Reliable OSPM Schema for Secure Transaction using Mobile Agent in Micropayment System

Chitra Kiran N
Asst. Prof: Dept of Electronics & Communication Engg.
Sai Vidya Institute of Technology
Bangalore, Indian
E-Mail: chitrakiran2002@yahoo.co.in

Dr. G. Narendra Kumar
Prof.: Dept. of Electronics & Communication Engg.
UVCE
Bangalore, India

***Abstract*— The paper introduces a novel offline payment system in mobile commerce using the case study of micro-payments. The present paper is an extension version of our prior study addressing on implication of secure micropayment system deploying process oriented structural design in mobile network. The previous system has broad utilization of SPKI and hash chaining to furnish reliable and secure offline transaction in mobile commerce. However, the current work has attempted to provide much more light weight secure offline payment system in micro-payments by designing a new schema termed as Offline Secure Payment in Mobile Commerce (OSPM). The empirical operation are carried out on three types of transaction process considering maximum scenario of real time offline cases. Therefore, the current idea introduces two new parameters i.e. mobile agent and mobile token that can ensure better security and comparatively less network overhead.**

Keywords-component; Micropayment System, Mobile Agent, Hash Function, Wireless Adhoc Network

I. INTRODUCTION

The area of m-commerce [1] has introduced a massive volume of applications and services on smart-phones or tablet PC. Although there are bunch of application already in use in m-commerce, but application based on payment system is still under the vulnerable zone of security loopholes. The prior research work has almost focused on providing security for online payment system. But the need of security for offline payment system has been highlighted in my previous work [2]. The investigation for m-payment has attracted the researchers for long time and has also posed significant issues in m-commerce to build its security. It has been seen that in the current mobile payment system, the third party and the financial institutions are considered to be trustworthy and reliable while there is not much focus on the internal threats by any untrusted party. However, there is always feasibility that the employees of any financial institutions might pose a lethal threat sometimes. Hence, it is critical to evaluate security in payment system in terms of the internal threats and attacks by some untrusted parties if the mobile cash system is deployed in real time. The offline payment systems can be categorized into 4 types [3] e.g. TYPE-1: Here, the user secret key is directly stored in bank database as the identification information and embedded in the withdrawn e-cash. TYPE-II: Here, the public key of user is stored in the bank database as identification parameters while corresponding secret key is only known to user (User's public key has no certificate). TYPE-3: The public key of the user is registered as identification parameters and payments are made with keys and certificates from the public keys. TYPE-4: Here, the secret key has two section-one known to both bank and user while other is estimated by the user. The corresponding public key and certificate are known only to the customer. Out of all the above mention 4 types of security measures, the last one can be considered as optimal secure as information furnished to the internal nodes are very limited and renders internal attacks more difficult.

The current article will introduce the security of the existing payment system that addresses internal threats. The article also addresses certain security protocols that are very recently explored along with discussion on the solution towards prevention of such malicious activities on offline payment system. The current work considers usage of micro-payment [4] system as medium of payment of mobile commerce. The work has also evaluated other protocols for micro-payment systems in mobile information content application that was accomplished by furnishing smart-phone based micro-payment application with well user-defined customization.

It is seen that a mobile enabled application that supports m-commerce application very often requires certain advanced mark up oriented scripts for mobile client interfaces that supports a large scale variation of m-commerce and other mini-applications too. The current work also introduces prime operation for the novel scheme of offline payment scheme for large scale operation considering large number of users that furnishes more flexibility, more mobility, and ensures security in micro-payment scheme proposed. The current work is inspired by the prior research conducted by Jianming Zhu [5]. The prime objective of the research work is to introduce a novel offline micro-payment schema in order to furnish better security in wireless transaction and communication system. Section 2 discusses in brief about the most relevant prior research work done in the similar area of security in Micropayment system. Section 3 highlights about the aspects prominent aspects of micropayment system that has been found to use in majority of prior studies in the same field. Section 4 illustrates about the proposed system that is followed by brief description of adopted methodology. This section also discusses three different secure offline transaction schemes along with illustration and finally in section 5 we make some concluding remarks.

II. Related Work

Zhi-Yuan Hu [6] has introduced a novel and realistic authentication system termed as anonymous micropayments authentication that is targeted for micropayments in mobile data network. However, some associated flaw has been explored in the work for frequent issues of verification procedures based on symmetric key cryptography.

Xiaoling Dai [7] has conducted a study on various micropayment procedures in offline mode with multiple availability of vendors.

Min-Shiang [8] has introduced numerous micro-payment designs that is based on one-way hash chain and performed appraisal on certain literatures on supporting multiple payment system. The author has also introduced a novel micropayment scheme that accomplishes three objectives e.g. i) micro-payment multiple transactions, ii) service providers, and iii) anonymity.

Samad [9] has discussed a trust based framework from user point of view and combined it with micropayment scheme. This trust framework was found to be supported by various micropayment providers and ensures the users that they will not be levied for in case the product is not acceptable or it is corrupt.

Ming e.t. al [10] have analyzed a variety of probabilistic micropayment policies to exhibit that the scheme by Rivest may minimize the administrative cost of the financial institution, however the framework is found to be accompanied by infrequent computational overhead to the vendor module.

Wuu [11] have proposed a secure and efficient off-line micro payment policy that deploys coin chain method to design the coin that the authentication of coin can be done quickly by hash computation. The policy was also found to guarantee that the coins could only be deployed by their vendor, and safeguards the confidentiality of the consumer module.

Katiyar e.t. al. [12] have discussed a technique about use of Elliptical Curve Cryptography (ECC) and have presented a review on the current deployment of ECC in the pervasive computing environment.

Osman and Taylor [13] have proposed a framework where they have used three key distribution considerations in execution of a fully distributed trust and reputation organization for adhoc m-commerce trading systems that also enhances the periodic reputation data, its associated storage and finally reliability.

Mousumi and Jamil [14] have illustrated a novel cost efficient push pull services that uses SMS based mobile banking concept for addressing issues for reliability in 24 hours banking convenience targeting to assist the online customers to stay on top of any fresh alteration to be made in their current account or even deposit account or loan through SMS.

Arogundade e.t. al. [15] have introduced a framework with an open network system that can become accustomed to users dynamic requirement as well as permitting a reliable, valuable and secured transaction using any customers' bank account.

Partha e.t. al [16] have presented a new technique by utilizing cancelable biometric features for safeguarding and storing the fingerprint template by generating Secured Feature Matrix (SFM). The author also suggested that the generated keys for cryptographic techniques can be applied in cryptography for data encryption or decryption.

Al-Fayoumi [17] have discussed an important e-payment protocol called as 'pay-word scheme' and performed scrutiny on its merit and demerit features along with study of its associated constraints that progresses the policy and restore all distinctiveness features intact without compromising any of the attributes of security robustness.

Chaudhary e.t. al [18] have discussed in his work about an analysis that is conducted for the security objective of micro-payment alongside a non-micro-payment credit systems for file sharing applications.

Ayo and Ukpere [19] have proposed an integrated smart card-based ATM card using biometric-based cash slot machine for all secured financial online transactions.

Wang [20] have presented a secure and efficient payment system that is incorporated with smart hand-held device, wherein customers are not limited to procure electronic currencies with the permanent face-value.

Several studies are conducted within the area of authentication and payments. Some studies [21-24] talked concerning the various techniques that may be wont to build a secure authentication methodology. These techniques embrace two-factor, single sign-on, robust and social authentication. However, most analysis has been that specialize in plat-form (operating systems e.g. iPhone OS, golem etc.) dependent authentication solutions, whereas less attention are paid on platform independent solutions. One could conclude from this trend that platform dependent solutions are safer. With this study, a researcher can have a tendency to highlight that employing a platform independent authentication methodology is adequate while not compromising the safety of the authentication answer. As an example, resisting victimization using multiple factors will maximize the safety of the authentication method. This idea of using multiple factors to strengthen the authentication methodology is supported in many prior studies [21][22] and [24]. Two different studies titled ECC-based Wireless native Payment theme [25] and on-line payment service providers and client relationship management [26] presents two different methods to conduct secure transactions.

III. Micropayment System

A. About Miropayment System

A micropayment system can be defined as a financial transaction that involves a very small amount of money and usually one that occurs online [27][29]. One of the impediments towards the technical adoption of micropayment system is the cost associated with the operation of the system that is quite inevitable. This is the prime reason why customers hesitate to use micropayment system even if the transaction amount may be small. Micropayments have to be appropriate

for the transaction of non-tangible merchandise over the Internet which inflicts necessities on speed and cost of processing of the payments: delivery occurs nearly immediately on the Internet, and often in arbitrarily small pieces. The prime contradiction in this concept is that although there is a threshold fixed for the cost to be lowered and nominal, but very few services are found to be much reliable in micropayment system in majority of the cases [28]. So, the evaluation criteria of micropayment systems should include [28]:

- *Ease of use*: The targeted micropayment application should be highly comfortable when it comes to usage by normal and ordinary customers. Not only this, there is a lack authorization procedure and secure PIN number usage that needs to be fed every time during course of transactions.
- *Security*: The prime aim of any security protocol is to maintain confidentiality, privacy, anonymity, and non-repudiation for any services offered to the most vulnerable networking situation like wireless environment. The application can be incorporated with security features for ensuring the trust and faith of clients to the targeted products and applications of micropayment system.
- *Anonymity*: The private communication of the customer module should be maintained anonymous and thereby their private information should be protected. Ensuring untraceability is the next prominent requisites for the secure micropayment system.
- *Divisibility*: The protocol supports multiple denominations and a range of payment values.
- *Performance*: The protocol provides high-volume payment support.
- *Robustness*: The protocol is tolerant of network traffic jam and broker/authorizer down-time.

Table 1 Comparison of E-commerce payment methods

Property	**CyberCash [28]**	**MPay [28]**	**PayWord [28]**	**NetPay [28]**
Ease of Use	Low	High	Medium	High
Security	High	Medium	Low	Medium+
Anonymity	Low	Low	Low	Medium+
Divisibility	Very High	Very High	High	High
Performance	Very Low	High	Medium	Very High
Robustness	Low	High	High	High

Hence, it can be seen that there is a dire requisites for an effective and secure micropayment system that has highest technical adoption from normal and common people. Because of security loopholes on wireless networking environment, if customer become hesitant to use it, this field cannot be advanced for understanding its future usage and innovation. Ultimately, it was explored that majority of the micropayment system are accompanied by security loopholes that requires serious attention in research domain.

IV. PROPOSED SYSTEM

The current offline payment system in m-commerce is designed considering multiple users (vendor) that is appropriate for real time mobile network scenario. The proposed protocol now termed as Offline Secure Payment in Mobile Commerce or OSPM deploys the authority that has to be signed by mobile agent and m-token key authorized by merchant. The authority file that is signed is utilized by merchant in order to confirm the transaction parameters and authorized m-token that needs to be used in order to resist any malicious activity from any customer. The similar phenomenon can also be used to determine any issues with merchants too. The operational charecteristics of OSPM is discussed here as following:

A case study is assumed with customer (C), service provider (S_P), merchant (M), and mobile-agent (M_a). It is considered that M_a is a trusted and reliable member and is supported by S_P, M, and C. However, the reliability and trustworthiness is not assured for the customer (C) and merchant (M). The customer (C) can open an account and credit financials with the M_a, where the transaction for payment process can also include M, S_P, C, and M_a. The mobile agent (M_a) is designed for customer (C) as well as for depositing the merchants (M) account and debiting the customer (C) account.

For the empirical analysis, let us consider X_{ID} as false name of assumed X party in offline-transaction system distributed by Mobile-agent (M_a), Pub_Key_X be public key of X, DS_X be digital signature of X, DS_X^Y be Y signed by X, $Pub\_Key_X^Y$ be Y is encoded by public key of X, and DS_{XS}^Y be Y signed by X using asymmetric key of X. Therefore, in the proposed OSPM schema, the considered modes of transactions are as follows:

- Customer (C) to Mobile-agent (M_a).
- Customer (C) to merchant (M).
- Merchant (M) to Mobile-agent (M_a).

Customer (C) to Mobile-agent (M_a): In this type of transaction, the customer C needs to be enrolled and send secure values along with the quantity of the password in a secure channel maintained by C to Mobile agent (M_a).

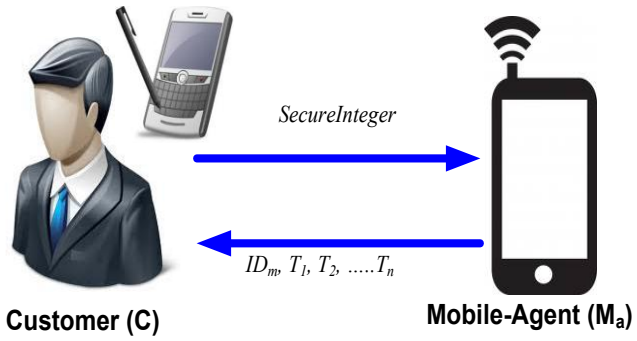

Fig 1 Customer purchase m-tokens

The M_a withdraws amount from account of C and design a secure channel T_o, T_2, T_3, . . ., T_n, T_{n+1} that satisfies T_i=hash(T_{i+1}), where i=n, . . , 0. The square root of T_o will be used to confirm the authenticity of the secure channel T_1, T_2, …., T_n by nodes and the M_a. The final value of Tn+1 is retained by Ma to be utilized for resisting the initial node from any malicious activity in that secure channel. The nodes then receive the m-token ID_m and the T_1, T_2, . . , T_n that are encoded by public key of C from mobile agent (V2=ID_m, T_1, T_2, . . , T_n). The Ma then estimates the authorization for the secure channel A={ID_m, T_o} and corresponding sensitive information is stored.

Customer (C) to merchant (M): This set of transaction introduces secure communication between C and merchants (M_1, M_2) in the path of a content delivery from merchants to C. The price of the digital content is known to the C from merchant's location.

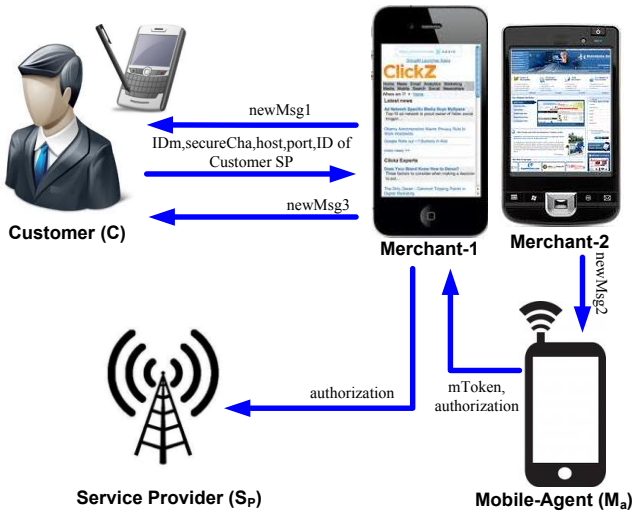

Fig 2 Customer purchases digital content

Therefore, M1 forwards the host request and port information to C when C tries to buy the digital content over wireless network from their mobile interface. The secure protocol than evaluate the host and port information recent furnished with prior records. In case the furnished information varies, the OSPM schema forwards a message that consists of ID_m, secure channel info, host and port info, and identity of C's S_P. If the customer C makes the purchases for first instant than M forwards ID_m with new message to the S_P for authorization request. The SP then forwards token (ID_X, 1) along with the secure channel authorization and re-forward them to M_1. The authorization and the m-token confirm M1 to evaluate the secure channel using square root of T_o and exchange with S_P. The furnished information is evaluated by considering hash function in the sequence of T_1 and then T_2 and so on. Therefore, it is very difficult for intruders or any unreliable parties to create T_1 even with knowledge of T_o as the creation of a secure value along with hash function to T_o is computationally infeasible due to potential charecteristics of invariant hash function. If the assumed constructs are legitimate than M_1 will be recorded for later usage. The M_1 then signs the current tokens that are forwarded to S_P. This is done for resisting that a merchant is not authorized to receive authorization if the prior merchant posses the content already. The customer C could continue to purchase other digital contents with M_1 itself. However, when C wants to opt for different merchant M_2, the M_2 has to request for current m-token and the authorization from M_1 in order to confirm the authenticity of m-token when C swaps the option from M_1 to M_2. Whenever, C wants to buy digital contents from M2, M2 needs to forward the information related to price, host and port to the OSPM schema that again compares the furnished host and port information with prior one in records. In case the information differs, a new secure message is created {ID_m, T_1, T_2, …, host & port, ID_S_P}. This newly generated message is forwarded to M_1 for authorization and m-token. Then M_1 signs the m token ($ID_{M1,\,i}$) along with secure channel, authorization, and forwards them to M_2 where the variable i specifies the counter of the last authorization used by M_1. This m-token can be deployed for any contradiction among different merchants and the authorization is deployed for any further offline payment system and to use the secure information from the service provider S_P. Once the secure information is authenticated and confirmed by M_2, the secure channel using the authorization and the m-tokens, the customer C will be authorized to receive the digital content from M_2. Therefore, in case of passivity of M_1 system, M_2 can broadcast the message to S_P and get authorization from S_P along with m-tokens. Therefore, the customer C could be able to make purchase even with M_2

Merchant (M) to Mobile-agent (M_a): This type of transaction is basically intended for offline secure exchange of information processing for Mobile-agent (M_a). One of the most real time fact is that all the merchants M will be require to forward all the sensitive information of secure channel that they received from customer C and exchange them in terms of commercial amount in bank at the end of final transaction offline. In order to perform this process, a merchant must collect the secure channel information by each m-tokens and their identity, and forwards the newly designed message {ID_m, ID_i, imbursement}. The Mobile-agent (M_a) will be required to authenticate each secure channel information received from the merchant by conducting hash function and reading the quantity of secure channel information. In case all the furnished secure channel information is legitimate then SP credits the amount to

merchant's account and forwards an acknowledgement too {BalanceSheet$_{INFO}$}.

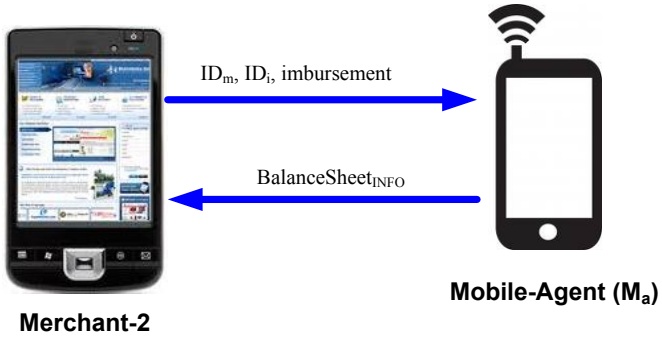

Fig. 3 Merchant-and Mobile Agent exchange transaction

V. CONCLUSION

The current work is focused on designing an offline payment system in mobile commerce specifically taking micro-payment as case study. Majority of the work done in prior research work is concentrated on online safety along with service provider too. But, in this work, it can be seen that S_P also requires generating secure supportive hash value for every secure channel information that is sent via smart-phone of the customer C. Then S_P forwards the legitimate secure channel information and subsequent supportive hash vale to the merchant in every transactions offline. The m-token in system schema considered in customer and merchant dependent. This phenomenon restricts the portability of the secure channel information to a greater extent.

The current work therefore has introduced a real time offline payment system from a Mobile-agent (M_a) and service providers (SP) and termed the schema as OSPM. The proposed schema restricts the customers for performing an malicious activity even in offline mode using m-token. Therefore, the proposed system is found to satisfy all the critical security requirements in micro-payment system. The proposed schema is also cost-effective as it do not posses any operation with public key for any types of purchases being made.

The secure channel information in the OSPM schema are not specific to customer C or merchant M thereby permitting secure offline transaction for payments evaluated for large number of merchants over the network. One of the noteworthy advantage of the proposed scheme is that OSPM transfer the authenticated network channel issues from Mobile-agent (M_a) and allocates it among all the merchant. Hence this schema balances the network and processing overhead from merchant over the network. Another advantage is that OSPM schema assures safe exchange of legitimate m-token for credit to the merchant as well as it also permits the merchants to concentrate on content scheduling and Mobile-agent (M_a) to furnish operation related to management of amount in their registered financial institution. The transaction between mobile user and vendor has dual benefits. Primarily, the transfer of the secure message from M_1 to M_2 does not include any mobile agent (M_a) and it diminishes the network overhead of the mobile agent (M_a). Secondarily, the consecutive secure message posses the m-token of the authorization for which it resists the customer C from any sorts of malicious activities while in offline even when C swaps to another merchant M_2. Exactly, this OSPM scheme thereby renders a novel, cost-effective, and secure network with better business role in m-commerce.

REFERENCES

[1] http://en.wikipedia.org/wiki/Mobile_commerce. Accessed on 20th August, 2012

[2] Kiran N.C., Kumar, N, "Implication of Secure Micropayment System Using Process Oriented Structural Design by Hash chaining in Mobile Network", *IJCSI International Journal of Computer Science Issues*, Vol. 9, pp, no 2, January. 2012

[3] Nishide,T., Miyazaki, S., Sakurai, K, "Security Analysis of Offline E-cash Systems with Malicious Insider," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol.3, no.1/2, pp. 55-71, 2011

[4] http://en.wikipedia.org/wiki/Micropayment. Accessed on 20th August, 2012

[5] Jianming Zhu; Ninghong Wang; JianFeng Ma, "A micro-payment scheme for multiple-vendor in m-commerce," *E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference on* , vol., no., pp.202,208, 15-15 Sept. 2004

[6] Zhi-Yuan Hu; Yao-Wei Liu; Xiao Hu; Jian-Hua Li, "Anonymous micropayments authentication (AMA) in mobile data network," *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies* , vol.1, no., pp.,53, 7-11 March 2004

[7] Xiaoling Dai; Ayoade, O.; Grundy, John, "Off-Line Micro-Payment Protocol for Multiple Vendors in Mobile Commerce," *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on* , vol., no., pp.197,202, Dec. 2006

[8] Hwang, M.S., Sung, P.S., "A Study of Micro-payment Based on One-Way Hash Chain", *International Journal of Network Security*, vol-2, no-2, pp.81–90, March. 2006

[9] Kardan, S., Shajari, M., "A Lightweight Buyer's Trust Model for Micropayment Systems", *WSEAS Transactions on Information Science & Applications*,vol.5, no.7,pp.1170-1179, 2008

[10] Yen, S.M., Chen, C.N., Lin, H.C., Wu, J.M., Lin, C.T., "Improved Probabilistic Micropayment Scheme", *Journal of Computers*, vol.18, no.4, January 2008

[11] Wuu, L.C., Chen, K.Y., Lin, C.M., "Off-Line Micro Payment Scheme with Dual Signature," *Journal of Computers*, vol.19, no.1, Apr. 2008

[12] Katiyar, V., Dutta, K., Gupta, S., "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment," *International Journal of Computer Applications*, vol.11, no.10, December 2010

[13] Osman, H., Taylor, H., "Design of a Reputation System for M-Commerce by Ad Hoc Networking", Technical Report of Heriot-Watt University, pp-1-7, 2010

[14] Mousumi, F., Jamil, S., "Push Pull Services Offering SMS Based m-Banking System in Context of Bangladesh", *International Arab Journal of e-Technology*, vol. 1, no. 3, January 2010

[15] Arogundade, O.T., Motunrayo, I.A., Ademola, O., "Developing a Usage-centered e-Payment Model using Open Network System", *International Journal of Computer Applications*, vol.12, no. 6, December 2010

[16] Ghosh, P.P., Pattnaik, S., Verma, G.,"Improving Existing e-payment Systems by Implementing the Concept of Cancelable Biometrics", *International Journal of Engineering Science and Technology*, vol. 2, no. 7, 2010

[17] Al-Fayoumi, M., Aboud, S., Al-Fayoumi, M., "Practical E-Payment Scheme", *International Journal of Computer Science Issues*, vol. 7, no. 7, May. 2010

[18] Chaudhary, K., Dai, X., Grundy, J., "Experiences in Developing a Micro-payment System for Peer-to-Peer Networks", *International Journal of Information Technology and Web Engineering*, vol. 5, no. 1, 2010

[19] Ayo, C.K., Ukpere, W.I., "Design of a secure unified e-payment system in Nigeria: A case study", *African Journal of Business Management*, vol. 4(9), pp. 1753-1760, August. 2010

[20] Wang, J.S., Yang, F.Y.,Paik, I., "A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices," *International Journal of Computer Science and Network Security*, Vol.11 no.6, June. 2011

[21] Aloul, F.; Zahidi, S.; El-Hajj, W., "Two factor authentication using mobile phones," *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* , vol., no., pp.641,644, 10-13 May. 2009

[22] Niu Ying; Zhao Yao; Zou Hua, "The study of multi-level authentication-based single sign-on system," *Broadband Network & Multimedia Technology, 2009. IC-BNMT '09. 2nd IEEE International Conference on* , vol., no., pp.448,452, 18-20 Oct. 2009

[23] Do van Thanh; Jrstad, I.; Jonvik, T.; Do van Thuan, "Strong authentication with mobile phone as security token," *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on* , vol., no., pp.777,782, 12-15 Oct. 2009

[24] Soleymani, B.; Maheswaran, M., "Social Authentication Protocol for Mobile Phones," *Computational Science and Engineering, 2009. CSE '09. International Conference on* , vol.4, no., pp.436,441, 29-31 Aug. 2009

[25] Gianluigi Me; Strangio, M.A., "EC-PAY: An Efficient and Secure ECC-Based Wireless Local Payment Scheme," *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on* , vol.2, no., pp.442,447, 4-7 July 2005

[26] Smith, A.D, "Online payment service providers and customer relation-ship management", in *Int. J. Electronic Finance*, vol. 2, no. 3, pp.257–283, 2008

[27] http://en.wikipedia.org/wiki/Micropayment [Accessed on 30th July, 2011]

[28] Xiaoling Dai; Grundy, John; Lo, B. W N, "Comparing and contrasting micro-payment models for e-commerce systems," *Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 International Conferences on* , vol.6, no., pp.35,41 vol.6, 2001

[29] Kiran, N.C.; Kumar, G.N., "Building robust m-commerce payment system on offline wireless network," *Advanced Networks and Telecommunication Systems (ANTS), 2011 IEEE 5th International Conference on* , vol., no., pp.1,3, 18-21 Dec. 2011