Review of Mobile Macro-Payment Schemes

Tan Soo Fun, Leau Yu Beng, and Mohd Norhisham Razali, *Member, IACSIT*

***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, designing a secure mobile payment schemes is more challenging than wired payment protocol due to the constraints of wireless network and mobile devices. The existing Public Key Infrastructure (PKI) based electronic payment protocol such as Secure Electronic Protocol (SET) and Internet Payment Protocol (*i*KP) cannot be directly adopted in wireless environment. Over the past ten years, a numerous of mobile macro-payment schemes have been proposed to solve the challenges of these constraints. As a result, this paper aims to summarizes the work of researches over the past ten years and four significant macro-payment schemes: KSL protocol, Anonymous protocol, Private Protocol and Secure Agent-based Protocol have been selected and further discussed. This paper gives a readers an overall idea of mobile macro-payment schemes and notably recommends both academic and industry researchers to complement each other, adopt the standardized and shared development.**

***Index Terms*—Payment protocol, cryptography protocol, macro-payment schemes, mobile payment, secure electronic transaction, communication protocol**

I. Introduction

Mobile commerce (m-commerce) has undoubtedly become an omnipresent and an active area in electronic payments. It allows mobile user to buy and pay for things or services, pay his bill or make a bet via mobile phone when on move, anywhere and at any time. According to Durlacher[1] , mobile commerce (m-commerce) refers as any transaction with a monetary value that is conducted via a mobile telecommunications network. Mobile payment is defined as any transaction that is carried out via mobile device, involves either direct or indirect exchange of monetary values between two or more parties involved. Based on the monetary value of transaction, the payment schemes can be further divided into two categories: micro-payment and macro-payment. In general, the micro-payment scheme is designed to allow payments as low as one-tenth of a cent (USD 0.001) to be made. Since it is involving a low value per transaction (generally less than USD 1), the effort of security mechanism is more focuses on reducing the payment verification cost such as minimize the computational operation and storage costs, and minimizing the communication traffic among engaging parties. On the other hand, when the transaction involves a higher monetary value per transaction, generally more than USD 10, it is categorized into macro-payment. The security requirements for macro-payment are more rigorous and more concerned with the authorization, privacy of data and non-repudiation aspect. It is undeniable that designing a secure mobile payment schemes is more challenging than wired payment protocol 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 focuses on discussing macro-payment schemes for securing a payment transaction. It first provides some background about mobile payment schemes, including the actors involves in payment transaction, the model of mobile payment schemes, the transaction flow model of payment data and the security requirements for macro-payment transaction. Section III provides a brief of history of mobile payment schemes and summarizes the work of researches over the past ten years. Four significant macro-payment schemes: KSL protocol [2], Anonymous protocol [3], Private Protocol [4] and Secure Agent-based Protocol [5] have been selected and reviewed in Section IV. This paper does not require reader to have any prior knowledge of mobile payment schemes. Readers who design and implement mobile macro-payment schemes are highly recommended to read the original paper of these payment protocols.

II. Background of Mobile Payment

This section provides an overview of mobile payment schemes characteristic: actors, model, transaction flow model and security requirements for macro-payment transactions.

Actors

In general, there are seven main actors involve in a mobile payment[6]-[8]:

1) Financial service providers (FSPs)

They are responsible for the backend processing which is required to settle a transaction between payer and payee. Currently, there are three different actors of FSPs in mobile payment schemes, namely banks, Mobile Network Operators (MNOs) and third parties.

2) Payment service providers (PSPs)

They provide the system access channel to the FSPs and

Manuscript received July 9, 2013; revised September 10, 2013. This work was supported in part by the Universiti Malaysia Sabah.

Tan Soo Fun and Mohd Norhisham Razali are with the School of Engineering and Information Technology, Universiti Malaysia Sabah, 88400 Malaysia (e-mail: soofun@ ums.edu.my, hishamrz@ums.edu.my).

Leau Yu Beng was with School of Engineering and Information Technology, Universiti Malaysia Sabah. He is now with the National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia 11800 Penang Malaysia(e-mail: leauyubeng@gmail.com).

facilitates the communication between FSPs. PSPs establish transactions among FSPs, payer and payee. Basically, they provide the payment software and interfaces users.

3) Payer

Also called as client/customer, act as payment sender. Payer is an actor who wants to make a payment either for his purchased goods or services from the merchant or merely transfer funds to payee. After the payment transaction, payer's account is debited

4) Payee

Also called as merchant, act as payment receiver. Payee is an actor who offers goods or services or merely receives the funds from payer. The role of payee varies with different payment methods. For example, in P2P method, payee is a mobile device holder who accepts payment from payer; in Internet payment method, payee is a web server; in POS method, payee refers to a retail store, restaurant, vending machine or even parking system; and in m-commerce method, a payee is a content service provider, etc. After the payment transaction, payee receives payment from payer and his account is credited.

5) Mobile network operators (MNOs)

Also known as Network Services Operators. They provide telecommunication facilities or support infrastructure in mobile payment. MNOs normally own the network, have means to identify who issuing their network and have the billing systems to charge end-users for their services

6) Device manufacturers

The device manufacturers produce mobile devices that come with mobile payment facilities. For instance, Nokia , a world leader in mobile communication, has designed the secure chip and an antenna in its Nokia 3220 model which can send a radio frequency signal to the terminal, to transfer payment information to the merchant's card terminal quickly and securely [9], [10]

7) Regulators

Another relevant party who indirectly influence mobile payments is regulators. These are government bodies, law enforcement agencies or banking regulators. They take care of the public interest by protecting the right of end-users. Regulators regulate rules and laws in relation to mobile payments.

III. Model of Mobile Payment Schemes

Recently, several researchers and academician have categorized the mobile payment schemes into two main categories, which are bank dominated and mobile operator dominated mode as describe following [11], [6]-[8].

A. Bank Dominated Model

In bank dominated model, the bank or financial institutional acts as FSPs and is responsible to settle the payment and clear the transactions. The mobile operators only have to transport payment data to the banks or FSPs. This kind of payment is further divided into two categories, with and without direct access to card. The first type of payment refers to the existing established payment methods such as credit card or debit card. The latter refers to placement of a payment card into mobile phone. The card will be directly read by the mobile phone. This requires modification on mobile phone equipment such as dual slots phones and dual chip phones [12]. One example is Mobile Visa Wave payment, which was launched in Malaysia on 2006 in collaboration with Maybank, Maxis Communications Berhad (Maxis) and Nokia. The credit card information is stored inside the mobile phone's secure chip and thin copper wire will acts as an antenna, transferring payment information quickly and securely to a reader connected to the merchant's terminal through Near Field Communication (NFC) [9], [10].

B. Mobile Operator Dominated Model

In mobile operator dominated model, the mobile operators act as PSPs, perform the payment settlement and clearing transaction via existent billing system without involving the banks and other financial institutions. All charges from a transaction are accrued in the MNO subscriber's account and subscribers are billed periodically. A leading mobile network operator in Japan, NTT DoCoMo I-mode employs this model using its mobile portal. Other similar examples are Valista [13] and Trivnet [14]. This medium of payment has more simplified process and allows the MNO to charge the subscribers directly via the existing billing system.[6] and [7]further emphasized that MNOs are, to some extent, a better choice to act as PSPs compared with bank in a mobile payment system for few reasons. Firstly, MNOs have well-established their billing system and relationship with the mobile phone users. Secondly, MNOs own the network and have means to identify who is using their network. Thirdly, MNOs have the technical expertise and lastly, MNO have a large customer base. In some countries, such as Austria, Cyprus, Finland, Germany, Italy, Singapore and United Kingdom, the mobile subscriber penetration rate is very high, that is over one-hundred percentages. Because of the MNOs owned a large customer base, they are able to generate a critical mass of customer and merchant acceptance for a new payment schemes compare to bank and financial institutional.

Billing on a monthly phone invoice is very cost effective compared with other billing system from user's perspective and it is a fast method to pay without a credit card. This may suggest an idea that consumers and business will enjoy a much lower cost of doing business if the credit card networks fees are eliminated, to the exclusion of financial institutional commitment from bank and credit card companies. Besides that, owing to lack of wireless expertise and direct access to mobile users, banks and other organizations face a larger up-front cost in rolling out mobile payment technology compared to MNOs. Some optimists even stated that integration with the banking system is nonexistent or insufficient. In the future, wireless service providers might supply banking services [15]. However, the pre-requisite of this modelis MNO billing system should become much more reliable than today's phone billing system

IV. Transaction Flow of Payment Schemes

The transaction flow of payment schemes concerns how to move forward the payment data such payment amount, payment execution date, etc. from a payer to a payee across the computer networks such as internet and wireless network. When both payer and payee hold bank accounts with the same financial services, the design of the transaction flow of payment scheme becomes simple and straightforward. The payer just need to inform his financial services providers to debited requested amount from his account and credited into payee's account without involving any financial clearing networks, as shown in Fig. 1.

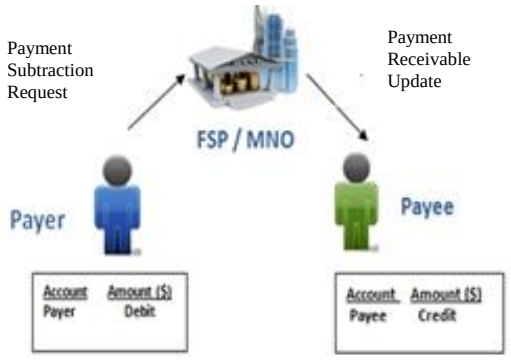

Fig. 1. Centralized account model for payment transaction flow

However, the situation becomes more complicated when both payer and payee hold accounts with two different financial services providers or subscribes to two different mobile network operators. In general, this decentralized account model can be further categorized into two sub-categories as following:

A. Payee Centric Model

The payee centric model also well-known as Debit Pulls Payment streams. This model follows the traditional transaction flow, where the payment instructions are initiated by the payee who receives a payment initialization from payer. On receipt of the payment initialization request, and under agreement with payee's FSP or MNO, payee may submit payment instruction to his FSP or MNO. Payee's FSP or MNO uses existing payment settlement and clearing system, either real-time clearing (such as ATM transaction), or batch clearing (such as Electronic Funds Transfer, EFT) in order to debit a requested amount from a payer's account and credited into payee's account.

One disadvantage of using traditional payment data flow scenario is full-connectivity. This can cause a problem, a payee who may suffer from either malfunction in connection or the use of other communication technologies is unaffordable due to the inconvenience and costs associated. [16]. Besides that, since the transaction flow is completely controlled by payee, payer faces a potential threat whereby their payment details such as credit or debit cards and account information can either be modified or captured by the payee or even used for later access to payer's account without any permission from payer.

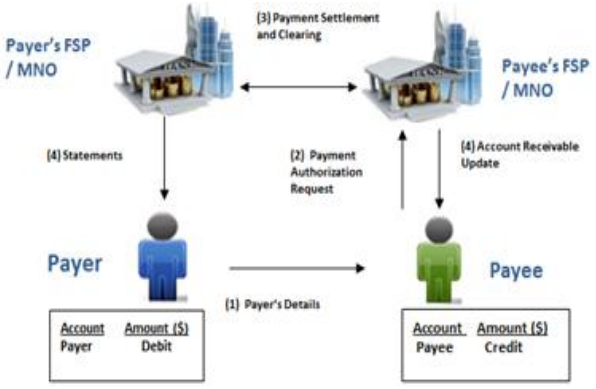

Fig. 2. Payee centric scenario

B. Payer Centric Model

Payer Centric Model also well-known as Credit Push Model in financial payment streams and it is very similar to the direct credit banking facility which is widely in use nowadays. In this model, payer is responsible for originate the payment instruction and send it directly to his FSP. Once the payer has been authenticated by his FSP or bank, the FSP/MNO can process requested payment instruction. With the existing payment settlement and clearing system, the payer's FSP clears and settles the payment with payee's FSP, and debits the payer's account. Since transaction flow is completely control by the payer and payee does not have a direct communications with payer's FSP, the problem of traditional payment data flow and full-connectivity problem were solved.

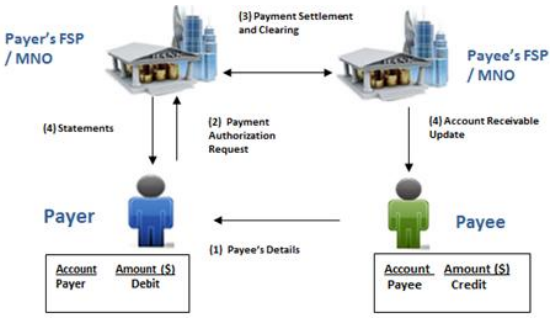

Fig. 3. Payer centric model

Looking into limitation of mobile devices and constraints of mobile network itself, it is recommended that the emphasis in designing the transaction flow of mobile payment data should focuses on minimizing the communication passes and traffic between the engaging parties and should keep the disturbance to the existing system as minimum as possible.

V. Security Requirements of Payment Transaction

Security serves as a fundamental critical success factor in relation to mobile payment system. If the security is low or unacceptable, then the payment system should never be introduced. Security is regarded as a challenging issue for mobile payment that can be challenged during sensitive and confidential payment information handling and transmission. Cryptography is the study of mathematical techniques related

to the aspects of information like confidentiality, message integrity, entity authentication etc. Cryptography provides the means to ensure that objectives of communicating parties are met[17]. The security requirements for payment transaction include authentication, integrity of payment data, confidentiality, anti-replay protection, anonymity, privacy protection authorization and non-repudiation.

A. Authentication and Confidentiality

Confidentiality is a protection against eavesdroppers who understand intercepted messages by keeping information secret from all but available for those who are authorized to see it. While, authentication means prove the identity of someone claiming to be a particular party. The security mechanism of payment 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. In general, authentication between payer and payer's FSP, and payee and payee's FSP will take place before payment transaction. Thus, the design of mobile payment schemes will be more focuses on authentication between payer and payee. Bothauthentication and confidentiality properties can be achieved by employing asymmetric encryption such as public key infrastructure (PKI), message authentication code (MAC), digital signature, or symmetric encryption.

B. Integrity of Payment Data

Integrity of payment data assures that the transaction data has not been changed or altered en route by unauthorized or unknown means. Integrity protects against the threat of corruption or modification of information (either accidentally or intentionally). The security mechanism of payment schemes should be able to prevent and detect alterations of the payment data from engaging parties and attack from outsiders such eavesdroppers, attackers, etc. Hashing algorithm, encryption or MAC can be applied to preserves the integrity of payment data,

C. Authorization

Authorization is the function of specifying access rights to resources, and it is very crucial for payment transaction. For example, payer's FSP cannot debit a payer's account balance without any authorization from payer. Bellare [18] considered a range of mandatory to optional authorization requirements for each party : FSP, Payer and payee, involved in the payment process when designing *i*KP protocol.

D. Non-Repudiation

Non-repudiation concerns about prevention of any deny for previous commitments or actions by the communicating parties and it works closely with authorization properties. The security mechanism should able to assure 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 FSP. With public key infrastructure, non-repudiation property can be achieved easily due to only corresponding payer have his own private key. However, the situation becomes more complicated if the payment protocol applying symmetric encryption to secure their payment transaction. Since the same key are shared between both parties, for instance between payer and payer's FSP, it is difficult to prove the genuineness of payment message. Accountability logic can be applied to analysis payment protocol in order to assurance the non-repudiation property. The accountability analysis of mobile 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. Traditionally, it is used only for resolving disputes among engaging parties.[19]

E. Privacy Protection

Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The privacy protection is includes identity privacy protection and transaction privacy transaction.

The payment 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.[4]

F. Anti-Replay Protection

Anti-replay protection ensures that if an attacker captures a message and transmit it again later, the receiver will not accept the message. This malicious activity known as Man-in-the-Middle attacks. The payment 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. To prevent replay attacks, insert either a nonce, timestamp or sequence number into each message that will never be used again in subsequent message. The engaging parties should not use the same nonce twice. The response from the server includes the same nonce sent in the request. By comparing a nonce in a request with previous request nonce, the server can ensure that the request is not a repetition of an earlier one. The client, in turn, can ensure that the response is not a repetition of a previous response

G. Anonymity

Anonymity refers to the personal identity, or personally identifiable information of that person is being unknown. Payers may needs protect their identity from eavesdroppers and (optionally) from payee, FSPs and PSPs. However, this property is only desirable for payment protocols that aim to imitate cash.

VI. Mobile Payment Schemes: A Brief History and Evaluation

Since the early of 21st century, a numerous of mobile payment schemes have been proposed to allow payment to be effected across the mobile networks. This section attempts to summarize the research of mobile payment protocol over the past ten years. It is undeniable that securing a mobile payment transaction over mobile network is more challenging than electronic payment protocol 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 These resulting existing Public Key Infrastructure (PKI) based electronic payment protocol such as Secure Electronic Protocol (SET) [20] and Internet Payment Protocol (*i*KP) [18] cannot be directly adopted in wireless environments as they designed for wired network and do not meet certain criteria in wireless environments.

The PKI is a technology and management needed for a certificate authority (CA) to create public key and private key pairs, distribute private keys, issue digital certificates, and maintain certificate revocation list. With public key encryption, client needs to perform high computational operations, and require sufficient storage in his mobile device to store public-key certificates. Although some mobile devices are equipped with special processors, performing such operations on them still requires longer procession time. 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.

In order to solve these problems, KSL payment protocol have been proposed [21] to solve the SET and *i*KP problems by reducing computational tasks at payer's wireless devices. In KSL payment protocol, all engaging parties except payer possess their own certificates. The payer is required to perform only symmetric cryptography operations and hash functions, which do not require high computation. Hence, the computational task and communication passes at payer side is reducing. Although KSL payment protocol has reduced the public-key cryptography to certain degrees, KSL payment protocols still impractically feasible apply into for mobile devices. Hence, in 2004, KSL payment protocol has been enhanced [2] by employing symmetric key operations not only for payer side but also for all engaging parties. This is a first attempt of applying symmetric key encryption for all engaging parties. There are no any public key encryption applied to this protocol, therefore reduces all parties' computation and communication passes.

Tellez *et al*. [3] proposed another anonymous protocol to solve the limitation of SET and iKP by employing a digital signature scheme with message recovery using self-certified public keys in order to reduce the communication passes between the engaging parties. Besides that, this protocol is a first attempt to solve the full-connectivity problem which does not consider the situation of payee who is not under the coverage of communication connection, or is unaffordable due to the inconvenience and costs.

TABLE I: Comparison of Related Works

Mobile Payment Schemes	KSL Protocol [7], [26]	Anonymous Protocol [8]	Private Protocol [9], [13], [27]	Secure Agent-based Protocol [10]
Actors	Payer, Payee, Payment Gateway , Financial Service Providers	Payer, Payee, Payment Gateway, Financial Service Providers	Payer, Payee, Mobile Network Operators	Payer, Payee, Payment Gateway, Financial Service Providers
Model	Bank Dominated	Bank Dominated	Mobile Operator Dominated	Bank Dominated
Transaction Flow	Payee Centric Model	Payer Centric Model	Payer Centric Model	Payee Centric Model
Security Protection				
Authentication & Confidentiality	Yes	Yes	Yes	Yes
Authorization	Yes	Yes	Yes	Yes
Non-Repudiation	No	No	Yes	No
Privacy Protection	No	Yes	Yes	Yes
Anonymity	No	Yes	No	No

Soo Fun *et al*. [8] proposed a private payment protocol based on Mobile Operator Dominated Model with the aim to provide a full privacy protection for all engaging parties. Besides that, it is also a first attempt to introduce the role of MNO as a financial services providers in order to reduce the banker's burden and trust dependency on them and simplifying the payment and billing process. In 2010, Soo Fun *et al*. [22] enhanced her protocol by focusing on non-repudiation aspect, with an ability to trace an action between parties engaging in payment protocol and then hold them accountable or responsible for their transactions.

In 2012, a Secure Agent-based Protocol [5] has been proposed with the involvement of intermediary (called as agent) in order to facilitate the payment transaction process. The main focus of this protocol is to solve the unreliability of wireless networks.

Besides that, several mobile payment protocol also have been proposed over [23]-[26] over the past ten year. Most of their works are concerning on reducing the work of cryptographic computational and communication passes between the engaging parties.

VII. Conclusions

This paper summarizes mobile payment protocol research

over the past ten years. Most of protocol schemes were concerning the reduction computational work and communication passes of PKI, either reduces the engaging parties possesses of secret key, using self-certified signature or applying symmetric encryption approach. However, with symmetric key encryption, there is a concern who is a originator of the payment message and who is accountable for the payment transaction since the same key are shared between both parties. Besides that, four significant macro-payment schemes: KSL protocol [21], Anonymous protocol [3], Private Protocol [4] and Secure Agent-based Protocol [5]have been selected and further discussed and compared. As a conclusion, to move forward, the community needs to adopt standardized and shared development with industry.

REFERENCES

[1] Durlacher, "Mobile commerce report," Technical Report of Durlacher Research Ltd, 1999.

[2] P. D. L. Kungpisdan and S. Bala, "A secure account-based mobile payment protocol," in *Proc. International Conference on Information Technology: Coding and Computing*, pp. 35-39, 2004.

[3] J. T. Isaac and S. Zeadally, "An anonymous secure payment protocol in a payment gateway centric model," *Procedia Computer Science*, vol. 10, pp. 758-765, Jan. 2012.

[4] T. S. Fun, L. Y. Beng, R. Roslan, and H. S. Habeeb, "Privacy in new mobile payment protocol," pp. 198-202, 2008.

[5] P. Limpittaya, M. Warasart, and S. Kungpisdan, "Design and analysis of a secure agent-based mobile bill payment protocol for bulk transactions," in *Proc. 2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE)*, pp. 71-76, May 2012.

[6] A. Cervera, *Analysis of J2METM for Developing Mobile Payment Systems*, University of Copenhagen, 2002.

[7] U. N. Agarwal and M. Khapra, "Security issues in mobile payment systems," *Journal of Computer Society of India*, vol. 35, no. 1, pp. 142 -152, 2008.

[8] T. S. Fun, "A lightweight and private mobile payment protocol," Universiti Malaysia Sabah, 2009.

[9] Visa launches mobile visa wave payment pilot in malaysia, *Avisian Contactless News*, 2007.

[10] Mobile visa wave: visa's contactless payment program for mobile phone in malaysia, VISA ASIA. (2007). [Online]. Available: http://www.visaasia.com/ap/sea/cardholders/cardsservices/visa_wave_mobile.shtml.

[11] H. Joachim, *Mobile Payment - the German and European Perspective*, Wiesbaden: Gabler Publishing, 2001.

[12] E. Vasenius, *Electronic Mobile Payment Service*, 2002.

[13] The International Business Awards: Valista. [Online]. Available: http://www.valista.com/market/market_operators.php.

[14] Trivnet Expands in LATAM. - Free Online Library - The Free Library. [Online]. Available: http://www.trivnet.com/products/overview.html.

[15] M. A. Me and G. Strangio, "Mobile local macropayments: security and prototyping," *Journal of IEEE Pervasive Computing*, vol. 5, no. 4, pp. 94-100, 2006.

[16] J. T. Isaac, J. S. Camara, S. Zeadally, and J. T. Marquez, "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2478-2484, Jun. 2008.

[17] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed. New Jersey: Prentice Hall, 1999.

[18] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. V. Herreweghen, and M. Waidner, "Design, implementation and deployment of the i kp secure electronic payment system," pp. 1-20, 2000.

[19] T. S. Fun, L. Y. Beng, S. Alias, and N. M. Rusli, "Accountability analysis of mobile payment protocol," 2012.

[20] Mastercard and Visa, *SET protocol specifications*, 1997.

[21] L. Kungpisdan, S. Srinivasan, and B. P. Dung, "Lightweight mobile credit-card payment protocol," *Journal of Lecturer Notes in Computer Science*, no. 2904, pp. 295-308, 2003.

[22] T. S. Fun, L. Y. Beng, and I. Technology, "Non-repudiation mobile payment protocol with symmetric approach school of informatics science," Universiti Malaysia Sabah.

[23] C. Huaihu, W. Lubin, and Z. Jianming, "A trust-aware mobile multiple micro-payment mechanism based on smart agent in distributed environment," in *Proc. 2007 2nd International Conference on Pervasive Computing and Applications*, pp. 314-318, Jul. 2007.

[24] A. A. Tabandehjooy and N. Nazhand, "A lighweight and secure protocol for mobile payments via wireless internet in m-commerce," in *Proc. 2010 International Conference on e-Education, e-Business, e-Management and e-Learning*, pp. 495-498, 2010.

[25] D. M. Tripathi and A. Ojha, "LPMP: an efficient lightweight protocol for mobile payment," in *Proc. 2012 3rd National Conference on Emerging Trends and Applications in Computer Science*, pp. 41-45, Mar. 2012.

[26] Y. Huang, S. Shieh, and F. Ho, "Payment model supporting multiple merchant transactions," vol. 19, no. 5, pp. 453-465, 2000.

Tan Soo Fun received Bachelor of Information Technology (majoring in E-Commerce) and Master of Science (Computer Science) from Universiti Malaysia Sabah (UMS) in 2006 and 2009 respectively. She is currently working as a lecturer position in School of Engineering and Information Technology at Universiti Malaysia Sabah. Her research interests are security of communication protocols, secure payment transaction, cryptography protocol and data-centric security. She is a member of Information Security Professional Malaysia (ISPA) and International Association of Computer Science and Information Technology (IACSIT). She is also a IBM Certified Academic Associate.

Leau Yu Beng received B.S (Multimedia Technology) degree from Universiti Malaysia Sabah, Malaysia in 2004 and M.SC. (Information Security) from Universiti Sains Malaysia (USM), Malaysia in 2007. Currently, he is a Ph.D candidate in National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia. His current research interests are intrusion alert detection and prediction. He is a member of Information Security Professional Malaysia (ISPA) and International Association of Computer Science and Information Technology (IACSIT). He is also a IBM Certified Academic Associate.

Mohd Norhisham Razali received B.Sc. (Hons) (IT) and M.SC (IT) from Universiti Teknologi Mara in 2008 and 2009 respectively. He is currently working as a lecturer position in School of Engineering and Information Technology at Universiti Malaysia Sabah. His research interests are User Science, Human computing and sustainable software design. He is a member of International Association of Computer Science and Information Technology (IACSIT) and also a Microsoft certified.