International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

BIOMETRIC MECHANISM FOR ENHANCED SECURITY OF ONLINE TRANSACTION IN ANDROID SYSTEM:A DESIGN APPROACH

A.Ragavan[1],J.Saranya[2],S.Sindhu[3]
[1]*Assistant Professor,Information Technology, S.K.P Engineering College*
[2,3] *InformationTechnology, S.K.P Engineering College*

Abstract:The next generation of banking application 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 focussed 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 cellphone 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 to server ,RSA algorithm will provide the enhanced security at transmission level.The current paper presents the proposed biometric mechanism 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,alsono 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 realtime fingerprint image for login the mobile banking application.The main research focus on the feature extraction from the runtime fingerprint image in the android mobile and send to the server for authentication.Anewly 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 transaction are part of daily routine for an individual.The existing online banking system has several drawbacks.Firstlyhacking,from the internet any one can hack the username and password and the result is third person get 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 transferthe money to his own account.Secondly, every time one has to carry laptop or PC with you.So for this issue secured payment applicatons on mobile device.i.e., M-commerce is proposed.

Today is the era of mobile,everyone having the mobile in hands,instead of using the laptop or PC,mobile is the best option to use for the banking purpose.The next generation of banking application wont be on desktops or mainframes but on the small mobile devices we carry every day.Mobile banking mobile location based services,mobile purchasing and so on.This represents an incredible opportunity to enable mobile devices,an universal devices for mobile commerce applications.

Existing smart phones in market is a 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.To avoid the general device attack,authors have used the android mobile for the payment application.Android has software stack basedon the linux kernel and it contain the Android Native Libraries.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 is having the inbuilt fingerprint scanner.It is also possible to install the fingerprint in runtime.Even if biometric mobile is not available,the camera with high mega pixel 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 in all the ways.

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.Today,single factor authentication ,eg., passwords is no longer considered as secured 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 organiztions 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 manufacturing and maintaining them is becoming a burden on both the client and organization.A biometric technology makes sense for E-payment.In today's world no one need pockets.Thatstuff jingling around in there keys,creditcards,checkbooks and 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 wont just identify,but it will authenticate as well.DilipKumaatm banking and andYeonsungRyu have suggested to use fingerprint for transaction.The drawback in this paper was for ATM banking and not for handy operations with mobile or iPod dependent operations.

Secondly,Dr.SureshSankaranarayanan has worked on biometric mobile but these mobiles still are very expensive the market.Hence technology cannot be available for common man,biometricscanneris used to take the fingerprint for the authentication on mobile device.

III. METHODOLOGY:

A.BIOMETRIC AUTHENTICATION:

Enter biometrics operation is 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 of the two (such as your voice). Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today and are already in use.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 method:

In the verification mode,the system validates a person's identity by comparing the captured biometric data with her own biometric template stored 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

positiverecognition, where the aim is to prevent multiple people from using the same identity.

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.

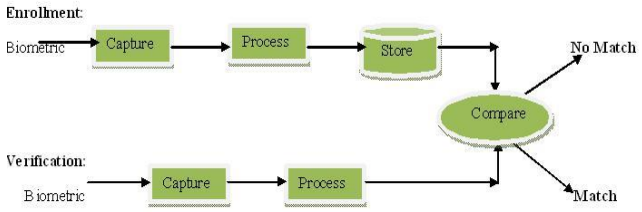

Figure 1: Biometric Enrollment and Verification Process

3)Fingerprints:

Inorder to be used for recognizing a person ,the human trait needs to be unique and not subject to change.Fingerprints, for eg., 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 h ave mobile with scanner, a digital image captured throug h its 3 pixel camera is being processed for authentication o f 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.

4)Feature extraction:

A generic fingerprint authentication system consists of two parts i.e., enrollment and verification.Inenrollment,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. Finger print 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 minute, 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 bio metric mechanisms captured by digital camera will be more efficient.

B.SECURED TRANSACTION:

Here authors prefer android mobile for secured payment application.The mobile phone landscape changed a 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 applications 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,applicationframework,and core applications.The android software stack is built on the linux kernel,which is used for its device 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.

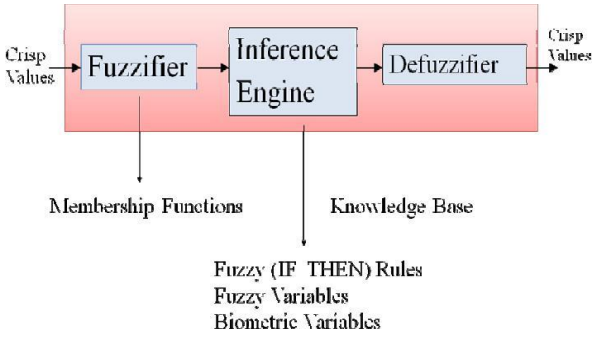

Figure 2: Structure of Fuzzy Logic Controller

A fuzzy logic controller consists of three main operation fuzzification,InterfaceEagine and Defuzzification.The input sensory 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 of a set of fuzzy "IF-THEN" rules within an inference engine to result in a new set of fuzzy biometric variables or consequent 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. PROPSED SECURED FINGERPRINT PAYMENT SYSTEM:

The solution involves the use a biometric authentication mechanism.A payment applications 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.

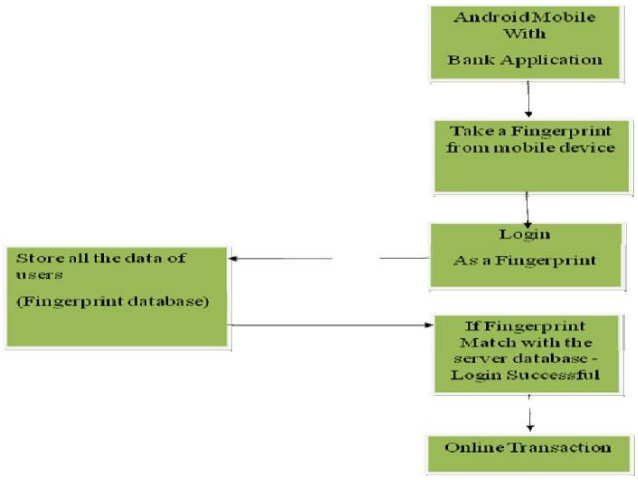

Figure 3: Flowchart of Secured Mobile Payment

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 applicationon 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 enchanced security of online transaction on android system has been proposed.Here run time fingerprint would be captured for mobile transaction.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-SikLee,Jung-Jae Kim,Moon-SeogJun,"A study on the two-channel authentication method which providestwo-way authentication in the Internet banking environment"
2. ChetanaHegde,Manu S,P Deepa Shenoy,Venugopal K R,L M Patnaik(2008)"Secure Authentication using Image Processing and Visual Cryptograhy for Banking Applications".