SecureSMSPay: Secure SMS Mobile Payment Model

Hany Harb, Hassan Farahat, and Mohamed Ezz
Systems and Computers Engineering, Faculty of Engineering Al Azhar University
harbhany@yahoo.com, *ezz.mohamed@gmail.com*

Abstract—**In this paper, we introduce a secure Mobile Payment model suitable for macro transactions that compromise cost, simplicity, security, and performance of transaction, with minimum number of cryptography key usages, and less encryption/decryption operations compared to other models. This model can use symmetric and asymmetric cryptography without the need of trusted 3rd parties or even PKI complexity. It is based on SMS as a transport channel which provides the capability to send transactions to payer not to payee; as usually done in most current payment transaction models. The payer receives a secured SMS message (invoice) waiting his/her confirmation (yes/no). Each entity in the payment system payer/payee trusts only his/her bank respectively, so the transaction will always go through trusted nodes. The payer/payee can also use any bank payment instrument (Credit Card, Debit Card, or even Current Account) without revealing confidential data during the payment. This model can be applied on any payment application e.g. e-check, money transfer, e-commerce, and even normal EFTPOS transactions with leverage infrastructure supporting the above mentioned payment applications.**

Key Words- Mobile Payment, Security, SMS

1. Introduction

Current payment trend goes toward a cashless society instead of paper banknotes (paper/coin) cash that will become absolute in the next decades. The Financial Institutions focuses these days to move all payment forms (i.e. transfers, deals, purchases, and bill payments) to electronic form instead of paper form. This revolution in the payment method produced a lot of issues and requirements to make these payment methods convenient and secure. Convention is required to allow fast spreading of these methods in the local domain then the international domain. Many organizations currently established e.g. VISA and Master Card, succeeded to switch purchase transactions to electronic form with international domain, and now this has become a common way of payment. Nowadays, these methods of payment face intensive fraud problems due to low levels of security involved. Fraud figures increased and became a barrier against using this method of payment and most of these organizations had to increase the level of security [1,2] for their payment methods, by reordering the security factor to become the first goal to regain customer satisfaction. Also due to the emergence of mobile technology in the last 10 years and due to its huge popularity, now mobile customers outnumber the banking customers (i.e. every credit/debit card holder have a mobile but not every mobile holder have a credit/debit card). This challenged the financial institution (Banks, Payment Processor) to introduce a payment facility over mobile. Mobile operators introduced a micro payment wallet for their customers. Nowadays, many mobile payments are sponsored by banks, mobile operators, or both. These payments are dependant on using a credit card/charged card with client/kiosk centric model of payment. They use a symmetric and/or asymmetric cryptography to secure the communication between payers and payees, The communication media can be Bluetooth or WiFi. The mobile can be connected using PG (i.e. Payment Gateway that provides payment facility to its merchants, and connected to both the payers' and payees' banks) using Internet through GPRS.

There are three models of payment [3], client centric; where the client has connectivity, while the merchant has no connectivity, and Kiosk centric; where the merchant has connectivity to PG, while the client is only connected to the merchant offline and connected to PG through the merchant's connection. Both models use dual signature mechanism that allows passing through the central entity (not trusted node) signature verified by another entity. The third model is full connectivity; where both client and merchant have connection with the PG, and both can be authenticated directly via the PG (that forwards client's authentication to its issuer, and notifies the acquirer in case of payment success). In our approach we will use the full connectivity model based on the SMS connectivity which is simple and involves a cheap method of connectivity for mobile. Also we will leverage the infrastructure of Banks; since most of them now provide notification and announcement SMS service for their customers' notification.

The outline of the paper is as follows. In section 2, a background will be provided, followed by the related work in section 3 which includes a description of some known results associated with our research. In section 4, our approach which includes a complete list of notations used in our scheme, the operational model, the initial assumptions and the proposed model will be presented. In section 5, a security analysis of the proposed model is discussed, then in section 6 case study applied for one of payment application. The full conclusion is then presented in section 7.

2. Background

2.1. Payment

There are two types of payment methods; exchanging and provisioning. Exchanging is to change coin, money and banknote in terms of the price. Provisioning is to transfer money from one account to another. In this method a third party must be involved. Credit card, debit card, money transfers, and recurring cash are all electronic payments methods. Electronic payments technologies are magnetic stripe card, smartcard, contact less card and mobile handset. Mobile handset based payments are called mobile payments.

2.2. Security

An authentication factor is a piece of information used to authenticate or verify a person's identity for security purposes. Human authentication factors are generally classified into three cases:

- Something the user has (e.g., identity document or card, security token, software token, phone, or cell phone)
- Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN))
- Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier)

Two-factor authentication often a combination of methods is used, e.g., a bankcard and a PIN, in which case the term two-factor authentication is used. Business networks may require users to provide a password and a random number from a security token.

Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. Although this concept can be applied to any transmission, including Television and Radio, by far the most common application is in the verification and trust of signatures.

2.3. SMS Payment

Most of payment using SMS based on premium rate SMS (PRSMS) where Media companies or mobile content merchants running a premium rate service whether use mobile terminated (MT: message send to mobile) or mobile-originated (MO: message send from mobile) SMS billing where customers pay a premium to send a message, and this payment service shared between merchant and operator, and suitable for a specific domain for media (ring tone, games,…) but not general purpose payment, also its faces a lot of attack (e.g. Spoofing, Inbox stuffing, and Message Filtering) [4] dangerous attack is SMS spoofing where attack able to deliver messages to users on a number of different international networks with the sender number manipulated [5]. This type of attack preventing most of payment proposed over SMS.

3. Related Work

A secure account-based payment protocol [6] proposed which is suitable for wireless networks, and employs symmetric key operations which require lower computation at all engaging parties, its applied on merchant centric model but satisfies transaction security properties provided by public key based payment protocols such as SET and iKP, where credit-card information not revealed during transactions which results a security enhancement of the system, but it is not suitable for p2p, and require change in merchant infrastructure for communicate with mobile through Wifi or Bluetooth.

[7] proposes a new security enhancement on smart phone using the Limited used Key generation technique based on the KSL protocol, the implementation adapts and compares two popular PKC systems (RSA and ECC) as a design solution for mobile phone payments security enhancement, its registration and payment protocol so similar [6] but different in involving PKI in the communication between merchant and PG, but this approach will require PKI infrastructure to support communication between PG and merchant.

[8] Developed a secure e-check payment system prototype that doesn't require an e-money institution to act as an intermediary, the system still relies on the existing network infrastructure of credit card or banking institutions for check clearance and settlement, but the e-check transaction comprises three communication sessions: (1) PDA to merchant (via Bluetooth), (2) PDA to bank (via GPRS), and (3) Merchant to bank (via the Internet). All of involved entities should acquire a digital certificate and full PKI infrastructure, also mobile internet connection will added cost over normal transaction, in addition of PKI complexity

[9] An anonymous protocol for a mobile payment system based on a Kiosk Centric Case Mobile Scenario where the customer cannot communicate with the issuer due to absence of Internet access with her mobile device and the costs, and employs a digital signature scheme with message recovery using self-certified public keys that reduces the public space and the communication cost, a portable device equipped with a short range link (such Bluetooth, Infrared or WiFi) should be enough to interact with a vendor machine in order to buy goods

or services in a secure way, but this approach will leak of portability because its used self-certified PKI.

4. Our Approach

4.1. Notations

- {Pr, Pe, PrB, PeB}: the set of payer, payee, payer bank, and payee bank respectively.
- {Pr-Mob, Pe-Mob}: the mobile number of payer, and payee respectively.
- TID: the identity of transaction including time and the date of the transaction.
- OI: order information. OI = {TID, Price, order descriptions).
- Yes/No : the status of transaction approved/rejected.
- {M}X : the message M symmetrically encrypted & MACed with the shared key X.
- Xi: cyclic shift key by i number of bits.
- h(X) : the one-way hash function of the message X.
- MAC(X, K) : Message Authentication Code (MAC) of the message X with the key K.

4.2. Initial Assumption and Registration

The payer and payee banks should at least provide 2-way SMS services, to their customers, with short code (e.g. 4333) number that gives the bank the ability to receive Mobile Originated SMS (also known as MO SMS or interactive SMS) through one of the Mobile Network Operator's SMSC protocol (CIMD, SMPP, or UCP/EMI), that is connected over leased line to the operator using VPN,. The security of this services is out of the scope of this paper.

The customer should have a mobile with WAP and J2ME[10] enabled, credit/debit/current…etc account at one of the national banks. The customer should register at the bank's premises or through secure internet banking service provided by the bank (by entering his mobile No. and selecting charging account). Through one of these channels, the customer will request SMS payment service, and he will receive a couple of things to start the service: first is the. J2ME application to be installed on his mobile through WAP-PUSH or Bluetooth at the bank premises, and second is a one-time secret code (a generated alphanumeric password received through secure internet banking services or sent by secure envelope to customer postal address) to exchange the master key between the customer (J2ME application) and the bank i.e. the master key is generated inside the customer's mobile and sent encrypted under the one-time secret code, to be stored in the mobile's key store protected by an offline PIN. The master key used in SecureSMSPay should be a double length key that was used to generate the cyclic shift session key [8] by applying a separate shift index in each part of the double length key to increase it security than [6]. The next section describes in details how to secure payment transactions using the installed J2ME application and the registered master key.

The proposed model involves a PG (payment gateway) to connect the payer's and the payee's banks. This PG should be attached to one of the national payment networks to leverage its infrastructure and benefit from the strong security applied on the connection to the bank's private network provided for normal credit/debit transactions over ISO8583 standard. The PG will be responsible for routing transactions based on the mobile number. So, it should store all mobile numbers and whether they belong to the payer's or the payee's bank. This association should be established during the customer's registration. It is supposed that the customer is associated to only one bank, and the PG can be employed into one of the national networks that is already connected to all the national banks in the country (e.g. 123 in Egypt, SAMA in KSA).

4.3. Cryptography technique

This section demonstrates the cryptography techniques used in the payment processing model.

The SMS sent between the customer and his/her bank will be secured using 3DES session key generated using cyclic shift technique [6] with applied shift in each part of the master key separately to increase its security.

The proposal involves three types of communications; first, from payers/payees to their banks over mobile operator SMS network and its security that encrypted using session key, second, from the payer's or payee's bank to the mobile operator which is a leased line secured by VPN, and finally, from the payer's bank to the PG, then to the payee's bank over one of the payment networks (banking private network) and it is out of the scope of this paper.

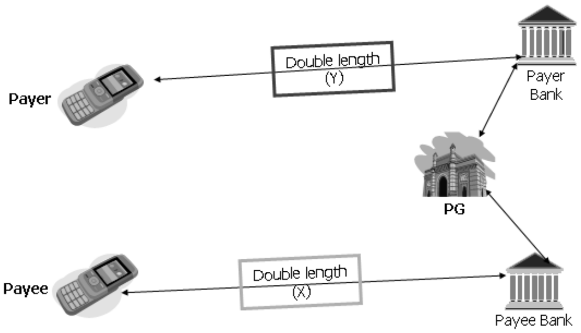

Figure 1

There are only two symmetric keys involved in the proposed model as shown in Figure 1, one key between the payee and his bank, and the other key between payer and his bank, this model is simple, secure and maintainable.

4.4. Proposed Model

The proposed secure payment model is divided into two sections; the request which requires six steps and the response which requires four steps as shown in Figure 2, 3 respectively. The payer started the payment by giving his/her mobile number to the payee as a payment instrument, then the payment request will start as follows:

1. Pe-->PeB : PayReq
   Where PayReq = {Pr-Mob, i, OI} Xi
2. 2- PeB -->PG : Pr-Mob, OI, Pe-Mob
3. 3- PG -->PrB : Pr-Mob, OI, Pe-Mob
4. PG : rout transaction to PrB based on Pr-Mob
5. PrB-->Pr: PayConf
   Where PayConf = {Pe-Mob, j, OI} Yj
6. Get Pr confirmation (Y/N)
7. Pr-->PrB : PayRes
   Where PayRes: {Pe-Mob, Status, TID)} Yj+1
8. PrB -->PG : Pe-Mob, Status, TID
9. PG -->PeB : Status, TID
10. PeB-->Pe : PayNotify
    Where PayNotify= {Status, TID} Xi+1

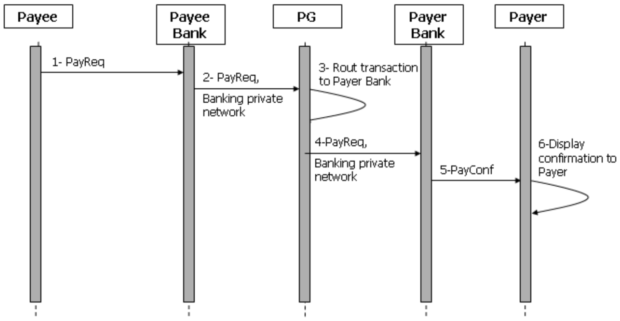

Figure 2

Step 1: The payee will open his/her J2ME payment application and enters his offline PIN to enable the generation of a session key from the protected master key, then he will enter the payer's mobile number and the amount of money to be transferred. The J2ME application will prepare and send the encrypted PayReq SMS using the symmetric session key between the payee and his/her bank.

Step 2: the payee's bank will decrypt the SMS coming from the payee, and then send the Pr-Mob, OI, Pe-Mob to the PG.

Step 3, 4: the PG will check to find the Pr-Mob is associated to which bank, and then rout the transaction to the specified payer's bank.

Step 5: the payer bank will check the balance of the payer charging account, and then send the encrypted PayConf SMS to the payer's mobile using the symmetric session key between the payer and his/her bank asking the payer for confirmation (response with Yes/No).

Step 6: the J2ME application on the payer's mobile will first prompt the payer to enter the offline PIN to generate the session key from the protected master key on the mobile. Then it will use it to decrypt the PayConf SMS and ask the payer for confirmation.

After step 6 is accomplished, the payment response will proceed in the following steps:

Step 7: the J2ME application at the payer's mobile will prepare the PayRes confirmation response [Yes/No] as an encrypted SMS with the next session key between the payer and his/her bank.

Step 8: the payer's bank will decrypt the SMS coming from the payer, then send the Pe-Mob, Status, and TID to the PG.

Step 9: the PG will check to find the Pe-Mob is associated to which bank, and then rout the transaction to the payee's bank.

Step 10: the payee's bank will debit the payee's account then sends the encrypted PayNotify SMS to the payee's mobile using the next symmetric session key between the payee and his/her bank for notification. Then the payee based on the confirmation coming from his/her bank will give the payer the service/goods he/she requested.

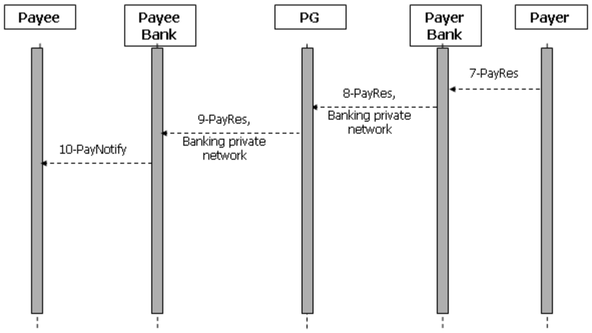

Figure 3

5. Analysis and discussion

5.1. Authentication

In this proposal there are two-factors, the mobile that identifies its owner (customer), and the offline PIN necessary for generation of the symmetric session key that is used during the payment process. So if the mobile is stolen or lost, the second factor (offline PIN) will lock the application after three failed trails, and send SMS to the payer's bank or payee's bank to expire the shared symmetric key.

Authentication in this model is not only applied for payers but also for payees as well. When the payer requests a payment, both banks, payer's and payee's, verify the identity of their customers using the mobile number which sent the SMS and also from the encryption, using the shared secret key between the bank and its customer.

5.2. Confidentiality/Integrity

The confidentiality is satisfied by encryption (using X and Y) between payer/payee and payer's/payee's bank respectively independent on the security applied by mobile operator, on the other hand communication between the banks and the PG is secured under banking private network,.

5.3. Non-Repudiation

Three factors will be used to prove non-repudiation of payers; (1) payer's bank sends PayConf to payer's mobile which responds with PayRes, (2) The PayRes encrypted with a session key that uses random index sent from payer's bank, (3) the offline PIN that is used to generate and send PayRes from the payer's mobile number in case the mobile was stolen or lost

Because we have two type of spoofing (payer and payee's bank spoofing) we proved that both spoofing impossible due to prove that Status (i.e. payer response Y/N) believed by both Pe and PrB by applying Ban Logic[11] for SecureSMSPay payment model.

5.4. SMS spoofing attack

The SecureSMSPay is immune from all types of SMS spoofing even if the symmetric master key (X or Y) was stolen.. There are two types of possible spoofing, payer's spoofing; where the attacker will send a PayRes to the payer's bank to confirm payment to payee, and thus gets the goods/services from the payee who will receive cascaded confirmation from the payer. The second type of spoofing is the payee's bank spoofing where the attacker will send a PayNotify to payee to give the goods/services to attacker. These two types are prevented using random index used in the generation of the cyclic shift session key generated at the payer's bank, and the random index used in the cyclic shift key (j) is sent to the real payer who will send PayRes using (j+1); or generated from payee (i) and sent to real payee bank who will send PayNotify using (i+1).

5.5. Lost/Stolen Payer mobile

If the payer's mobile was lost or stolen, he/she should inform the bank to expire the symmetric master key, but if the payer didn't inform the bank about the lost/stolen mobile, the J2ME application will accept only three trails of offline PIN, and after the fourth failed trail, it will send a remote locking SMS to the payer's bank to expire the symmetric master key, and the payer should go again through the registration process to renew the master session key.

6. Case Study

Cheque payments are the preferred method for medium and high value transactions. Cheques provide the payee an assurance of guaranteed payment as the payments are generally made to the payee's account before goods or services are delivered to the payer.

The Check 21 U.S. federal law [12] became effective on October 2004. The law allows the banks to process cheques faster and more effectively as the paper cheque deposits are converted to an electronic image for processing.

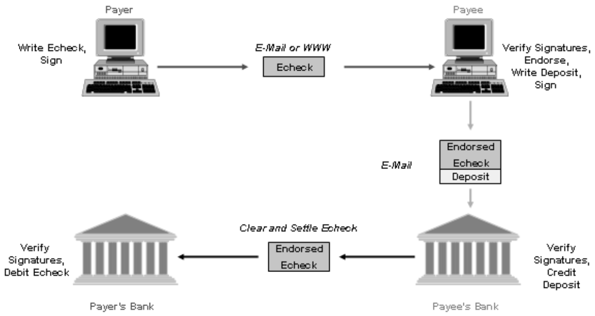

Figure 4

A Payer is an entity registered with the issuer bank, and wishes to issue an e-cheque so as to make a payment to another entity. A Payee is the entity whom the e-cheque is addressed to, based on the payer's instructions. Trusted Third Parties (TTP's) are entities who are implicitly trusted by other entities in an e-cheque system. They include certification authorities for digital signatures, hardware and software manufactures for smart cards and their interfaces, and also public key databases required for the verification of an entity's public key.

Processing Information: At the very least an e-cheque should have the following necessary information for processing: a unique identifying e-cheque number, a unique account number that identifies the payer, a unique issuing bank identifier, e-cheque date and time stamp of when it was drawn, amount and currency of payment, payee's name, and payer's signature.

Figure 4 shows the basic flow of an electronic cheque, where the payee starts the payment process by sending an invoice to the payer, the payer then writes/signs the e-cheque and sends it back to the payee, who verifies it and endorse it, then send it to his/her bank. At the end of day, the payee's bank will clear and settle the e-cheque with the payer's bank. As demonstrated, the cheque should be signed by the payer and verified by the payee, this requires the existing of TTP (CA). Also, the transaction didn't go to payer's bank until the end of the payment process, this lead to some risks; risk of insufficient balance of customers also his is not suitable for certified cheques where the bank holds the amount of money for the cheque before writing it. The proposed payment model as shown in Figure 5, and 6 demonstrates requests and responses involved in the e-cheque payment from the proposed approach's prescriptive.

The payment is initiated from the payee, who sends the invoice number, payer's mobile number, and the amount of money through J2ME application on the mobile, and then the payee's bank sends request for e-cheque to PG with payer's mobile number. The PG will forward the e–cheque request to the payer's bank, then the payer's bank will send confirmation SMS to the payer asking his/her confirmation. Once the payer sends the confirmation SMS through his/her J2ME application, the payer's bank will create an e-cheque and sends it back to the PG which will forward the e-cheque to the payee's bank. The payee's bank will consequently send a notification to the payee to deliver the goods or services to the payer.

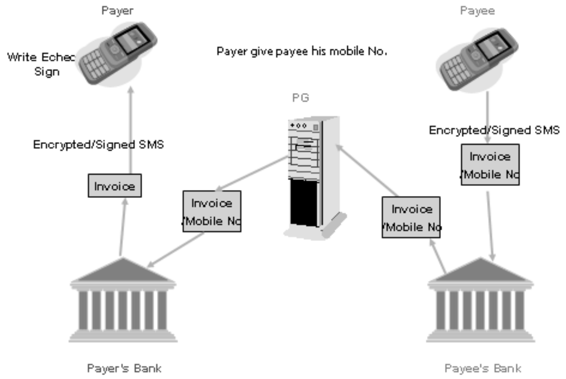

Figure 5

As demonstrated, the proposed payment provides e-cheque with simple and secure way of communication between the payer and the payee without the need of a secure TTP infrastructure (e.g. CA), only symmetric cryptography. Also the proposed model will support certified e-cheque model by default since it goes through the payer's bank which deducts the e-cheque value from the charging account after the payer confirms payment. Also, this will reduce the probability of the out of balance risk and e-cheque disputes because it uses the proposed secure payer confirmation which ensures integrity, authenticity, and non-repudiation. This was proved in the proposal analysis section.

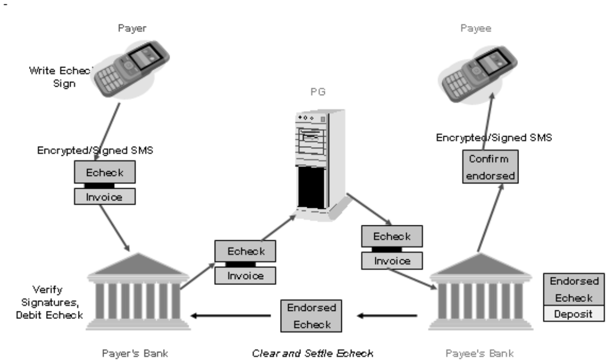

Figure 6

The proposed payment model can be applied also on another case study where the merchant has POS or e-commerce site. The merchant will ask the payer to enter his/her mobile number during the payment, then the transaction will proceed from the acquirer's bank (payee's bank) to PG, then to issuer's bank (payer's bank) and then the issuer will ask the payer for confirmation through secure SMS. As shown in the proposed model, money payment applications can be achieved without exposing credit or debit card information. Even anonymity can be provided by using nick names, instead of mobile numbers, and at this time the PG should handle the mapping between customers' nick names and their mobile numbers. Also one of the important benefits achieved is the leverage of the national scheme (e.g. 123, SAMA,…) to provide the function of the PG.

7. Conclusions

Nearly half of all consumers have concerns about data theft, and many people avoid online shopping and bill payment for this reason. People don't like revealing financial information to an unknown third party and shoppers certainly don't like sharing their private data on the web. SecureSMSPay eliminates these concerns, keeps customer data with their bank, making them more comfortable with payment and even e-commerce.

The introduced secure Mobile Payment provides all security factors; confidentiality, integrity, authenticity, and non-repudiation using a simple cryptography operation suitable for mobiles with limited resources, also it provides the same security strength of asymmetric cryptography without the need of its complexity. The proposed model is built over SMS protocol that is common, asynchronous, cheap, and also, as demonstrated in the proposed payment model, it can be involved in many types of payment application; e.g. e-cheque, e-commerce, and even EFT POS. In addition, the proposed model will leverage the infrastructure of the national payment network e.g. 123, SAMA and international network e.g. VISA/MasterCard to route mobile payment transactions through it.

In future work, we should study asymmetric cryptography, and offline transactions which are suitable for e-wallet applications and micro- transactions.

8. References

[1] MasterCard and Visa, SET Protocol Specifications, 1997, http://www.setco.org/set_specifications.html

[2] Europay, MasterCard and Visa international. Security and Key Management. http://www.emvco.com.

[3] D. Suarez1, J. Torres1, M. Carbonell1 and J. Tellez2, "A new domain-based payment model for emerging mobile commerce scenarios", Proceedings of 18th International

Workshop on Database and Expert Systems Applications, IEEE, 2007, pp. 713-717.

[4] P. Garner, I. Mullins, R. Edwards, and P. Coulton, "Mobile Terminated SMS Billing – Exploits and Security Analysis", Proceedings of the Third International Conference on ITNG, IEEE, 2006, pp. 1-10.

[5] Indiatimes, “The new phony crime: SMS spoofing”, http://tinyurl.com/3kgbb, July 2004.

[6] Supakorn Kungpisdan, Bala Srinivasan, and Phu Dung Le "A Secure Account-Based Mobile Payment Protocol", Proceedings. ITCC 2004. International Conference on Volume 1, Issue , 5-7, Pages: 35 – 39, April 2004

[7] Xianping Wu,Osama Dandash, and Phu Dung LeGeethapriya, "The Design and Implementation of a Smartphone Payment System based on Limited-used Key Generation Scheme", Journal of Theoretical and Applied Electronic Commerce Research, Volume 1 , Issue 2, Pages: 1 - 11 August 2006

[8] Gianluigi Me, Alexander Schuster,and Maurizio Adriano Strangio, "Mobile Local Macropayments: Security and Prototyping", IEEE 2006

[9] Isaac & Camara -Spain, "Anonymous Payment Protocol in a Kiosk Centric Model using Digital Signature scheme with message recovery and Low Computational Power Devices", IEEE 2006

[10] Java 2 Platform, Micro Edition (J2ME). http://java.sun.com/j2me.

[11] A semantics for BAN logic, http://dimacs.rutgers.edu/Workshops/Security/program2/bleeker/.

[12] Check clearing for the 21st century act. http://www.federalreserve.gov/ paymentsystems/ truncation/, October 2004

.