Non-Repudiation Mobile Payment Protocol with Symmetric Approach

Tan Soo Fun[#1], Leau Yu Beng[*2], Chin Su Na[*3], Mohd Norhisham Razali[#4]

[#]*School of Engineering and Information Technology, Universiti Malaysia Sabah*
Sabah, Malaysia.
[1]soofuntan@gmail.com
[4]hishamrz@gmail.com

[*]*School of Informatics Science, Universiti Malaysia Sabah*
Labuan, Malaysia
[2]leauyubeng@gmail.com
[3]chinsuna@yahoo.com

***Abstract* - The increasing development of wireless networks and the widespread popularity of handheld devices such as Personal Digital Assistants (PDAs), mobile phones and wireless tablets represents an incredible opportunity to enable mobile devices as a universal payment method, involving in daily financial transactions. Unfortunately, security issues are hampering the widespread acceptance of mobile payment. These security requirements for the payment transaction include authentication, message integrity, confidentiality, anti-replay protection, anonymity, privacy protection, authorization and non-repudiation. Among these security requirements, the non-repudiation serves as a very fundamental of critical success factor in making mobile payment a reality. Non-repudiation of payment protocol refers to the ability to trace an action between parties engaging in payment protocol and then hold them accountable or responsible for their transactions. The non-repudiation property can be achieved with asymmetric cryptography and digital signature. However, it is impractical to be applied in securing the mobile payment transaction due to the constraints of wireless network and mobile devices. Firstly, the limitations of mobile devices such as lower power, computational and storage capabilities. Secondly, the constraints of wireless network such as lower bandwidth, less reliability and higher latencies than wired network. Furthermore, the cost of wireless network connection is higher than wired network. This paper presents how the proposed mobile payment protocol achieves non-repudiation property by using the symmetric approach.**

***Keywords* - non-repudiation, mobile payment, privacy, symmetric key**

1. INTRODUCTION

The increasing development of wireless networks and the widespread popularity of handheld devices such as Personal Digital Assistants (PDAs), mobile phones and wireless tablets, have led to mobile payment(m-payment) merged as the next generation of electronic payment(e-payment). Today, most people never leave their home without mobile phone. Not only as a storage, it's computing and data transmission capabilities makes mobile phone as an ideal device to store everything we normally carry in our wallet, including cash, ATM cards, cheque, debit cards and credit cards. This represents an incredible opportunity to enable mobile devices as a universal payment method, involving daily financial transactions such as web store-front payment, physical Point-of-Sale (POS) purchase, Person-to-Person (P2P) payment, and payment for mobile commerce application. Mobile Commerce (M-Commerce) refers as any transaction with a monetary value that is conducted via a mobile telecommunications network [3]. Mobile payment (or called M-Payment) playing a critical role in M-Commerce transactions and it is defined as any transaction that is carried out via mobile device, involves either direct or indirect exchange of monetary

[1]Correspondence Author

values between two or more parties involved [4,7,15].

Some issues hampering the widespread acceptance of mobile payment such as ease of use, expenses, security, universality and technical feasibility. According to [1,9,13], security issues serve as a very fundamental of critical success factor in making mobile payment a reality. The security requirements for payment transaction are including authentication, message integrity, confidentiality, anti-replay protection, anonymity, privacy protection, authorization and non-repudiation [11,14,18]. Currently, most of the payment protocol analysis focuses on non-repudiation aspect [5,6,8,11]. Non-repudiation of payment protocol refers to the ability to trace an action between parties engaging in payment protocol and then hold them accountable or responsible for their transactions. Particularly, the parties involved must be able to prove to a dispute resolver (verifier) that they are honest for the transaction relevant to them.

To achieve non-repudiation property, several mobile payment protocols based on digital signature scheme have been proposed. Digital signature provides non-repudiation protection and prevents the denial of some previous commitments or actions by the communicating parties. However, digital signatures employ a type of asymmetric cryptography, which are inefficient to be applied into wireless networks. With asymmetric encryption, client needs to perform high computational operations, and his mobile device is required to have sufficient storage to store public-key certificates [4,12,17]. Furthermore, during a transaction, each certificate sent to the payer has to be verified by a Certificate Authority (CA) located in a fixed network, which results in an additional communication passes between engaging parties[10, 12,20,21]. To design a lightweight mobile payment protocol, the proposed mobile payment protocol applies symmetric key encryption and hash function which requires lower computational, lower storage and lower communication passes compared with asymmetric approach. However, how can an originator of an encrypted message can be identified and proved due to the same key is shared between two engaging parties is still a critical issues. To solve this problem, the proposed mobile payment protocol applies the cryptographic concepts employed by [2, 10,13].

The main contribution of this paper is to present a secure and non-repudiation mobile payment protocol for M-Commerce applications. Without any public key encryption and digital signature during payment transaction, the proposed mobile payment not only overcomes all the constraints of mobile environments but also satisfies engaging parties' security requirements. The proposed mobile payment does provide security properties with a same level as asymmetric key, which includes authentication, message integrity, confidentiality, anti-replay protection, non-repudiation, privacy protection and anonymity for engaging parties.

The remainder of this paper is organized as follows. Section II summarizes the security requirements of the proposed mobile payment protocol. Section III outlines the notation and presents the protocol in details. Section IV analysis its security against the requirements as stated in Section II. Finally our conclusions are made in Section IV.

2. SECURITY REQUIREMENTS

To achieve secure and non-repudiation payment transaction between engaging parties, the proposed mobile payment protocol should meet the following security requirements:

(S1) Authentication

The proposed protocol should allow the authentication of the payer to payer's MNO, authentication of the payee to payee's MNO and authentication between payee and payer. These assurances that engaging parties are who they claim to be and prevent an attacker from masquerading as an engaging party during the payment transaction.

(S2) Message Integrity

The proposed mobile payment protocol should assure that the message exchange among engaging parties has not been changed or altered en route by unauthorized or unknown means.

(S3) Confidentiality

The proposed mobile payment protocol should keep information secret from all but available for those who are authorized to see it, and provides protection against eavesdroppers for understanding intercepted messages.

(S4) Non-Repudiation

The proposed protocol should ensure that payer must not be charged on the payment

that he has never made. Thus, either network rogues or malicious payee must be unable to generate spurious transactions which later on will be approved by payer's MNO. Besides that, payer can prove not having authorized a payment even if the payer's MNO secret key is available to the adversary (e.g. adversary colludes with an insider). The proposed protocol should also allow payee's MNO ensures that payee has asked this payment made to him and agreed upon payment amount.

(S5) Privacy Protection of the Payer

The proposed protocol should provide the privacy protection to payer. Payer needs an identity protection from eavesdropper, payee and payee's MNO. Besides that, payer needs a privacy protection of the order and the payment information. For example, one investor who purchasing some information on certain stocks may not want his competitors to know which stocks that he is interested in, or payer prefers a delivery address to be protected from payer's MNO and payee's MNO.

(S6) Anti-Replay Protection

The proposed protocol should prevent an adversary from trying to intercepts an encrypted message and transmits it again. Besides that, information sent is previous transaction must not enable a later spurious transaction

3. PROPOSED PROTOCOL DESIGN

The proposed mobile payment protocol is composed of four engaging parties, which includes payer, payee, payer's MNO and payee's MNO. The notation to be used for the protocol presentation is summarized as follows:

TABLE 1
NOTATIONS

Symbol	Description
AI_P	Account Information of party *P*, which including credit limit for each transaction and type of account (post-paid or prepaid account)
AMOUNT	Payment transaction amount and currency
DATE	Date of payment execution
DESC	Payment Description, which may includes delivery address, purchase order details and so on. Payer will include only the information that he wish to disclosure to Payee
H(M)	The one way hash function of the message *M*
ID_P	Identity of engaging party *P* which identifies party *P* to MNO; computed as $ID_P = PN_P + H(PN_P, PIN_P)$
i	Used to identify the current session key of X_i and Y_i
$K_{P\text{-}P}$	The secret key shared between payer's MNO and payee's MNO.
{M}X	The message *M* symmetrically encrypted with shared key *X*
NONCE	Random number and timestamp generated to protect against replay attack, that is ensure old communication cannot reused in replay attack.
$PayeeID_{Req}$	The request for payee identity
PIN_P	Party *P* selected Password Identification Number (*PIN*)
PN_P	Phone Number of party *P*
R	Payer's nick name, random number and timestamp generated by payer act as payer's pseudo-ID, which uniquely identifies payer to payee
Received	Payment receivable update status, which includes the received payment amount
Success/Failed	The status of registration, either success or failed
TID	The identity of transaction
TID_{Req}	The request for *TID*
TSC	Time Stamp Center
Yes/No	The status of transaction, either approved/rejected

The proposed payment protocol is based on Client Centric Model, which the transaction flow is completely controlled by the Payer. Both payer and payee are required to register with their own mobile network operator (MNO) before any transaction could take place. Payer sends

registration details such as account information, payer identity and phone number, encrypted with session key K_1 to payer's MNO.

Payer→Payer's MNO: $\{PN_{Payer}, ID_{Payer,} AI_{payer}\}_{K1}$

During the registration process, payer is required to set his password identification number (PIN_{Payer}) for later access to his mobile wallet application. Then, payer's MNO sends confirmation message to payer and encrypted with the session key $K_{1.}$

Payer's MNO→Payer: $\{Success/ Failed\}_{K1}$

If registration process is successful, payer receives mobile wallet application through email or downloading from payer's MNO site. The mobile wallet application contains symmetric key generation and payment software. After installed successfully, a set of symmetric key $X = \{X_1, X_2, \ldots, X_n\}$ is generated, store into payer's mobile devices and send to payer's MNO. Similarly, the payee must go through the similar registration process with payee's MNO to enable them to receive payment from payer. The payee generates a set of symmetric key $Y = \{Y_1, Y_2, \ldots, Y_n\}$ with payee's MNO and store into his terminal and MNO database.

In this section, we present our mobile payment protocol, which consists of seven transactions, T1 to T7, as shown in Figure 1.

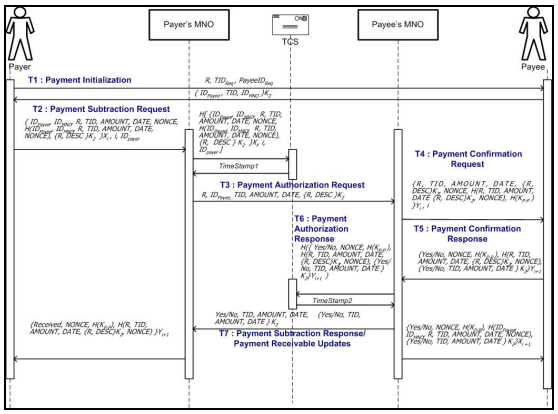

Figure 1. Proposed mobile payment protocol

T1: When the payer plans to make a payment, he has to enter his password, PIN_{Payer} in order to have an authorized access to his mobile wallet application. Then, payer sends the payment initialization request message to payee, which encrypted with session key K_2. If payee accepted, the payment initialization response message will be sent to payer to initiate the payment process.

T2: Payer starts making payment by sending payment subtraction request message to his MNO, by combining ID_{Payer}, transaction details and *NONCE* , then encrypted by using X_i . Payer's MNO decrypts the received message with their shared X_i to retrieve payment information. The hash value, $H(ID_{Payee}, ID_{Payee's\ MNO}, R, TID, AMOUNT, DATE, NONCE)$ is used to check message integrity and referred as H_1. Then, payer's MNO computes a hash function from payment information that he received, ID_{Payee}, $ID_{Payee's\ MNO}$, *R*, *TID*, *AMOUNT*, *DATE* and *NONCE*. This hash function referred as H_2. If the value $H_1 = H_2$, then payer's MNO accepts the payment subtraction request and assurance that message has not been changed en route. Otherwise, payer's MNO rejects the payer's payment subtraction request. To provide accountability evidence in case of dispute, once payer's MNO received the payment subtraction request message from payer, immediately payer's MNO computes hash function of message and sends to TSC to get a timestamp. Note that, hash function is used here to reduce the storage space and prevent revealing of any payment transaction details to TCS.

T3: Payer's MNO checks the payer's account credit limit for those subscribed as post-paid account or account balance for those subscribed as pre-paid account. If credit limit is allowed or balance is sufficient, then payer's MNO reserved corresponding amount for the transaction and sends payment authorization request to payee's MNO. Note that, the communication passes between MNOs can be done under the well-established secure network, such as Intranet or private network. Hence, the proposed protocol does not concern its security issues.

T4:Payee's MNO forwards payment transaction details to payee and encrypted with their shared Y_i . The element $H(K_{P\text{-}P})$ provides accountability evidence for payee. Payee can assurance that this payment confirmation request is really sent from payee's MNO due to

only payee's MNO obtains both Y_i and $H(K_{P-P})$.

T5: Payee decrypts the payment confirmation request message. The element *H(R, TID, AMOUNT, DATE, {R, DESC}K_2, NONCE)* inside payment confirmation request is used to check message integrity, and referred as H_3. Then payee computes the hash function of payment information, *R, TID, AMOUNT, DATE {R, DESC}*K_2 and *NONCE* and referred as H_4.Then, payee compares H_3 and H_4. If $H_3 = H_4$, payee accepts the transaction and ensures that message has not been changed en route. Otherwise, payee will reject the transaction. Payee further decrypts the *{R, DESC}*K_2 with his K_2 which only shared with payer and compares the value of *R* he received from payment initialization request message with the value of *R* from the payee's MNO to determine whether *R* has been change en route. *R* together with the corresponding *TID* uniquely identifies payer to payee. If payee agreed upon the transaction details such as payment amount, then he sends an acceptance of payment transaction to his MNO which encrypted with their shared Y_{i+1}. If payee disagrees with the transaction details from payer, payee can rejects payment transaction. Besides that, the elements *{Yes/No, TID, AMOUNT, DATE }*K_2 serves as a receipt from payee to payer. Only the authorized payer can retrieves the payment receipt from payee due to it is encrypted with K_2.

T6:Payee's MNO decrypts the payment confirmation response message with their shared Y_{i+1}. To avoid non-repudiation of payee, who may deny later that he does not agreed with the transaction amount, or claimed that his Y_{i+1} is compromised before the payment transaction, the payee's MNO computes hash function of message and sends to TSC to obtain a timestamp. Then payee's MNO forwards the result of payment authorization response to payer's MNO under their secure network.

T7:Payer's MNO retrieves the payment authorization response that received from payee's MNO. If payee accepted the payment transaction, the payer's MNO debits payer's account and transfers payment to payee's MNO. Meanwhile, payee's MNO credits the payee account. If payee rejected the payment transaction, the payer's MNO terminates the payment transaction. Then, payer's MNO sends payment subtraction response to payer, which encrypted with their shared X_{i+1}. Payer decrypts payment subtraction response with shared X_{i+1} to retrieve the result of transaction. Payer can checks whether this message is response of his payment subtraction request by compares the received has value from payment subtraction response message with the hash value in payment subtraction request message. If they are not matched, payer sends a message to the payer's MNO to point out the problem, so that the payer's MNO can start a recovery procedure. Note that, payment subtraction request may be returned before payment authorization request. At the same time, the payee's MNO sends an acknowledgment on the payment receivable updates message to payee. If all the transaction processes are successfully completed, the payee releases or delivers the purchased goods or services to payer.

To prevent replay of the secret key from payer and payee, both payer's MNO and payee's MNO make sure that the symmetric *key* X_i and Y_i have not been used before proceed the payment transaction. The MNO will maintain a list of generated secret key by discarding used or expired symmetric key X_i and Y_i from the list. If symmetric key X_i and Y_i were compromised, there must be revoked. Both payer and payee may receive an update notification from MNO when their key was expired. To update their secret key, they may connect to their MNO to generate a new session key, K_1 and then offline generates a new set of secret key X_i and Y_i with a new session key K_1.

4. SECURITY ANALYSIS

This section presents a security analysis of the proposed mobile payment protocol against the requirements stated in Section 2.

(*S1) Authentication*

The authentication property of proposed mobile payment protocol is ensured by two-factor authentication, the usage of both symmetric keys, X_i and Y_i, and session key, K_1 and K_2 which generated by Diffie-Hellman Key Agreement approach. The payer is authenticated by mobile wallet application with two-factor authentication, that is something he has (mobile devices and mobile wallet application) and something he knows (PIN_{Payer}). If the PIN_{Payer} is valid, payer is authorized to start making payment transaction. The authentication between the payer and payee is achieved with K_2, R and corresponding *TID*. The payer is authenticated by his MNO with X_i and ID_{Payer}. Meanwhile, the payee is authenticated by payee's MNO with Y_i and ID_{Payee}.

(S2) Message Integrity

To achieve message integrity, the proposed mobile payment protocol applies a hash functions. The hash function, $H(ID_{Payee}, ID_{payee's\ MNO}, R, TID, AMOUNT, DATE, NONCE)$ is used to check message integrity. By comparing the hash function of received payment subtraction request from payer and self computed hash functions, the payer's MNO can detect whether important transaction data have been modified or replaced during the transaction.

(S3) Confidentiality

To achieve confidentiality property, any important transaction details are encrypted during the transaction. The payment initialization request and response message are encrypted with K_2 which generated by running the Diffie-Hellman Key Agreement approach and only known between payer and payee. The payment subtraction request and response message are encrypted with X_i that only known between payer and payer's MNO. Finally, the payment confirmation request, payment confirmation respond and payment receivable updates message are encrypted with symmetric key, Y_i that is only shared between payee and payee's MNO.

(S4) Non-Repudiation

The payment subtraction request contains the ID_{Payer}, which generated by computes the hash function of PN_{Payer} and PIN_{Payer}. Since the symmetric key X_i is only shared between a payer and a payer's MNO, it ensures that payer does not unwittingly send the ID_{Payer} and payment subtraction request to an unauthorized party. An adversary unknown the PIN_{Payer} and does not owned payer's mobile phone can neither create a fake payment subtraction request nor modify the encryption of a legitimate one to its advantage. Note that PIN-based authentication only provides a weak proof of transaction authorized by payer.

The craftiness payer's MNO may collude with adversary to counterfeit the payer's payment subtraction request because payer's MNO also holds X_i. By including the $\{R, DESC\}K_2$ into payment subtraction request, the payer's MNO cannot generate this payment subtraction request due to payer's MNO unknown session key, K_2. Furthermore, the payee who may be an adversary does not hold the X_i also cannot generate the fake payment subtraction request. Hence, the payer's MNO can ensures that the payment subtraction request is really originated and sent by payer who holds both X_i and K_2.

However, in the case of dispute, the payer can further deny that he has sent payment subtraction request by claiming that his X_i is compromised before the transaction. To handle this problem, payer's MNO computes hash function of received payment subtraction request and sends to TSC to testify that certain transaction exists before the corresponding timestamp. Payer's MNO preserves the time stamp and corresponding payment subtraction request message to provide accountability evidence in case of disputes. Hence, the proposed mobile payment protocol provides undeniable proof to resolve the dispute between payer and payer's MNO.

(S5) Privacy Protection of the Payer

The proposed mobile payment protocol emphasizes this requirement by following the client centric model. Without sending any order and payment information through payee minimizes significantly the risk of disclosure payer's sensitive information of payer to payee and also payee's MNO. During payment initialization phase, payer

identifies himself to payee by sending the *R* rather than sending a real identity, ID_{Payer} to payee. *R* represents one-time payer's identity together with corresponding *TID* which uniquely identifies the payer to payee. This provides additional privacy protection for payer. Note that, the proposed mobile payment protocol protects not only protect the payer's privacy from payee, but also from payer's MNO and payee's MNO. The payer's sensitive information such as delivery address, purchased items (e.g which stocks payer is interested in) are been hidden by encrypting with payer and payee shared K_2. Payee can include the information that he wish to disclose to payer in $\{R, DESC\}K_2$. Hence, the proposed mobile payment protocol satisfies this requirement. Besides that, the comparison result of privacy protection in [19] shows that proposed mobile payment protocol achieves the complete privacy protection for payer, that is payer's identity protection, and from the payee and eavesdroppers and the payer's transaction privacy protection, such as which stocks that the payer purchased, what the payer pay for and the delivery address are protected from outsiders and even from payer's MNO and payee's MNO.

(S5) Anti-Replay Protection

The proposed mobile payment protocol prevents an adversary from trying to intercept an encrypted message and transmit it again by padding the *NONCE* into message. The payer's MNO can ensure that the payment subtraction request is not a repetition item of an earlier one by comparing a *NONCE* in the current message with a *NONCE* in the previous message. Similarly, the payer can ensure that the payment subtraction response is not a repetition of a previous response. Therefore, the proposed mobile payment protocol does provide anti-replay protection.

As a result, the proposed mobile payment protocol satisfies all the security requirements defined in Section 2.

5. CONCLUSION

This paper has presented the proposed mobile payment that achieves secure and non-repudiation for mobile payment transactions. Without asymmetric cryptography and digital signature during payment transaction, the proposed mobile payment not only overcomes all the constraints of mobile environments but also satisfies all criteria of end-to-end security property and non-repudiation as demonstrated in section IV. The proposed mobile payment provides security properties that have same level as asymmetric approach, which includes authentication, message integrity, confidentiality, anti-replay protection, non-repudiation, privacy protection and anonymity for engaging parties. The future work will concentrate on improving the verification solution to support mobile user authentication and authorization for mobile payment transactions.

REFERENCES

[1] Cervera, A. 2002. *Analysis of J2ME™ for Developing Mobile Payment Systems*. IT Copenhagen :University of Copenhagen.

[2] Cimato, S. 2001. Design of an Authentication Protocol for GSM Javacards. *Journal of Lecturer Notes in Computer Science*. **2119**(2001): 487-501.

[3] Durlacher. 1999. "*Mobile Commerce Report*. Technical Report of Durlacher Research Ltd.

[4] Jun L., Liao, J.X. & Zhu, X. 2005. *A System Model and Protocol for Mobile Payment*. Proceedings of the 2005 IEEE International Conference on e-Business Engineering. October 18-21, 2000. Beijing: 638-641.

[5] Kailar, R. 1996. Accountability in Electronic Commerce Protocols. *Journal of IEEE Transactions on Software Engineering*. **22**(5): 313-328.

[6] Kessler, V. & Neumann, H. 1998. A Sound Logic for Analyzing Electronic Commerce Protocols. *Proceedings of the Fifth European Symposium on Research in Computer Security*. September 16-18, 1998. London. 345-360.

[7] Krueger, M. 2001. *The Future of M-Payments–Business Options and Policy Issues*. . Background Paper No.2. Electronic Payment Systems Observatory .

[8] Kungpisdan, S. & Permpoontanalarp, Y. 2002. Practical Reasoning about Accountability in Electronic Commerce Protocols. *Journal of Lecturer Notes in Computer Science*. **2288**(2002): 268-284.

[9] Kungpisdan, S., Srinivasan, B. & Phu Dung, L. 2003a. Lightweight Mobile Credit-Card Payment Protocol. *Journal of Lecturer Notes in Computer Science*. **2904**(2003):295-308.

[10] Kungpisdan, S., Srinivasan, B. & Phu Dung, L. 2004a. A Secure Account-based Mobile Payment Protocol. *Proceedings of the 2004 International Conference on Information Technology: Coding and Computing*. Las Vegas. 35-39.

[11] Kungpisdan, S., Srinivasan B., & Phu Dung, L. 2004b. Accountability Logic for Mobile Payment Protocols. *Proceedings of the International Conference on Information Technology: Coding and Computing*. Las Vegas. 40-44.

[12] Li, X. & Hu, H-P. 2008. Efficient Protocol for Secure Mobile Payment. *Journal of Communication and Computer*. **4(**5):22-26.

[13] Marvel, L. M. & Boncelet, C.G., Jr. 2001. Authentication for Lower Power Systems. *Proceedings of IEEE Military Communications Conference-Communications for Network-Centric Operations: Creating the Information Force*. 135-138.

[14] Panko, R.R., 2004. *Corporate Computer and Network Security*. New Jersey: Prentice Hall.

[15] Pousttchi, K., Kreyer, N. & Turowski, K. 2003. Mobile Payment Procedures: Scope and Characteristics. *Journal of e-Service*. **2**(3):7-22.

[16] Pousttchi, K. & Zenke, M. 2003. Current Mobile Payment Procedures on the German Market from the View of Customer Requirements. *Proceedings of the Fourteenth International Workshop on Database and Expert Systems Applications*. 870-874.

[17] Ramfos, A., Karnouskos, S., Vilmos, A., Csik, B., Hoepner, P. & Venetakis, N. 2004. SEMOPS : Paying with Mobile Personal Device. *Proceedings of Fourth IEEE Conference on e-Commerce, e-Business, and e-Government*. 22-27.

[18]Stallings, W. 1999. *Cryptography and Network Security: Principles and Practice*. (2nd Edition). New Jersey :Prentice Hall.

[19] Tan Soo Fun, Leau Yu Beng, Rozaini Roslan. 2008. Privacy in New Mobile Payment Protocol. Proceeding of International Conference on Information and Communication Technologies 2008. World Academy of Science, Engineering & Technology (WASET), Paris, France, Volume 30: 2008.

[20] Tellez, J. & Sierra, J. 2007. Anonymous Payment In a Client Centric Model For Digital Ecosystem. *Proceedings of IEEE International Conference on Digital Ecosystems and Technologies*. 422-42.

[21] Wang, C. & Leung, H-f. 2005. A Private and Efficient Mobile Payment Protocol. *Journal of Lecturer Notes in Artificial Intelligence*. **3349**(3802):1030-1035.