzzification. The input sensory (crisp or biometric) data are fed into fuzzy logic rule based system where physical quantities are represented into biometric variables with appropriate membership functions.

These biometric variables are then used in the antecedents (IF-Part) of a set of fuzzy “IF-THEN” rules within an inference engine to result in a new set of fuzzy biometric variables or consequent (THEN-Part). Fuzzy logic controller will be design at the server side, Server database contain the extracted features, and controller efficiently match the features of runtime image with the server database.

IV. PROPOSED SECURED FINGERPRINT PAYMENT SYSTEM

The solution involves the use a biometric authentication mechanism. A payment application would be installed onto a android device, for authentication finger print is taken at run time. The finger print template would be captured by the

phone and compared against a stored template on a database server.

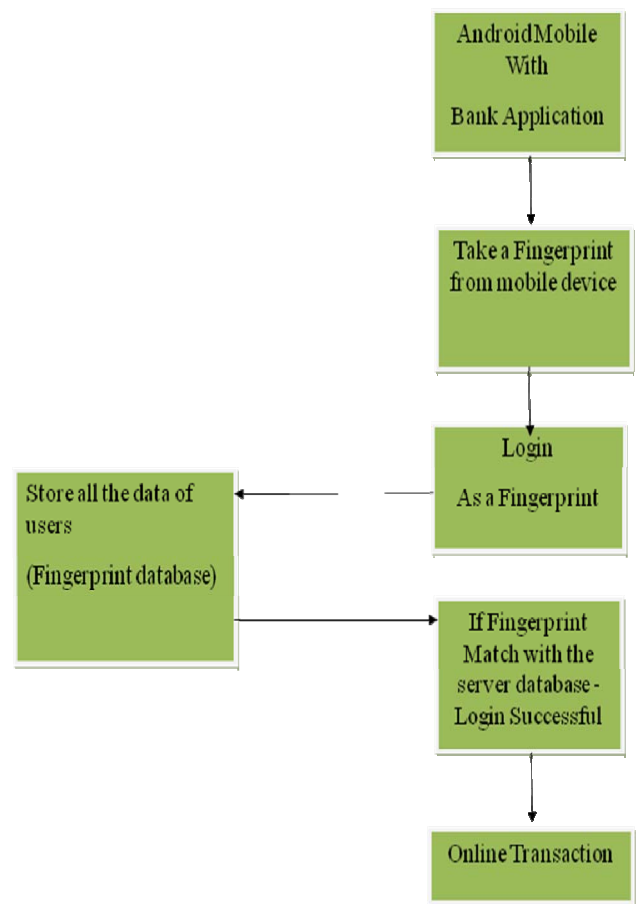


Figure 3: Flowchart of Secured Mobile Payment

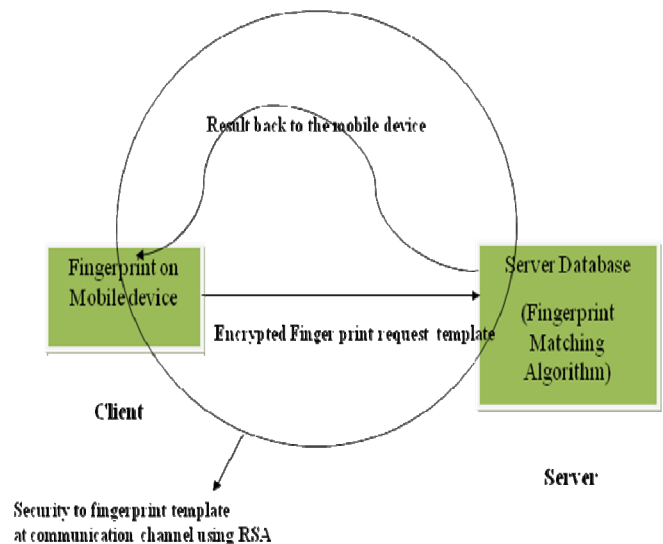


Figure 4: Enhanced security at the client server wireless communication

The fingerprint template is encrypted by using the RSA algorithms and sends it to the host server (i.e. Bank). Fingerprint is used for the login purpose for the bank application on mobile.

Mobile will act as a client and the bank website will act as a server (host server). Once fingerprint is taken as a login, it sent to the server for matching as request, and server send the reply message. If it is matching then only login will be successful and user can do the transaction. In the client server module for providing the enhanced security authors use the encryption technique so at the wireless transmission no one can hack the fingerprint template, as shown in fig. 4.

V. CONCLUSION

The design approach for a Biometric Mechanism for enhanced Security of Online Transaction on Android system has been proposed. Here run time fingerprint would be captured for mobile transaction; it is not stored already in the mobile device so it provides more security and not stolen by third party. Authentication request and reply are in the encrypted form. This gives the better level of security mechanism for mobile payment system. The proposed system can be used in mobile banking and M-commerce.

The Proposed system is under implementation, result will be shown in the next version of the paper.

REFERENCES:

- [1] Han-Na You, Jae-Sik Lee, Jung-Jae Kim, Moon-Seog Jun, "A study on the two-channel authentication method which provides two-way authentication in the Internet banking environment"
- [2] Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik (2008) "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications"
- [3] Asaf Shabtai, Yuval Fledel, Uri Kanonov, Yuval Elovici, Shlomi Dolev (2010), "Google Android: A Comprehensive Security Assessment." *IEEE security and Privacy*.
- [4] Machigar Ongtang, Stephen McLaughlin, William Enck and Patrick McDaniel (2009) "Semantically Rich Application-Centric Security in Android", Annual Computer Security Applications Conference.
- [5] Fadi Aloul, Syed Zahidi, Wassim El-Hajj (2009) "Two Factor Authentication Using Mobile Phones"
- [6] Dilip Kumar, Yeonseung Ryu, "A Brief Introduction of Biometrics and fingerprint Payment Technology", Published by the IEEE Computer Society, 2008.
- [7] Dr Suresh Sankaranarayanan, "Biometric Security Mechanism in mobile

Payment", Published by the IEEE Computer Society, 2010.

- [8] Fernando L. Podio, "Personal Authentication through Biometric Technology", National Institute of Standards and Technology, Gaithersburg.
- [9] L. O'Gorman, "Seven Issues With Human Authentication Technologies", Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), pp. 185-186, Tarrytown, New York, March 2002.
- [10] B Y Hiew, Andrew BJ Teoh and David CL Ngo, (2006) "Preprocessing of Fingerprint Images Captured with a Digital Camera", IEEE, ICARVC.

Additional References:

- [11] Ross Anderson's: "Chapter 13th Biometrics of Security Engineering".
- [12] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" *IEEE Transactions on Circuits and Systems for Video Technology*, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
- [13] Salil Prabhakar, Anil Jain: "Fingerprint Identification".
- [14] Dileep Kumar, Dr. Yeonseung Ryu, Dr. Dongseop Kwon: "A Survey on Biometric Fingerprints: The Cardless Payment System" *IEEE ISBAST* April, 2008.
- [15] Black Hat (2009), "MOBILE APPLICATION SECURITY ON ANDROID" *Context on Android security*.
- [16] Nicolai Kuntze, Roland Rieke (2010) "Secure mobile business information processing", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.