Journal of Computer Science 5 (12): 1034-1041, 2009
ISSN 1549-3636

A Prototype Design for Enhancing Customer Trust in Online Payments

Thair Al-Dala'in, Peter Summons and Suhuai Luo
School of Design, Communication and Information Technology,
Newcastle University, Newcastle, Callaghan NSW 2308, Australia

Abstract: Problem statement: The adoption of mobile device technology can contribute significantly to enhance customers trust in online payment systems. **Approach:** The perceptions and preferences of online shoppers are influenced by several key factors which serve to both enhance and compromise this trust and in turn affect a customer intentions and behavior in relation to use online payment systems. The first part of the research was a quantitative study to investigate these factors. In the second part of this research, a mobile payment model for online payment systems was proposed. In this model, the customers do not need to trust merchants during the transaction because merchants will not act as an intermediary between customers and the acquirer. Customers can therefore send their financial details without concern of disclosure, or potential misuse by the merchant. **Results:** In this study, the key factors influencing to adopt mobile payment systems were identify. The proposed model was developed and an analysis of the model architecture against conventional online payment systems was discussed. **Conclusion/Recommendations:** The significance of this research comes from providing a practical mobile payment model as a possible step towards increasing customer acceptance of online shopping and increasing their trust in online payment systems. The new model focuses on enhancing the feeling of security of the use of an online payment system and satisfying the security requirements.

Key words: Trust, security, online payment, e-commerce

INTRODUCTION

Electronic commerce (e-commerce) has been growing at an exponential rate in recent years and has become an essential tool for financial services. The nature of the online interactions used in e-commerce systems, without the cues that face-to-face contact affords, requires trust for successful communication and secure payment. A fundamental requirement must be that customers ought to have absolute trust in the online system in which they participate. Therefore, any adoption of e-commerce must consider trust as an important determinant of adoption behavior. At the outset it is appropriate to note several different understandings of trust which have been used in the literature, for example trust has been defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party[1]. Trust is the enabling of confidence that something will or will not occur in a predictable manner. The enabling of confidence is supported by identification, authentication, authorization and availability[2]. Trust has also been defined in the electronic payment system as an important (subjective) security feature which Pousttchi[3,4] stated as the degree to which a customer believes that using a particular electronic payment system would be secure.

Hundreds of electronic payment (e-payment) services as well as Internet banking were introduced all over the world by using mobile devices. Dahlberg *et al*.[5] questioned why Visa Electron and PayPal have succeeded while e-payment services using mobile devices have not worked as well. Therefore, we need to carry out more studies in order to attract customers, merchants and banks to use mobile devices in online shopping. An apparent conclusion is that these services have failed to meet customers' payment needs[6].

Related work: Several trust models have been proposed in e-commerce to deal with customers' trust; such as the reputation models[7]; mathematical trust model[8] and computational trust models[9]. Zhang *et al*.[8] proposed a computational model ERS2G based on user's attitudes, opinions and motivations, which attempted to improve

Corresponding Author: Thair Al-Dala'in, School of Design, Communication and Information Technology,
Newcastle University, Newcastle, Callaghan NSW 2308, Australia

the trust level and to provide some insight for customers of e-commerce. They proposed a model based on the idea of reputation aggregation in Role Play Games. Their model combines the concepts of a reputation system and the mathematical trust model by using a representation of the customer's direct experience, customer evaluations and recommendations, digital credentials and also certificates and system guarantees, to provide a metric for the trust level.

Reputation models have also been used as methods to enhance trust in e-commerce environments and so help customers make decisions about who to trust in the future. Organizations such as eBay and BizRate have used aggregated feedback from many of their customers to enhance the trust of potential future customers in them. However, these systems still encounter significant challenges[10]. For instance, feedback can be erased if merchants change their name and a dishonest participant can use this to build a new business and lose their bad reputation. However, the first thing customers usually think of in relation to trust is the question of security in electronic transactions. Therefore, the most security protocols currently popular are SSL/TLS (Secure Socket Layers/Transport Layer Security)[11] and SET (Secure Electronic Transaction)[12]. There are still some challenges and problems for its acceptance in credit card payments. One of these problems is that, while SSL solves the problem of transmitting secure information between the customer and the merchant, it does not help with the rest of the transaction. SET has not been widely adopted for use[13]. One of the most important obstacles to SET implementation is that the protocol is very complex and confusing for its users.

On the other hand, with the popularity and availability of mobile devices such as, mobile phones, PDAs (personal digital assistant) and laptop computers, these devices have became effective for managing payment and banking transactions by providing security and convenience advantages. Some solutions have been proposed the use of the Global System for Mobile communications (GSM) in e-commerce such as[3,4] and Bottoni *et al*.[14] showed that mobile devices fulfill the security requirements and thus can be used as a personal trusted device. A proposal by Joris *et al*.[15] tried to enhance the security of e-payment systems by combining the features of SSL/TLS with GSM. The merchant can rely on the GSM network to ensure they receive an authenticated payment from the customer (via the network operator later on). The purpose of this model is to use GSM as an extension to the Internet to provide security and functionality. The payment protocol proposed by Vorapranee *et al*.[16] is focused on eliminating the possible security risk of storing debit/credit card details at the merchant's server. The protocol provides user authentication and card detail confidentiality based on GSM data confidentiality.

As result, the trust models have been proposed to solve specific trust issues in e-commerce environments without considering the relationship between security and trust[17]. A trust and reputation model largely relies on customer feedback and focuses only on evaluating and establishing a trust relationship without consideration of the security requirements in their design. It was identified that customer trust in these models is influenced by customer evaluation from the amount of experience customers have and the degree of associated satisfaction. However, these mechanisms do not guarantee protection for customers and customers may therefore misinterpret cues which may be misleading. Furthermore, in reputation models, it is possible that some users may provide false feedback to intentionally raise the reputation of a service.

MATERIALS AND METHODS

The first part of the research is to investigate the perceptions and preferences of online customers and their current use of mobile payment systems. It attempts to identify key factors influencing online customers trust and the capacity to adopt mobile payment systems. An on-line survey developed using the insights gained from the literature and a further discussion meeting in order to obtain the first part data. Structural Equation Modeling (SEM) with AMOS software was used to examine the research data. The second part of the research is to present the design of a practical mobile payment model for online payments.

RESULTS

The online survey was advertised on various Internet group websites and Blackboard sites at The University of Newcastle, Australia. Participants are directed to a web page where there is full disclosure of the research (with a link to the research information statement). There is a consent button making participants aware that they are consenting to the survey. 118 cases in total were gathered over a period of two months. There were 17 unusable cases due to missing values or were inappropriate in nature. Thus, 101 cases were finally analyzed. The sample population consisted of individuals with experience using e-payment systems.

For the initial assessment, we followed the instrument validation process suggested by Straub and

Boudreau[18,19]. 'Internal consistency reliability' is tested first and then 'construct validity'. Cronbach's alpha coefficients were used for assessing the reliability of the items. Principal Component Analysis using Varimax Rotations were used for assessing the construct validity of the items. The resulting alpha value was 0.87. Joseph, *et al*.[20] suggests that the lowest limit for Cronbach's alpha should be approximately 0.70. Therefore, all constructs in the research conducted demonstrated acceptable reliability.

Most survey participants were aged in their twenties or thirties with a high level of education. 43% of the participants were female, 57% were male. Detailed descriptive statistics relating to the respondents' characteristics are shown in Table 1.

The result of the survey shows that about 12% of the participants had experience using their mobile phone for the purpose of e-payment. From the 88% who had not used their mobile phone for e-payment before, 67% expressed their willingness to use their mobile phone for online payments in the future, provided it was available a payment option over the Internet. Detailed statistics relating to the participants' current use of e-payment systems are shown in Table 2.

Table 1: Descriptive statistics of respondents' characteristics

Measure	Items	Percent
Gender	Male	57
	Female	43
Age	18-24	48
	25-34	41
	35-44	4
	45-54	6
	55-64	1
Highest educational level	University student or graduate	87
	TAFE student or graduate	6
	High School (HSC) or equivalent	7

Table 2: Descriptive statistics of respondents' current use of e-payment systems

Measure	Items	Percent
Used a mobile phone for online payment	Yes	12
	No	88
Degree of used a mobile phone for an online payment	6 months or less	31
	Between 6 months and 1 year	38
	Between 1 and 2 years	8
	More than 3 years	15
Degree of like using a mobile phone for online payments	Very much	62
	Not much	38
	Not at all	0
Degree of recommend using a mobile phone for online payments	Yes	62
	No	38

The survey results indicate that: the shopper's ability to control their transaction; the security built into a mobile phone payment system; the prior perception of security evidence; the perception that no personal data is sent through the merchant in a transaction; the perceived ease of use and the perceived usefulness; were all significant factors in affecting people to adopt the mobile payment model as a new payment system. The results also indicate that the customer's adoption of the mobile payment model will increase their intention to purchase online in the future.

Mobile payment model development: using the results from the first part of the research, a mobile payment model is developed in which customers trust in the use of online payments will be enhanced. This is achieved by changing the traditional electronic payment transaction processes between customers and merchants through the use of a mobile device, where the device participation in the payment processes gives customers the feeling of being in control of the payment process. The new payment model allows customers to purchase services/goods from merchant's webpage and let them authorize the payment by using their mobile device. A webpage simulating a merchant's webpage was designed. The merchant's details as well as the acquirer's details are stored in servers using Oracle Database. The servers allow multiple clients access, concurrency control such as mutual exclusion implemented as well as Multithreading using Web programming environment. The customers can use any Personal Computer (PC) to connect, browse and select the goods/services from a merchant's webpage. The mobile phone in this model is implemented as a program installed at a PC and it plays the communication rules as a real mobile phone.

Model components: Six principal participants are involved in the payment model as describe (Fig. 1):

- Customer (C): Holder of a payment card, in the proposed model a customer is required to have a GSM mobile phone with a Subscriber Identity Module (SIM). This card has software installed by an authorizer and this acts as a "credit card" that is recognized by the authorizer
- Merchant (M): Merchant is the organization sells services/goods to the cardholder through the Internet and accredited by a known trusted third party
- Mobile Phone (MP): Any GSM mobile phone with a SIM card. However, the mobile phone does need some special capabilities

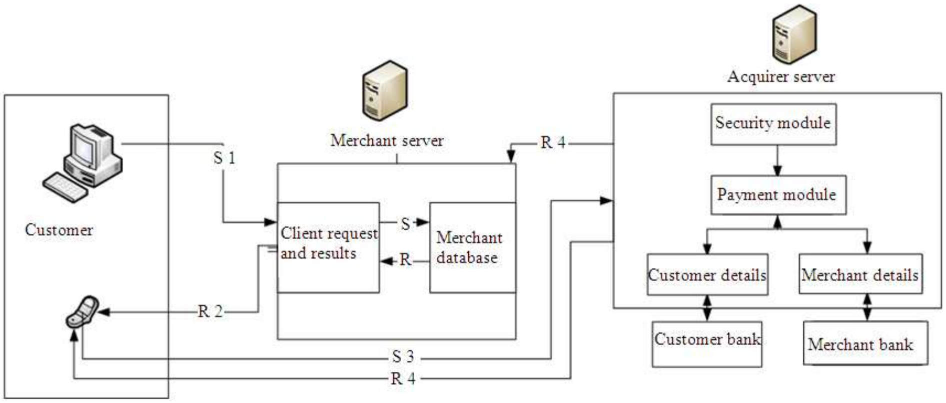


Fig. 1: The payment model

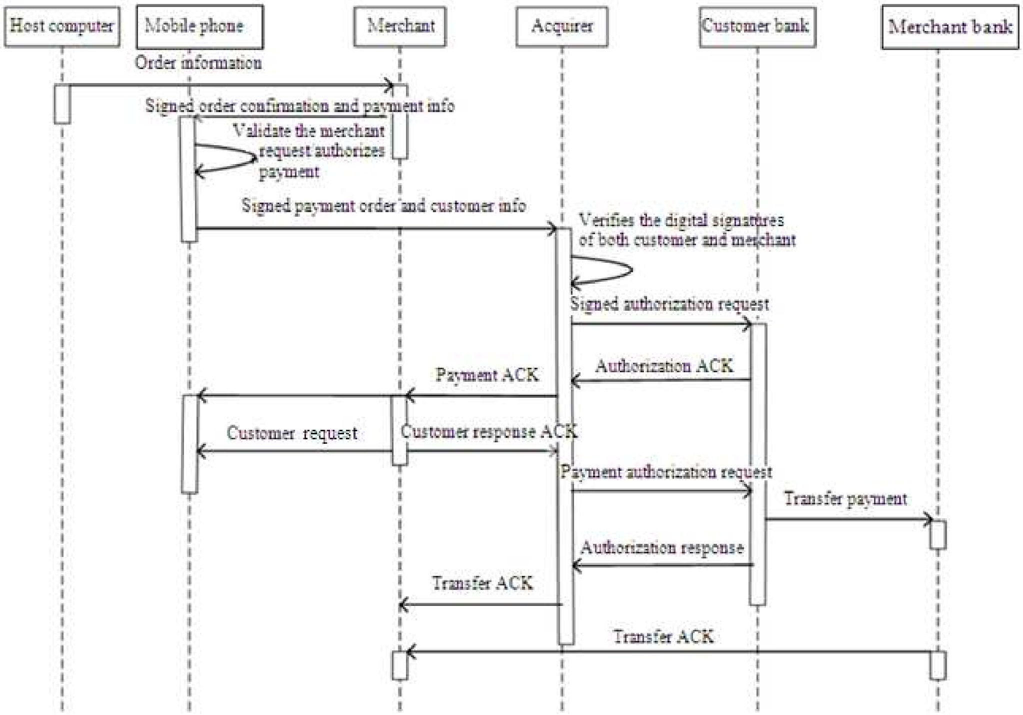
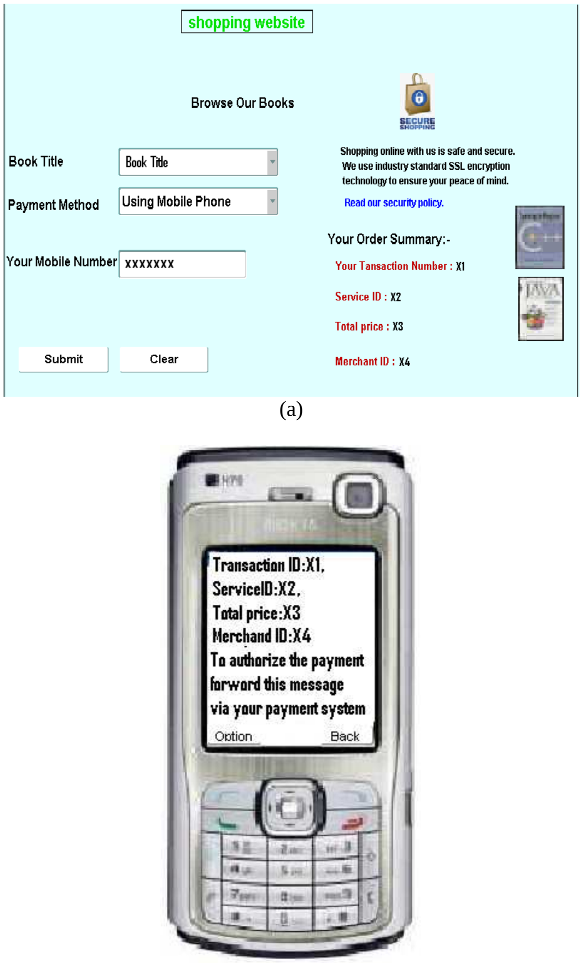

Host computer
Mobile phone
Merchant
Acquirer
Customer bank
Merchant bank
Order information
Signed order confirmation and payment info
Validate the merchant request authorizes payment
Signed payment order and customer info
Verifies the digital signatures of both customer and merchant
Signed authorization request
Authorization ACK
Payment ACK
Customer request
Customer response ACK
Payment authorization request
Transfer payment
Authorization response
Transfer ACK
Transfer ACK

Fig. 2: Sequence diagram of the payment model

- Acquirer (A): A financial institution which processes payment card authorizations and makes payments. The Acquirer provides electronic transfer of funds to the Merchant's account from the Customer's bank account over a secured payment network
- Customer's bank (Issuer): A financial institution that provides payment software to install to the customer mobile device and is responsible for the cardholder's debt payment
- Merchant's bank: A financial institution that receives the customer's payment and deposit in the merchant's account

Model time sequence: The sequence diagram (Fig. 2) describes the time dependent communication involved in messages between the model components. It illustrates how the customer, merchant, issuer and the acquirer communicate with each other.

As shown in the sequence diagram, the system is designed in two different phases:



Book Title: Book Title

Payment Method: Using Mobile Phone

Your Mobile Number: xxxxxxx

Shopping online with us is safe and secure. We use industry standard SSL encryption technology to ensure your peace of mind.

Read our security policy.

Your Order Summary:-

Your Tansaction Number : X1

Service ID : X2

Total price : X3

Merchant ID : X4

(a)

Transaction ID:X1,
ServiceID:X2,
Total price:X3
Merchand ID:X4
To authorize the payment forward this message via your payment system

(b)

Fig. 3: (a): Simulated merchant webpage; (b): Mobile simulated (with payment software)

Negotiation phase: in this phase a customer browses the merchant's website and selects item to buy. During this phase, the merchant and the customer reach an agreement upon a set of item's information that describes the purchase such as the item's price. A customer selects the payment method from the merchant webpage (in this case the customer will select the "Using Mobile Phone" method instead of other payment methods such as credit card) as shown in Fig. 3a. A customer can use any host computer to send the Order Information (OI) to the merchant such as the selected item's description and the customer's mobile number but without any financial details. The transactions process can be summarized as:

C→M: OI

When the merchant receives the order information they will send an order confirmation and the Payment order Information (PI) that has been Digitally Signed (DS) by the merchant to the customer's mobile device. The payment information includes details such as a transaction number, service ID, amount of money to be paid, merchant's ID and the merchant bank ID as shown in Fig. 3b. The merchant stores details of the transaction in their transaction database to use them in some stage later. The transactions process can be summarized as:

M→MP: [OI, PI, DS]

Payment phase: Upon receiving the payment order message (only readable message) from the merchant, the customer will verify the order information, especially ensuring that the price is correct. If all order information is correct, the customer forward the payment order information message via the payment software that is installed in SIM card by an authorizer. This acts as a "credit card" that is recognized by the authorizer. In order to authorize the payment, the payment software in the SIM card will request the customer to enter a personal PIN in their mobile phone and this satisfies the customer authentication. After the customer authorizes the payment, the mobile phone will send an encrypted message with the acquirer's public key (Kpu) that contains the validated PI message received from the merchant, plus Customer Information (CI) such as the customer's bank ID and customer's bank account details to the acquirer and this satisfies data confidentiality. The process in the MP can be summarized as:

```
Verify PIN
IF PIN is correct THEN
{MP → A: [[PI, DS], CI] Kpu}
ELSE Terminate
```

When the acquirer receives the payment order message from the customer it verifies the digital signatures of both the customer and the merchant in order to ensure their authenticity. The acquirer will go through a financial network if and only if that message from the merchant has been digitally signed by the customer using his mobile device. That means the customer has authorized the payment transaction and agrees to transfer the payment to the merchant. If successful, the acquirer then decrypts the received data to obtain the payment information and goes through the financial network to obtain payment authorization. The acquirer informs the customer's bank to reserve the payment to the merchant and the customer bank notifies the acquirer that the payment has been reserved for the merchant in order to transfer it to the merchant's account in the merchant's bank if the acquirer requests that later on.

The acquirer sends a confirmation message to both the merchant and the customer's mobile device to inform them of the success or failure of reserving the payment. When the customer and the merchant receive these response messages from the acquirer, both of them check the digital signature of the message to ensure that it comes from the acquirer. In addition, the merchant checks the transaction number and timestamp to ensure that the receipt message corresponds to the original transaction stored in their transaction database. If all of these processes are completed successfully, the merchant then releases the services/goods to the customer and sends two notification messages. The first message is to the acquirer to inform it that the goods/services have been released to the customer. When the acquirer receives this message, it verifies the digital signature of the merchant to ensure its authenticity. The second message is to the customer's mobile device to inform the customer that the services/goods have been released. Therefore, the customer can use the service. In the case of the purchase begging goods, the customer can collect them from the merchant shop or from the merchant's deliverer. In the two previous cases, the merchant, or the merchant's deliverer, verifies the merchant's signature from the merchant's message that informed the customer that the goods had been released. If the signature is valid, the merchant delivers the goods.

When the acquirer receives the merchant's message for releasing the services/goods to the customer then the acquirer can inform the customer's bank to transfer the reserved money to the merchant's bank and then the customer's bank informs the acquirer that the payment has been transferred to the merchant's account in the merchant's bank. If the process fails at some stage such as if the merchant does not inform the acquirer to release the services/goods to the customer after a period of time, then the acquirer informs the customer's bank to cancel the money being held

When the merchant's bank receives the payment, it sends a confirmation message to inform the acquirer that the customer has paid for the goods.

When the acquirer receives the message from the merchant's bank, it informs the merchant that the customer has paid for the goods.

Model analysis and comparison with a traditional system: We note that crucial messages from both customers and merchants are digitally signed. This means that there is no need for the customer and merchant to trust each other, they just need to trust the use of the correct public keys, which should be ensured by the certificates issued by a trusted Certification Authority (CA). In the case of a dispute they can verify the digital signature of both customers and merchants by a Judge where the financial level of the transaction warrants this. Furthermore, in the model the mobile device acts on behalf of the cardholder and plays the role of the customer in the payment transaction with the acquirer, by sending the validated message received from the merchant, plus customer information to the acquirer. The mobile device encrypts all these details with the acquirer's public key and this satisfies data confidentiality. In these processes the customer does not need to ensure that the merchant is trusted because in the model the merchant does not act as an intermediary and the information that is transmitted to the merchant is not sensitive. Incidentally, the customer knows that the purchase will be done through a trusted third party and knows that it is the responsibility of the acquirer to verify that the merchant is accredited by a known trusted third party. Therefore, the customer will then not feel reluctant about being involved in the e-payment transaction. In these processes the acquirer ensures that parties cannot deny the payment processes to improve the non-repudiation. Furthermore, the customer authorizes the payment transaction by entering a personal PIN in their mobile device and this satisfies the customer authentication. Therefore, no one can complete the payment process except the person who has both the personal mobile device and the PIN at the same time.

DISCUSSION

The first part of the research aims to identify key factors that may influence online customers trust in adopting mobile payment systems. It closely examines whether the adoption of a mobile phone which provides security of payment details, would influence customers trust to use online shopping in the future. It also investigates perceptions and preferences of online customers and their utilization of current e-payment systems. Results demonstrate that the six variables (shopper's ability to control their transaction; security built into a mobile phone payment system; prior perception of security evidence; perception that no personal data is sent through the merchant in a transaction; perceived ease of use and perceived usefulness) have a significant direct effect on the adoption of mobile devices. This in turn gains customers trust in online payment systems and thus increases their utilization of online shopping. The results indicate that there is a positive relationship between the use of a mobile device for online transactions and a customer's trust in the transaction. In other words, the results demonstrate that the adoption of a mobile device has a significant and direct affect on customers trust.

The first part of the research also discovered that there is a considerable lack of people experienced in using their mobile phone for online payments. From those participants sampled who are not experienced in mobile payments, expressed a willingness to use their mobile phone for online payments in the future. That is, provided it was available as a payment option over the Internet.

This study proposed a mobile payment to solve problems in a conventional e-payment system. From the survey results, there are six variables that have been identified as key factors that may influence online customers trust in adopting mobile payment systems. The proposed a mobile payment has been developed to provide these factors.

The analysis of the proposed model provides strong support for the using of a mobile device for online transactions. The model has more advantages compared with a conventional e-payment system, which makes the model more usable. For instance, some customers may be unfamiliar with the trust solutions used by a website, such as trust evaluation or a trusted signature. A false website might counterfeit these and so customers may be the victim of a 'phishing' attack. Moreover, this model has an additional advantage in that it combines the personal computer with a personal mobile device and uses existing infrastructure and technologies to minimize the extra cost of a new e-payment method. While the SIM does initially require additional software from the issuer, this solution provides mobility which is not possible in the conventional solutions where software has to be installed in any PC participating in a transaction, as in the SET case. The use of a mobile phone and SIM can offer a more economical, secure and more flexible solution than conventional e-payment systems. Using any available personal computer in the navigation phase is more comfortable for a buyer than using a mobile phone, with its limited navigation and display capability, for the entire transaction.

CONCLUSION

This study has presented the design of a practical mobile payment model as a possible step towards increasing customer acceptance of online shopping and increasing their trust in online payment systems. The proposed model developed based on the results of a quantitative study. The new model focuses on enhancing the feeling of security of the use of an online payment system and satisfying the security requirements by using a mobile device and changing the traditional online payment transaction processes between customers and merchants. In the model customers do not need to disclose their financial information during the transaction and the merchants will not act as intermediary between customers and the acquirer. The model has more advantages compared with a conventional e-payment system by providing high security, low cost and convenience, which are key factors to make the mobile payment more usable.

The model has been simulated as apart of current research. Future research will evaluate performance and acceptance of the model with people using the simulation.

REFERENCES

1. Mayer, R.C. and J.H. Davis, 1995. An integrative model of organizational trust. Acad. Manage. Rev., 20: 709-734. http://www.jstor.org/pss/258792
2. Andert Donna, Wakefield Robin and Weise Joel, 2002. Professional Services Security Practice. Sun BluePrints™ OnLine.
3. Pousttch, K. and D.G. Wiedemann, 2007. What influences customers' intention to use mobile payments? University of Augsburg, Germany. http://www.marshall.usc.edu/assets/025/7534.pdf
4. Linck, K., K. Pousttchi and D.G. Wiedemann, 2006. Security issues in mobile payment from the customer viewpoint. University Library of Munich, Germany. http://ideas.repec.org/p/pra/mprapa/2923.html
5. Dahlberg, T., N. Mallat, J. Ondrus and A. Zmijewska, 2007. Past, present and future of mobile payments research: A literature review. http://www.janondrus.com/wp-content/uploads/2008/05/ecra2007-inpress.pdf
6. Peffers, K. and W. Ma, 2003. An agenda for research about the value of payment systems for transactions in electronic commerce. J. Inform. Technol. Theor. Appli., 4: 1-14. http://direct.bl.uk/bld/PlaceOrder.do?UIN=133207648&ETOC=RN&from=searchengine
7. Audun, J. *et al.*, 2007. A survey of trust and reputation systems for online service provision. Dec. Support Syst., 43: 618-644. http://portal.acm.org/citation.cfm?id=1225716

8. Zhongwei, Z. and W. Zhen, 2006. Assessing and assuring trust in e-commerce systems. Proceeding of the International Conference on Computational Intelligence for Modeling Control and Automation and International Conference on Intelligent Agents Web Technologies and International Commerce, Nov. 28-Dec. 1, IEEE Computer Society, pp: 124. http://portal.acm.org/citation.cfm?id=1192332
9. Sabater, J. and C. Sierra, 2005. Review on computational trust and reputation models. Artif. Intell. Rev., 24: 33-60. http://portal.acm.org/citation.cfm?id=1057849.1057866
10. Al Dala'in Thair, Luo Suhuai and S. Peter, 2008. Using a mobile device to enhance customer trust in the security of remote transactions. Proceeding of the IEEE 8th International Conference on Computer and Information Technology, July 8-11, IEEE Xplore Press, Sydney, NSW., pp: 396-401. DOI: 10.1109/CIT.2008.4594708
11. Sherif, M.H. *et al*., 1998. SET and SSL: Electronic payments on the Internet. Proceeding of the 3rd IEEE Symposium on Computers and Communications, June 30-July 2, IEEE Xplore Press, Athens, Greece, pp: 353-358. DOI: 10.1109/ISCC.1998.702546
12. Fourati, A. *et al*., 2002. A SET based approach to secure the payment in mobile commerce. Proceeding of the 27th Annual IEEE Conference on Local Computer Networks, Nov. 6-8, IEEE Xplore Press, USA., pp: 136-137. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1181777
13. Levi, A. and C.K. Koc, 2001. CONSEPP: Convenient and secure electronic payment protocol based on X9.59. Proceeding of the17th Annual Computer Security Applications Conference, Dec. 10-11, IEEE Computer Society, Washington DC., USA., pp: 286. http://portal.acm.org/citation.cfm?id=872164
14. Bottoni, A. and G. Dini, 2007. Improving authentication of remote card transactions with mobile personal trusted devices. Comput. Commun., 30: 1697-1712. http://portal.acm.org/citation.cfm?id=1243186
15. Joris, C., P. Bart and V. Joos, 2001. Combining world wide web and wireless security. Proceedings of the IFIP TC11 WG11.4 1st Annual Working Conference on Network Security: Advances in Network and Distributed Systems Security, Nov. 26-27, Kluwer, BV., The Netherlands, pp: 153-172. http://portal.acm.org/citation.cfm?id=710568
16. Vorapranee, K.S. and J.M. Chris, 2002. Using GSM to enhance e-commerce security. Proceedings of the 2nd International Workshop on Mobile Commerce, Sept. 28-28, ACM Press, Atlanta, Georgia, USA., pp: 75-81. http://portal.acm.org/citation.cfm?id=570705.570720
17. Al Dala'in Thair, Luo Suhuai and S. Peter, 2008. A review of current online payment systems related to security and trust solutions. Proceeding of the IADIS International Conference, e-Commerce, July 25-27, IADIS Press, Amsterdam, The Netherlands, pp: 244-249. ISBN: 978-972-8924-66-9.
18. Straub, D.W., 1989. Validating instruments in MIS research. MIS Q., 2: 147-169.
19. Boudreau, M.C., D. Gefen and D.W. Straub, 2001. Validation in IS research: A State-Of-The-Art Assessment. MIS Q., 25: 1-16. http://www.misq.org/archivist/vol/no25/issue1/vol25n1art1.html
20. Joseph, F. R.E.A., Hair, W.C. Black and L. Ronald, 2005. Tatham, Multivariate Data Analysis. 6th Edn., Prentice Hall, ISBN: 10: 0130329290.