Design of Improved Algorithm for Mobile Payments Using Biometrics

Jyotsana Goyal[1] and Dinesh Goyal[2]

[1] CSE, Suresh Gyan Vihar University, Jaipur, Rajasthan, India

[2] CSE, Suresh Gyan Vihar University, Jaipur, Rajasthan, India

Abstract

As mobile technology is growing; the payment technology is also growing with it, which enables end-to-end payment processing system in context of daily routine transactions or associated business (sales) transactions. It offers enormous flexibility to customers as to pay their bills anytime and anywhere without having the need to go outside.

But inspite of all the benefits mobile payments are not very common since everyone does not possess a phone with such capabilities. Also with the ease of m-payments comes the issue of security, especially, authentication issue. Thus, we will be designing such a mobile payment system integrated with biometric authentication model which will provide the facility of mobile payments with increased security levels and that it would enable more and more people to use mobile payment system even with the simplest mobile phones.

Keywords: M-payments, authentication, biometrics.

1. Introduction

India is the world's second largest telecom market, with 929.37 million mobile phone users. Phone is quite common, even in remote villages. Mobile phone industry is growing at an annual rate of more than 2 million visitors annually. It is expected to reach 1 billion in 2013 to mark. Urban users share was 66%, while the share of rural users was 34%. In May 2011, the monthly increase in the number of users in terms of a net 13.35 million. The 13.35 million new subscribers, 7.33 million people from urban and rural parts of Section 6.02 million. Subscribe monthly growth rate of 55% of the urban segment, while the rural part of the 45% [6]. Given such a background, the phone can be considered as an economically viable tool that enables include access to financial services.

With the increasing mobile technology, mobile payment system has paved its way in to people's life. But still not a large portion of people use mobile payment system mainly for two reasons. Firstly, still people in India have a question about the security of their payments made online. While the second reason is, that not all people possess smart phones hat support the mobile payment facility.

2. M-Payments

Mobile payment, also known as mobile money, mobile money transfer and mobile wallet generally means the financial supervision and implementation of payment services from or through a mobile device. Besides by cash, check or credit card, consumers can use the phone to pay for a variety of services and digital or hard goods.

The mobile device may include a mobile phone, PDA, wireless tablets, and any other device may be connected to the mobile telecommunications network to make payments.

Mobile technology landscape offers various possibilities to realize M-payment. SMS, USSD or WAP / GPRS are the three possible channels through which a GSM phone can send or receive information (mobile data services). Selection of the channel will affect the way mobile payment program implementation. Second, mobile payment client application may reside on the phone, or it may reside in a subscriber identity module (SIM).

Fig. 1 Various possibilities using m-payments

For any mobile payment system to be widely accepted must overcome some of the key challenges like interoperability, usability, simplicity, universality, security, confidentiality, cost, speed, and cross-border payments. [1] In all of these challenges security is the most critical one and authentication is the main area of concern when talking about security in m-payments.

Authentication means verifying that the user is who that he claims to be. Authentication can be carried in the three ways.

- The first method is by using a PIN (Personal Identification Number) or password which is a secret knowledge based technique. This technique is commonly used as it provides cheap and quick authentication.
- The second method is using the token- based technique or SIM (Subscriber Identification Module). In this technique, user removes the SIM from the mobile phone when not in use. But this is an inconvenient manner. Moreover, Payment systems that are based on the passwords and tokens are easily misused, due to the shortcomings (Forgotten, lost, copied, shared, distributed).
- The last method is the application of biometric technique. In this technique, the unique characteristic of a person is used for the purpose of identification and verification of individual, since each individual possesses the human characteristics that are unique with himself only.

3. Biometrics

(Nanavati et al., 2002, p. 9)[2] define biometrics as the "automated use of physiological or behavioural characteristics to determine or verify identity." A more detailed definition is given by (Bolle et al., 2004, p. 3)[3] who say:

"Biometrics refers to identifying an individual based on his or her distinguishing characteristics. More precisely, biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioural characteristics".

Biometric methods can be classified into two basic types – behavioural and physiological.

i.) Physiological biometric is based on bodily characteristics, such as fingerprints, iris scanning and facial recognition.

ii.) Behavioural biometric is based on the way people do things, such as keystroke dynamics, mouse movement and speech recognition.

Various types of biometric techniques are Facial Recognition [10], Fingerprint Identification [11], Retinal Pattern Recognition [12], Iris Based Identification [12], Voice Recognition or speech recognition [13][14] and Signature Recognition [13][14].

3.1 Fingerprint Identification

Fingerprint verification is the earliest biometric to be used and the first computer-aided personal identification system (O'Gorman, 1999)[4]. It functions by reading the pattern on the upper third of the finger. This pattern is made up of whorls, loops and arches, which are the primary types of fingerprints.

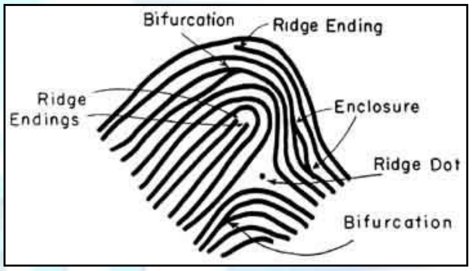

Fig. 2 Minutiae example [7]

Basically the fingerprints consist of ridges (raised skin) and furrows (lower skin) that are twisted to form a unique pattern, which uniquely identifies the fingerprints. Although the flow of the ridge are unique and distinctive, while the other characteristics of the fingerprint called "minutiae", is the most unique to the individuals (see Fig. 2 represents several details). These features are specific patterns of terminal or ridge bifurcation. In addition, all fingerprints can be classified into three categories based on their major central pattern [7]. These categories are arch, loop, and the thread, which is shown in Fig. 3.

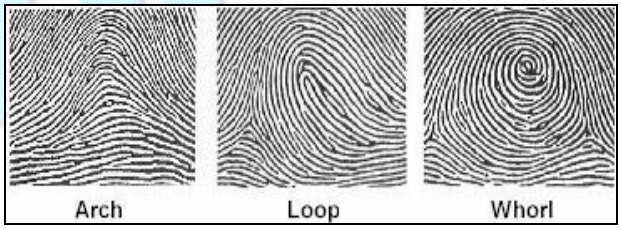

Fig. 3 Three major fingerprint classifiers [7]

Fingerprint matching techniques can be divided into two categories: minutiae-based and correlation-based. Minutiae-based technique first finds out the details using minutiae points, and then maps the fingers of their relative position. However, there are some problems when using this method. It is difficult to accurately extract minutiae if fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. Based on the difficulties associated with the minutiae-based method, correlation-based method is used to overcome its difficulties. However, it has some of its own shortcomings. This technology requires precise position of the registration point, and is affected by the image translation and rotation, as shown in Fig. 4 [8].

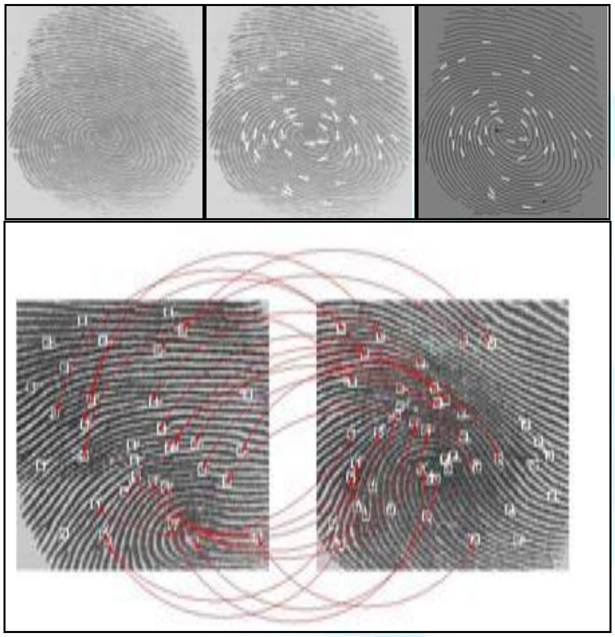

Fig. 4 Fingerprint matching

3. Related Work

Vibha Kaw Raina (2011) proposed an idea to integrate the proposed payment model with multi server authentication model for the purpose of maintaining security and accessing different servers (websites). The author proposed a multi-model biometric authentication procedure with respect to the payment system and has integrated it with the existing payment system.

Kanaan A. El Bhissy (2011) proposed a payment system for mobile phones for the people of Palestine. Author has designed and programmed the speaker-verification system, which does not depend on the text, i.e. that the system can verify the speaker regardless of the phrase pronounced. System works entirely on a mobile phone to pick up the sound, and analyze it to extract the characteristics of the vocal tract, then the verification process, which compares the extracted speech's features with the stored vocal model audio of the speaker, which can be modified when necessary.

Shiny Sreekumar (2010) dealt with the issue of authentication in m-Payments and how this could be realized using biometrics with the goal of developing a viable business model. A special focus is given to the process of enrolment as it forms the basis for an accurate authentication process, as well as to customer acceptance: without which the application will not be successful.

Uludag et al. (2004) defined biometric technology as an automated method Recognition based on behavioral or physiological characteristics of people. These Features include features such as a hand, hand, face, fingerprint, vein, voice, retina, iris. The authors concluded that biometric technology is the key to a wide range of highly secure identification and personal verification solutions arrays. Welzl (2004) pointed out that the biometric system is a pattern recognition technology to enable individuals to identify an individual by determining the user has a specific physiological or behavioral characteristic of authenticity.

Jain et al. (2003), has described the significant difference between the physiological and behavioural biometric characteristics. Physiological biometrics data gathered by the measurement part, and direct measurement of the human body. These samples include, but on the other hand, behavior characteristics originated from the individual actions, which indirectly measuring the unique characteristics of the human body is not limited to hand geometry, face recognition, fingerprint, iris scan. These samples include, but are not limited to, the signature scanning, the scan key, speech recognition. Time can be used as a measure of behavioural characteristics, as it passes through the process of considering a given (behavior Shoniregun, 2003 year schedule measures; Strasser et al, 2001; Putte and Keuning, 2000).

Jain and Uludag (2003), and Soutar (2002), which includes noted that an ideal biometric system should be universal, unique, permanent and collection value. It must be universal, everyone has the characteristics and unique, no two people share the characteristics and permanent; where the characteristic should neither be changed nor is variable, the final characteristics must be recovered , and at any decent sensor , and easy to quantify (Uludag, et al, 2004). Some other studies have found to meet all the above requirements may be impractical or characteristic of a useful practical biometric identification system (Linnartz and Tuylus, 2003).

Schneier (1999) and Timmers (2000) in their study showed that biometric technology is integrated into applications using proprietary software developers kit (SDK 's) reach. However, a recent study concluded that a standardized biometric application programming interface, BioAPI phase, was set up in the Specification, version 1.1, released in 2001, in order to enhance the portability of internal application-independent biometric technology (Suter, 2002; Jain and Uludag , 2003; Adler, 2004) .

Biometrics -based identity verification applications are many functions vital to global economic growth contained. These measures include, but are not limited to, single sign-on, Web security, transaction security, application logins, data protection , workstations , remote access to resources, and so on. (Maltoni, 2003).

4. Methodology

In this section we have described our proposed algorithm of biometric authenticated payment system designed especially for implementing m-payments. Since our model will be typically based on biometric authentication and we have used fingerprint (thumb impression) biometric.

4.1 Biometric Authentication Process

The biometric authentication process consists of two phases– Enrollment process and Verification process.

i.) *Enrollment Process*
Enrollment relates to the process of registering the fingerprints of a customer against their other demographic data as a record of their biometric identity. It will be a one-time process in which a customer will be asked to present their fingers on a scanner and the fingerprints will be recorded and stored.

ii.) *Verification Process*
The verification process involves the customer verifying their identity through a live fingerprint to authenticate a payment. This process will be carried out every time the customer is carrying out a payment. In verification process the customer will enter their customer identity number into the verification system. The system will then prompt the customer to present their live fingerprint on the scanner. The live fingerprint will be then compared with the biometric template stored against the customer identity number in the biometric server.
In case the verification is successful the payment transaction will be considered authenticated and the transaction will be sent to the bank for processing.
In case of a failure the customer may be asked to present the finger again up to a certain maximum number of tries.

In order to implement a biometric authenticated payment system we will require three primary system elements that are put in place by a bank or acquirer. These are:

i.) *Enrollment system:* This system will be used for enrollment of the customers on to the program and recording their fingerprint identity.

ii.) *Verification system:* This system will be used at retail locations for verification of the live fingerprints with the stored fingerprints for authenticating the payments.

iii.) *Biometric server:* This system will be used for storing the fingerprints, extracting and verifying fingerprints during a payment process and providing an interface to banks and acquirers for managing the customer data and reports.[5]

4.2 Components Required For Biometric Payment System

The different components that will be required for the biometric payment systems are:

i.) *Secure Online Banking Server (SBS):* It will have access to customer's data; establish connection with the Online Banking Software (OBS); conduct capital transactions and will be able to identify a Biometric Trusted Device (BTD) as a communication partner to establish a secure connection.

ii.) *Online Banking Software (OBS):* It will be stored on the client and will communicate with SBS in order to process different transactions.

Our model will be having three levels of security for authentication of the user. [9]
The first step in the proposed model will be to check the first level of security i.e. in the form of account number and password. After entering the account number and password the system will check the validity of the user credentials. If the user enters the right account number and password the system will enter into second level of security

otherwise will again ask for the account number and password.

After authenticating the first level the system will ask for the second level of security which will be the biometric template of the user. The system will verify the biometric template of the user with the stored biometric template in the database. If the user enters the valid biometric template then the system will enter the third level of security i.e. registered mobile number.

The system will verify if the biometric template is received from the registered mobile number. Otherwise the system will again ask for the biometric template. After verifying the mobile number, the system will be checking for its validation.

If the validation is right then the system will proceed and enter into the mode of transactions/payments otherwise it will continue asking the valid set of credentials till the loop ends (three times).

a) The first option provided in the model will be to check the current balance of the account holder. By this option the user will be able to check the details of the balance in the account.

b) The second option will be updating of the account.

c) The third option will be for transferring the funds from existing account to another account in any of the banks (money transfer). For this option again the user will have to go through the authentication process.

d) The fourth option will be the payments with the help of mobile wallets. This option will be further having different choices that include payment with Pay Pal, M-check, Obapay, Pay mate. These payment options are useful for P2P transactions providing the facility to do transactions with electronic money. For this option too the user will have to go through the authentication process.

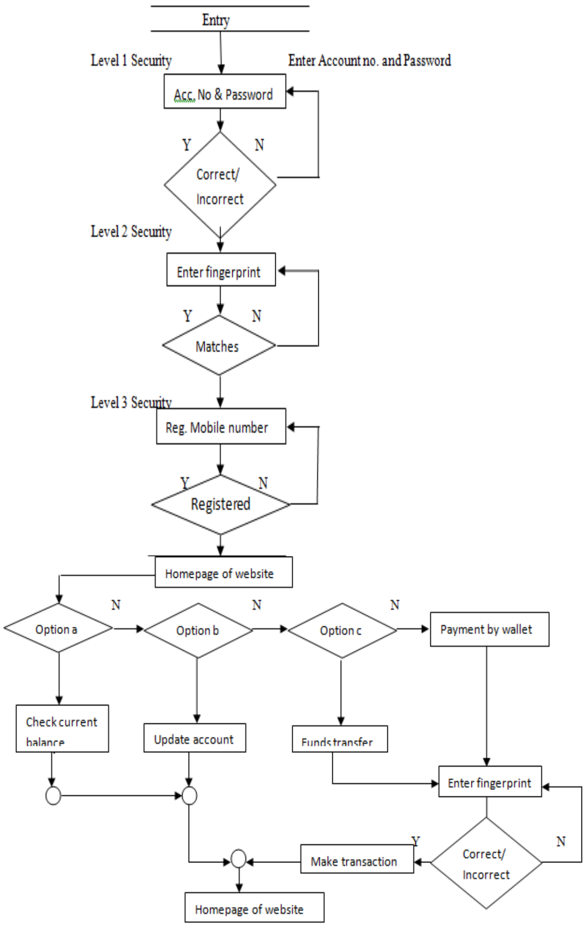

Fig. 5 The flow chart of the proposed model using if then else statement

4. Conclusions & Future Work

In this paper, the biometric payment model incorporates biometric authentication mode at multiple levels. This idea has been developed from a broader perspective to cover the shortcomings of the existing mobile payment system and to provide better security features in mobile payments. The proposed biometric payment model provides the user-friendly approach to trade and make payments from the customer perspective. And multi-level authentication mode provides the user much better security. Moreover, this model provides a payment system for mobile phone that supports the most basic features like a camera in it. Our model is not only for smart phone holders but also for the simple phones with a camera. Thus, this feature of our model will make the mobile payment system acceptable by more and more number of people.

In future this work can also be diversified in the field of mobile payments and implementing other type of biometric technique for authentication purpose. The research in the field of extracting the fingerprint template from the camera image has a great scope in future. Also, there is a great need of a secure system that can be used for encryption of the image or data.

References

[1] Praveen Chandrahas, Deepti Kumar, Ramya Karthik, Timothy Gonsalvis, Ashok Jhunjhunwala and Gaurav Raina "Mobile Payment Architectures for India", National Conference on Communications,2010.

[2] Nanavati, S., Thieme, M., & Nanavati, R. (2002). Biometrics – Identity Verification in a Networked World. New York: John Wiley & Sons, Inc.

[3] Bolle, R., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A.W. (2004). Guide to Biometrics. New York: Springer Verlag.

[4] O'Gorman, L. (1999). Fingerprint Verification. In A. K. Jain, R. Bolle & S. Pankanti (Eds.), Biometrics - Personal Identification in Networked Society (pp. 43-64). Boston: Kluwer Academic Publishers.

[5] Innoviti Simplifying Communications "Online Biometric Authenticated Payment Systems. 2008.

[6] Annual Report, 2009-10, TRAI, Govt. of India.

[7] Dileep Kumar, Dr.Yeonseung Ryu, Dr.Dongseop Kwon: "A Survey on Biometric Fingerprints: The Cardless Payment System" IEEE ISBAST April, 2008.

[8] Salil Prabhakar, Anil Jain: "Fingerprint Identification"

[9] Vibha Kaw Raina: "Integeration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices", December 2011

[10] Yadan Li, Xu Xu. "Revolutionary Information System Application in Biometrics". IEEE International Conference on Networking and Digital Society 2009.

[11] Ashbourn, J., Biometric Methodologies in Biometrics Advanced Identity Verification The Complete Guide, 2002, pp.45-63, Springer, London.

[12] Jain, A., Biometrics, WA: Microsoft Corporation, 2005.
Fernando L. Podio: "Personal Authentication thr1ough Biometric technologies".

[13] 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.