Biometric Security Mechanism in Mobile Payments

U.S. Pandey¹ and Geetanjali²
¹Associate Professor, School of Open Learning, Delhi University, Delhi
²Assistant Professor, Maharaja Agrasen Institute Of Management Studies
¹us_pandey@rediffmail.com and ²geetanjalibar@rediffmail.com

ABSTRACT
M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants PDA. Today many people never leave home without their mobile phones. As content delivery over wireless devices becomes faster and scalable, there is wide speculation that m-commerce will surpass wireline e-commerce. 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. At the same time security is the biggest threat in such applications, particularly while paying through the use of Credit card, etc. The dangers of mobile commerce are the same as computer based e-commerce wireless hacks, identity theft and phishing. Phones, however, carry unique security risks like theft, cell Cloning, eavesdrop and man in middle attacks. To secure mobile commerce during payment there are some techniques in vogue like pass codes, pin number of card, identification of serial numbers stored in the sim, signature, etc. But still, these security mechanisms are not that effective, as it is easy to replicate for example one's signature or get the password or pin number. So, we here propose, one more level of security mechanism that could be used viz., the finger print, as fingerprints are one that cannot be replicated.

KEYWORDS
e-commerce, M-commerce, PDA, Cell

1. INTRODUCTION
Mobile commerce (m-commerce) refers to all purchases made using mobile wireless devices such as smart phones and PDAs. Already in countries like Japan cell phones usage is a major purchasing method. Individuals already purchase ring tones, and small applications from manufactures such as apple. Apple online stores serve over thousands of iPhone shoppers. The supporting infrastructure for mobile commerce includes the cell phone handsets and platforms, cell communication technologies, payment gateways, credit clearing houses, banks and merchants. Mobile commerce can be done by using applications that send TEXT-SMS towards a payment or NFC near field communication in which the phone is swiped against a purchasing station. The financial information is sent to a payment gateway which instructs the bank to debit from the buyer's account and to credit the same in the merchant's account. To have a vibrant and viable mobile commerce system, one must satisfy the following requirements viz., Identification, Non-repudiation, Data Integrity and Confidentiality. Many PDAs and cell phones these days come with finger print scanners. Authen Tec and LG have created a cell phone LP3550 which has a biometric scanner for authentication and transactions. Authen Tec has built a generic penny size device which can be embedded into any product requiring biometric authentication. There are two types of biometric authentications which have physical and behavioral characteristics. It is found that finger print is a powerful mechanism in biometric authentication. These finger print authentication systems, however, require more powerful processing power. Also embedded processors which are fast coming up, enhance the processing of finger print processing technique. Java smart card is one that has implemented the finger print as a mechanism for biometric authentication system. Wireless network security protocols and encryption methods are notoriously weak and are easily cracked. It is suggested that m-commerce channels be supported by VPN or public key methods used to share symmetric keys at the start of each session. Symmetric keys are changed at each session. As the processing power of phones and servers increase, so does the number of bits used to encrypt transaction data. Taking these aspects into consideration, we here focus on finger print analysis - biometric Authentication system as a means to identify and authenticate users in the mobile payment. The remainder of the paper is organized as follows. Section 2 talks about Security in Mobile Payment Systems. Section 3 talks about fingerprint analysis in a Mobile Payment system. Section 4 presents the implementation of biometric system in a mobile payment System. Section 5 is the concluding section.

2. SECURITY IN MOBILE PAYMENT SYSTEMS
The present security issues surround the loss of personal information through the theft of the cell phone. The use of biometrics has virtually eliminated the possibility of some one gaining access to a third party cell phone directly. However, if that individual removes the smart card holding the biometric template he could then authenticate himself. It is therefore important that the fingerprint templates are not certainly stored
on the phone. Similarly other authentication information such as logins and passwords should not be stored on the cell phone, but is gathered at run time. The possibility of a man in the middle, attacking at NFC terminals or WAP gateways is of great concern, as these wireless protocols are known to be weak. The WAP gateway provides encryption between the gateway and the client, the gateway has to be authenticated to prevent a fake gateway being placed in a public hotspot by a perpetrator. The analysis of packets could lead to the breaking of symmetric keys and weak passwords or simple determining the structure of information being exchanged between the client, store and the bank. This perpetrator could remove packets, inject packets or adjust packets in order to divert funds, change bank account information or passwords. The client could also get subjected to a phishing scam, providing credit card and personal information to a criminal entity posing as a store. Similarly GSM networks which uses Sims are vulnerable as Sims can be cloned, fake base stations can be used to gather or adjust packet communication. Allowing a third party to begin gathering packets of data exchanged between server and clients is dangerous. It is important that the service provider is authenticated as genuine and that data exchange is strongly encrypted at run time only on the phone Le., communication of data between the server and the user is encrypted before the data leaving the phone.

The possibility of malicious code is greatly minimized due to the need of software programs to be digitally signed and the lack of possibility to dynamically create new or fake certificates. Programs before being installed have to be associated with a certificate already existing on the phone, Le. the manufacturer, the carrier, or a public service such as Thawte, Verisign or the Java Verification Program. However, there is the possibility of WML code conducting malicious activity. WML is browser based, although the site might be verified and possesses an SSL, a perpetrator could install a virus or worm on the server that would send dangerous WML scripts to unsuspecting clients. The best solution to this is to ensure that individuals use reputable software and websites. Security at the server is also paramount; a fraudulent employee could remove or adjust fingerprint templates, passwords or customer information. It is important that public and private keys be held in a secure password protected location on the server. In a situation in which a phone is stolen or lost, passwords and codes could prevent access to your identity or purchase items with your card by unscrupulous individuals. A finger print scanner however, is even more secure; it cannot be lost, shared or easily discovered by a third party. We would now describe in brief about the finger print authentication system

3. SECURED FINGER PRINT BASED MOBILE PAYMENT
Our solution involves the use a biometric authentication mechanism. Our software would be installed onto a device that has a supporting finger print scanner. The finger print template would be captured on the phone and compared against a stored template on a database server. A finger print is unique to any one user and so it cannot be easily duplicated. We do not intend to store any authentication or processing information on the phone. The finger print would be captured and processed at run time only, logins and passwords would be also gathered at run time. The finger print template and authentication Information wi" be transmitted encrypted, via the use of asymmetric keys. A PKI public key infrastructure provides the strongest known method of security. Our approach would ensure an end to end encryption of a" communication between a" parties. Additional finger print templates will never be stored or compared in their raw state. A hash will be created to ensure that a thief will not be able to capture the finger print in its raw form. Similarly finger prints are not stored on the database in their raw form but as hashes. The finger print is never stored on the phone or server to be processed but is directly captured from the scanner, processed and hashed. In short the Biometric security in mobile payment system would perform the payment taking the fingerprint as the basis before revealing the financial information to the shopper for buying.Fig.1 gives the flowchart that gives the process of secured mobile payment. Encrypt template hash and credit card information with public
4. IMPLEMENTATION DETAILS
The implementation of biometric security mechanism is targeted at Java enabled platforms that support CLDC using MIDP forms[9-10]. The tools used include the
• SUN Microsystems Java Wireless Toolkit
• Bouncy Castle Lightweight Cryptography package
The application is intended to be a general purpose application pluggable into any service or business package. It gathers information necessary for the processing of credit card payments at a bank. This information is secured using various encryption methods and a biometric based identification mechanism.
The information collected includes
• First name
• Last name
• Address
• Credit Card Number
• Security Code
• Expiration Date

- Signature - this is an image file which is assumed to be loaded onto the phone by the user or at the bank.
- The finger print is to be scanned using an embedded finger print scanner or an attached device.

During a transaction, the credit card information i.e. the credit card number, security code and expiration date are encrypted using a public key received from the bank. As mentioned the finger print is never stored on the phone but is hashed directly into a class on the device using a SHA digest of 512 block size. The signature is also hashed using SHA of 512. The entire class is then serialized and transmitted to the bank server, where it is reconstructed. The bank server will have the registered information of the customer. The credit card is decoded with the private key and the records located. A hashed copy of the finger print and signature are stored on the server, never the unencrypted images. The finger print hashes from the phone and the server are compared, where there is a 97% match it is assumed that this is the finger print of the client. The signature is treated in a similar fashion. If both finger print, signature match then the purchase is authorized. The system will be further secured with a login and password. The results of the implementation are shown as screenshots in the paper. Fig. 2 shows the user entering personal Information like Name, Address, Credit card, Expiry date. Fig.3 and 4 prompts the user to give signature and biometric i.e. fingerprint Information. Now that the user has entered the information, the finger print information is actually hashed as shown in fig.5 and are submitted to the bank server using public key as shown in Fig.6. The validation of buyer information is performed which is shown in Fig.7. Fig.8 shows the validation of credit card failed as one of the buyer's information entered is wrong. Fig.9 shows the success of credit card validation. Once validated, payment is processed and shopping is done. Figs.10-12 shows the personal information of clients stored which includes the Finger print image and hashed image of finger print too. This information is compared against the buyer's hashed biometric information for validation.
Proceedings of the 5th National Conference; INDIACom-2011

Fig.2- Personal Information

Fig.3- Signature Information

Fig.4- Biometric Information

Fig.5: Hash code - Fingerprint
Biometric Security Mechanism in Mobile Payments

Fig-6: Connecting to Server

Fig-7: Buyer information
Fig-8: Credit card not validated

Fig-9: Credit Card Validated

Fig-10: Personal information- Bank server
CONCLUSION
For such mobile payments, we have been using till now only information like credit card, signature and so on. These security mechanisms are still not secure. So we here have introduced a biometric mechanism- fingerprint that gives a better level of security mechanism for mobile payment systems. We have shown the validation of the biometric implementation through screenshots. In future we propose to interface the fingerprint scanner with the mobile phone for validating too.

REFERENCES