Securing Online Transactions Using Biometrics In Mobile Phone

Miss. Rajeshree Sudhir Thakur[1], Prof. Kirti Kakde[2]

[1]MCA student, YMT College of Management, kharghar, Navi Mumbai.
[2]Assistant Professor, YMT College of Management, kharghar, Navi Mumbai.

Abstract -*Internet shopping is a strong alternative to traditional "go, see, touch and buy" shopping .It has been one of the mostly used facilities of the Internet. Security in online payment systems has been a wide research area among various organizations. Several approaches have been devised for providing security. But, none of the system overcome the weakness in the system. Many online shopping systems serve internet users all around the world and help people to get the products they need with a small effort. This paper proposes a new solution that combines finger print recognition with online credit card transactions. The proposed system is developed with fingerprint recognition, hence is more secure then the existing system because the finger print is unique. Also using this approach there is no need to remember more passwords, your finger is your password[1].*

In today's world ,online shopping using mobile phone is being used widely. Credit cards and Debit cards are used as the currency during e-business and e-Shopping. Due to advancement in technology in the negative side hackers steal, misuse credit card numbers, even though the network has been made secure. In this paper we have proposed a biometric model (fingerprint scanning) that can be embedded in a mobile phone to make e-transactions more secure and the model is very cost effective .

This paper presents the biometrics mechanism which can be used for providing securing to the mobile payment and at the wireless transmission level. Shopping through 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 Android mobile is used for taking the real time fingerprint image for login the Mobile Banking Application. The main research focuses on the feature extraction from the runtime fingerprint image on the Android mobile and send to the server for authentication of an individual. [2]

***Key Words*: Biometric model, Security, Mobile banking, Mobile payment, Android , M-commerce.**

1. INTRODUCTION

Nowadays everyone has a mobile in his hands, instead of using the laptop or PC, mobile is the best option to use for the banking purpose. It is obvious that the next generation of banking applications won't be on desktops or mainframes but on the small mobile or devices that we can carry every day. Secured e-banking on the mobile is the current need for all mobile users . The statistics shows online transactions are hacked most often. In this paper we have focused on, how biometric mechanism provides the highest security to the mobile payment. The present system has various security issues like the loss of personal information through the theft of the cell phone. Hence use of biometrics in mobile phone is needed, i.e. it uses the secure device, biometric security mechanism to open the payment application and wireless browser security, with the aim of systematizing the existing techniques into a big picture that promotes future research. The online banking transactions are just like a part of their daily routine for many people. The existing online banking system has various drawbacks. Firstly, hackers can hack from the internet important details like the username and password and the result is hacker gets access to owner's account. As anyone is not twenty four hours on the Internet, i.e. accessing their bank website. So it takes some time to know that the user's account has been hacked and hacker can g transfer the money to his own account. Secondly, every time one has to carry laptop or PC with them, which is bit difficult. So for this reason secured payment applications on mobile device i.e. Mcommerce is proposed[3].Another reason is that today people need to type in nine-digit passwords everywhere. This leads many of the people using simple passwords and reusing them across multiple services. This, in turn, makes it easier for criminals or hackers to take control of the bank account. Building a smart biometric experience solves the problem of usability and drastically increases the security level.

1.1 Biometrics

Biometrics in general refer to the study of measurable biological characteristics. The word "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Biometrics is used for identification of humans by their characteristics or features. It is also used to identify individuals in groups that are under inspection. A biometric system is a recognition system, which is used for personal identification of an individual. It determines the authenticity of a specific physiological or behavioral characteristic possessed by the user. This method of identification is more preferable over traditional methods like passwords and PIN numbers for various reasons:

- Physical presence of the person to be identified is required at the point of identification.

- Identification based on biometric techniques makes the process of online shopping easy and eliminates the need to remember a password or carry an identity.

Based on the context on which a biometric system works, it can be classified in two system namely an identification system or a verification system .Identification involves identifying an particular individual whereas verification involves confirming or denying a person's claiming the identity. The traditional way of access control include token-based identification systems , such as a passport, driver's license or and knowledge-based identification systems, such as a password or personal identification number. Biometric identifiers are unique to every individuals, hence they are more reliable in verifying identity than token and knowledge-based methods.

1.2 Fingerprints

Human fingerprints have been used for many centuries for personal identification and the matching accuracy using fingerprints has been shown to be very high . Human fingerprints are unique, detailed, difficult to alter, and durable over the life of an individual. Therefore they are suitable as long-term markers of human identity. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The formation of fingerprint is determined during the first seven months of fetal development. Even the fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, the cost of embedding a fingerprint-based biometric in a system (e.g., laptop or computer) has become affordable .Fingerprint analysis is a biometric technique where comparison of scanned image of prints with a database of fingerprints is done. The basic concept of fingerprint is its uniqueness and also the fact that they do not change during a person's life, form the basis for fingerprint analysis. The minute changes in local environment during fetal development determine the uniqueness of the finger print. Therefore, the identical twins which cannot be distinguished by DNA analysis can be differentiated with fingerprint analysis.

2. RESEARCH METHODOLOGY

HOW A BIOMETRICS PROCESS WORKS :

2.1 Verification of the individual:

This is the first step of biometrics . In the verification mode, the system validates an person's identity .Here comparison of the captured biometric data with data stored system database is done. In such a system, an individual who wants to be recognized(for example, Bob) has to claim an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc , and the system then analyse it by conducting a one to one comparison to identify whether the person is true or not. The basic motive is to prevent multiple people from using the same identity and help in achieving security of the system[4].

2.2 Identifying the Individual:

In this step ,the system search the templates of all the user and matches it with the template of an individual. So the system here performs a one-to-many comparison and search an individual's identity .Therefore the person can be identified without claiming his identity [5].

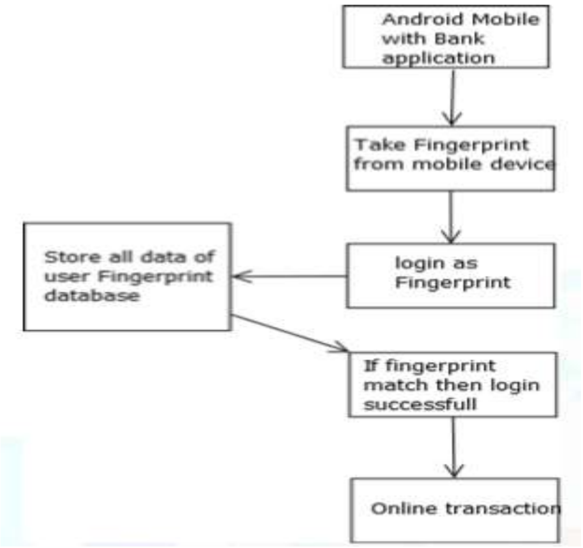
Android Mobile with Bank application
Take Fingerprint from mobile device
login as Fingerprint
Store all data of user Fingerprint database
If fingerprint match then login successfull
Online transaction

Fig-1: Biometric Authentication Process

3.3 Verification using Fingerprints:

For recognition of an individual, the human features should be unique and should not subject to change. Fingerprints have been used for over one hundred years and, therefore, are generally well accepted as a recognition technology. There are many other technologies such as hand geometry, face, speaker and iris recognition which are also generally accepted but fingerprints are important. This biometric technology make use of 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 need not to type the passwords ,instead he has to only touch to a fingerprint device and it provides almost instant access .A typical enrollment identifier includes 2 finger samples (e.g., 1 KB) although smaller finger samples are also used[6].A capacitive scanner can be used to measures your finger electrically. When the individual keep his/her finger on a surface, the ridges in their fingerprints touch the surface whereas the hollows between the ridges stand slightly clear of it. Hence , there are varying distances between each part of your finger and the surface below. A capacitive scanner builds up a picture of your fingerprint by measuring these distances[7].

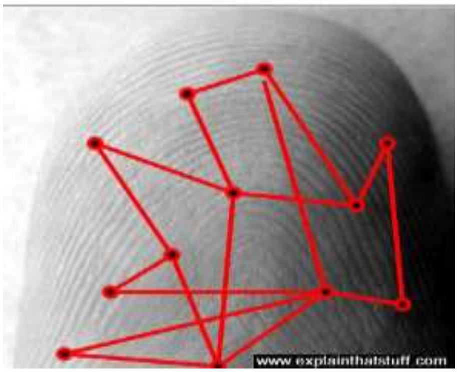

Fig-2: Comparing fingerprints by identifying key features, then measuring the distances and angles between them. Algorithms can turn patterns like this into unique numeric code

4.4 Extraction of Features :

In a generic fingerprint authentication system there are mainly two parts: enrolment and verification. In enrolment, the raw fingerprint image is collected pre processed, and then the features are extracted and stored. In verification the enrolled fingerprint features are compared with the features computed from the input fingerprint to find similarities between them. Preprocessing is an important step prior to fingerprint feature extraction. The generic process of preprocessing includes segmentation, enhancement, and core point detection. Each print is analyzed to find very specific features called minutiae, where the lines in your fingerprint split in two. The computer measures the distances and angles between these features-a bit like drawing lines between them and then uses an algorithm (mathematical process) to turn this information into a unique numeric code. Later, Comparison of fingerprints is done by comparing their unique codes. If the codes match, the prints match, and the person can gain the access.

.

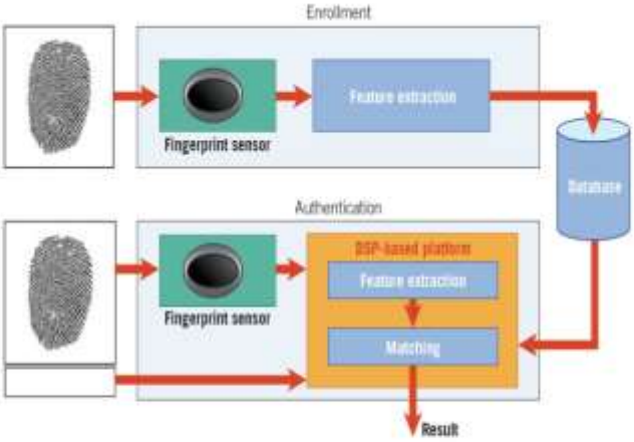

Fig -3: Biometric Enrollment and Verification Process

3. FUTURE MOBILE PHONE

Password protection is an very old technology that was developed for a far simpler digital world. Nowadays this technology has became ineffective against modern hacking arsenals because of various reasons First, passwords are vulnerable to guessing, phishing, brute-force attacks, interception, and large-scale data breaches. Second, passwords are mostly stored in a central location. Finally, other knowledge-based factors such as one-time-passwords and security questions are also not sufficient. So future mobile phone can be developed which uses biometric authentication .This promises to provide a suitably modern replacement for password protection, security questions, and one-time passwords Fingerprint biometric can be adopted widely for access control in places where there is requirement of high level of security such as military bases and laboratories . By attaching a fingerprint scanner to the mobile phone, this biometric could be utilized for phone related security for securing online transaction**.**

Fig -4: Future moblie phone

4. CONCLUSIONS

In this Paper, we study how the mobile phone can be used in biometrics for securing the transaction. This versatile technique(fingerprint scanning) has proven to be a unique and promising participant in the areas of biometrics. Privacy and Security are the two major factors that affect customers trust in electronic transaction. Hence companies , websites or organizations that offer and sell their products or services online should put more efforts for increasing customer's privacy and security. Systems security is a worldwide problem that is affecting private as well as corporate users of IT. Information technology users should be informed and should take responsibility for the security of resources that they are using and building. Accordingly, they should play an active role in protecting their privacy. The design approach for a Biometric Mechanism for enhanced Security of Online Transaction on Android system has been proposed. The Proposed system is under implementation, result will be shown in the next version of the paper. 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 paper concludes that the mobile biometrics can be applied in mobile phone for maintaining security. Phone is cost effective since no special hardware is required and is highly secure. Thus, if this mobile phone becomes a reality, it will provide more secure e-Business and E Transactions [9] .

REFERENCES

[1] Dr. M.Umamaheswari et al. / International Journal of Engineering and Technology

[2] Shuo Wang and Jing Liu , Department of Biomedical Engineering, School of Medicine, Tsinghua University, P. R.China " Biometrics on Mobile Phone "

[3] 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"

[4] L. O'Gorman, "Seven Issues With Human Authentication Technologies", Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), Tarrytown, New York, March 2002.

[5] A.K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, 1999.

[6] Fadi Aloul, Syed Zahidi, Wassim El-Hajj (2009) "Two Factor Authentication Using Mobile Phones".

[7] Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. Springer, 2009.

[8] Han-Na You,Jae-SikLee,Jung-Jae Kim,Moon-SeogJun,"A study on the two-channel authentication method which provides two-way authentication in the Internet banking environment"