World Applied Sciences Journal 12 (Special Issue on Computer Applications & Knowledge Management): 07-12, 2011
ISSN 1818-4952
© IDOSI Publications, 2011

Non-Repudiation in Order, Delivery and Payment Process for a Sustainable Online Business

[1]*A.S.A. Rahman,* [2]*S. Masrom and* [3]*K. Jusoff*

[1]Department of Computer and Information Sciences, Universiti Teknologi PETRONAS,
Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
[2]Faculty of Computer Science and Mathematics, Universiti Teknologi MARA,
Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
[3]Faculty of Forestry, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Abstract: Online businesses in Malaysia suffer from the lack of non-repudiation in the ordering, delivery and payment process. Most businesses cannot sustain their growth because of this limitation. The paper presents a new model for the implementation of online business. The solutions can also be adapted to any country for the most part except for the delivery process that requires the use of a smartcard-based national identity card. The non-repudiation evidences that are generated from the system can be used by both the consumer and the merchant to resolve possible future disputes. The evidence is also admissible in the court of law since they are generated from the Public Key Infrastructure (PKI) that is recognized by the authority as legally binding.

Key words: Non-repudiation · Online business · Cybersecurity · Security framework

INTRODUCTION

Online businesses are booming in Malaysia. As of recently, with the pressure of the economic downturn and unemployment rate that is on the rise, Malaysians are turning more and more towards the online businesses. Undeniably the online business is beneficial to both the consumer and the merchant. Consumers can visit more e-shops with the same amount of time than real brick and mortar shops. It is easier and faster for them to make comparison of products. Very often they would get the best deal from these online shops. The merchant also benefit from the low cost in the company start-up and operation overheads. They do not have to rent any physical space. In fact often times they are working right from the comfort of their own home. Their shop is not subjected to operating hours, except for the very rare system downtime.

There are however a number of problem with the current online business model. The shop owners are often inexperience in setting up the online system. They either rely on service providers or try to replicate whatever system that is currently available in the market. Through survey, it has been have found that these systems do not provide legally binding proof of the business transaction. Consumers are often asked to bank-in the amount necessary for any item they want to purchase before the merchant would even consider processing their order. There is however, no legal evidence that the money transferred to the merchant's account is a payment for anything in particular. Hence there is no way for the customers to prove that they have made the payment in accordance to any electronic order form prior to the transaction. Once the money is in the merchant's account, there is no guarantee that the merchant will ship the product to the consumer. Because of the lack of a trustworthy system, potential customers are not likely to make purchases of significant values as there are not willing to risk losing their money. Honest and legitimate businesses are therefore denied of their opportunity to prosper.

The objective of this paper is to develop a secure and trustworthy online business model that is suitable to be implemented in Malaysia.

Related Works: A lot of works have been done towards the improvement of online transactions. These works have created interest for researchers to develop a variety

Corresponding Author: A.S. Rahman, Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia, E-mail: sanirahman@petronas.com.my.

of online business models. Security has always been considered as an essential and critical area of research for many type of online business [1]. One of the works can be seen in paper [2] that introduces flexible e-payment system with fraud detection system. The design proposed in the paper was based on the concept of atomic transactions or coupons by using e-wallet account. However, no prove has been shown in the paper about either the success of implementation or the performance of the e-wallet system. Another work regarding online business security comes from the paper [3] by Sung Woo Tak, Yugyung Lee, Eun Kyo Park and Jerry Stach that introduces an adaptive secure protocol for e-commerce. Cryptographic techniques have been applied in this protocol for the purpose of providing information.

The security methods proposed in [2-5] were more focussed on the systems security in the network domain for the purpose of information confidentiality as well as payment guarantee. Although these security aspects are generally important in a business transaction, it is still arguably biased towards the seller since it concentrates more on securing the latter's interests. A holistic solution should include aspects such as business agreement and contract signing. The protocols regarding negotiation and contract signing is explained in detail by A. Ruiz-Martínez, C.I. Marín-López, L. Baño-López and A.F.G. Skarmeta in paper [6]. However, these protocols are not designed to be implemented in the process involving product delivery.

Upon realizing that online transaction and processing are facing with security risks, many researchers have proposed online security framework. In [7], a conceptual framework for electronic information security management among federated and related organizations has been introduced. In this study the authors have suggested a collaboration model among organizations that needs a sustainable trust and mutual cooperation. So, the proposed framework has been shaped with regards of many or aspects of organizational dimensions such as culture and policy. Similarly, an Electronic Supply Chain (ESC) framework has been introduced in [8]. This framework has placed security online transaction as the major component to be considered for implementing ESC. Both proposed framework in [7] and [8] are not designed with concern of legal binding proof. A technology of RFID has been used by [9] to propose a software framework for secured e-commerce environment. In the system, an automatic identification technology has been utilized to provide electronic identity to an item for tracking purposes. However, with regards to business agreement and contract signing, the system has not been designed with such kind of facility.

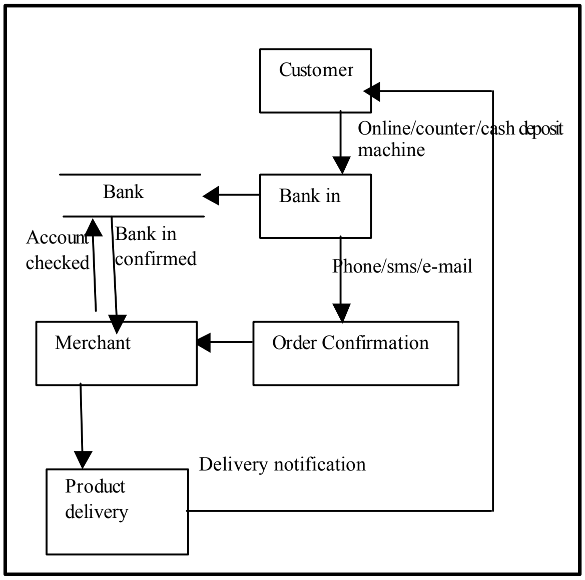

Fig. 1: Current online business process flow

Current Framework: The current process flow in a typical Malaysian based online business can be generally illustrated in Fig. 1. This process begins when a buyer decides to buy any product advertised on merchant's website. Customarily the buyer would fill up and send an electronic order form to the seller. This document, although containing detailed information is not considered legally binding as anyone can create it without authenticating himself.

The delivery of the product will only be made after the seller has received payment in the bank account. In the best possible scenario, the customers will only be able rely on the merchant's good reputation to make sure that the transaction will go through. In the worst case scenario, where the merchant is relatively unknown or has not yet built his reputation the buyer would not dare to make purchase of significant value.

A number of problems in the current online business model have been identified, as summarized in Table 1. Three processes in online business model have been identified to require improvement, namely ordering, delivery and payment recovery. A problem is identified when there is a disadvantage in any of the processes either from the perspective of the customer, merchant or both of them.

In the ordering process, the first problem occurs when consumer is asked to fill up an electronic order form without any means of authentication. This will create an opportunity for any imposter to mischievously order anything on behalf of the unsuspecting consumer.

Table 1: Common Problems In The Current Online Business Practice

	Problem		
Process	Description	Customer disadvantage	Merchant disadvantage
Ordering	Order form is not digitally signed		√
	No legally binding proof of payment for ordered product(s)	√	
Delivery	Only addressee can collect the package	√	√
	Representative for addressee is allowed to receive on his/her behalf without legally binding proof of identity	√	√
Process	No legally binding proof of acceptance of package		√
	No legally binding proof of rejection of package	√	
Recovery	Delivery time limit is not enforceable	√	
	Complicated process for rejection of damaged product	√	√
	Complicated process for rejection of non-compliant product.	√	

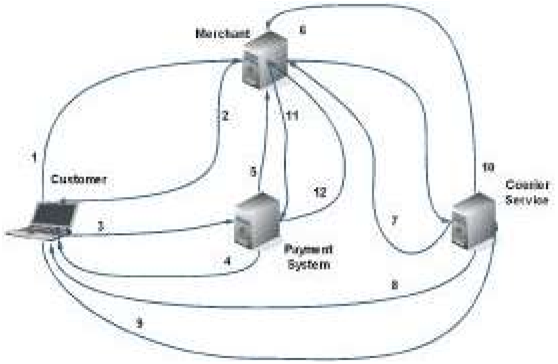

Fig. 2: Proposed online business process flow

Secondly, there is no legally binding proof of payment for any ordered product(s) and customers must only rely on the bank's receipt as a proof of payment. In any cases, a dishonest merchant may deny the transaction and refuse to deliver the product.

Generally, these same problems occur in many online business systems involving the delivery process. These problems have impacts on both the customer and the merchant. In normal practice, the merchant would employ courier services to deliver their product to the customer.

In Malaysia, when the addressee cannot be reach the product will be stored temporarily in the nearest distribution centre. And the courier personnel would leave a message in the mailbox, telling the addressee to collect his product at the centre.

After a certain period, all the unclaimed products will be returned to the sender (merchant). There are courier companies that will make the extra effort to re-attempt a second and a third delivery but in most cases the cost is too prohibitive for them to provide this level of service. An alternative approach would be to deliver the product to a member of the family or the neighbor. This will also create other problems in terms of privacy, confidentiality and non-repudiation.

Non-Repudiation for the Overall Process: The following model is proposed as depicted in Fig. 2 for implementation. It consists of at least five parties: the Customer, the Merchant, a Payment System, a Courier Service and a Certificate Authority. For simplicity Certificate Authority is not depicted in the diagram. The process of applying for certificates and verification of signature are also not discussed here as they have nowadays become quite common.

Henceforward C, M, PS and CS are used to denote the Customer, the Merchant, the Payment System and the Courier Service. $S_X(m)$ denotes a party X's signature on a message or document *m*. We use "," as a separator for messages containing multiple items. We use *term* in italic to denote a placeholder for any object(s) described by the term.

Explanation of the Process:

- The Customer (C) accesses the Merchant's (M) online system, browses through the displayed products and checks some items that he wishes to buy in the shopping cart. When he is satisfied with the purchase he would then enter the necessary information in the Purchase Order Form (POF) and affixes a digital signature on the form.
  $C \rightarrow M$: POF, S_C(POF)
- The merchant's online system generates a Promise of Delivery, stating that the items ordered are available and will be delivered to the customer within N days after the payment is made to a certain trusted third party denoted as Payment System (PS). To link the POD to the POF the merchant will include S_C(POF) in the POD.
  $M \rightarrow C$: POD, S_M(POD)

- The customer will send a Payment Instruction (PI) to PS. The money is to be released to the Merchant as soon as the customer received the products ordered.
  $C \rightarrow PS : PI, S_C(PI)$
- PS will generate a Payment Receipt to the customer as a proof of the transaction.
  $PS \rightarrow C : PR, S_{PS}\,(PR)$
- PS will also send a notification to the Merchant, stating that the money has been received on the Merchant's behalf.
  $PS \rightarrow M : PR, S_{PS}(PR)$
- The merchant will proceed to ship the product through Courier Service (CS).
  $M \rightarrow CS :$ *Product(s)*
- CS will generate a Courier Receipt (CR) for the Merchant stating that the package is now under its custody and ready to be shipped.
  $CS \rightarrow M : CR, S_{CS}(CR)$
  CS will find the Customer and deliver the product.
  $CS \rightarrow C :$ *Product(s)*
- The Customer or his representative will inspect the package for compliance to specification and digitally sign the Delivery Acceptance Form (DAF).
  $C \rightarrow CS : DAF, S_C(DAF)$
- CS will forward the delivery acceptance document to the Merchant as a proof of delivery.
  $CS \rightarrow M : DAF, S_C(DAF)$
- Merchant will forward the proof of delivery to PS in order to get payment.
  $M \rightarrow PS : DAF, S_C(DAF)$
- PS will verify the authenticity of the document, transfer the money into the Merchant's account and send a notification of money transfer (MT) to the Merchant.
  $PS \rightarrow M : MT, S_{PS}(MT)$

Non-Repudiation in the Delivery Process: Delivery is somewhat a special process since currently it is the least automated process in the whole system. Only in the delivery process does it involve physical transaction while in the other processes everything can be carried out electronically. It is also the least secured process because it involves the weakest link in a secure system: the human.

Often when a package is being delivered to any residential address, the intended recipient is either away or not available. Some courier service will just drop a notification letter in the mailbox asking the addressee to collect the package from a nearby collection centre. Some courier company might allow the neighbour to accept the package on behalf of the addressee. Multiple problems may arise from this situation:

- It might be troublesome for the addressee to go and self-collect the package. The addressee may also insist for another round of delivery to be made when he/she is available, hence increasing cost to the courier service.
- The neighbour who accepted on behalf of the addressee might not know how to properly inspect the product(s) delivered. He/she might end up accepting a product that is either damaged or not compliant with what the addressee had ordered.
- The addressee might not want the package to be inspected by his/her neighbour in the first place because of either privacy or confidentiality concern.
- In current practice, the neighbour does not have to show any form of identity, he/she is only asked to sign/initial on a piece of form. Clearly that is not sufficient to guarantee non-repudiation.

A system prototype has been developed to provide non-repudiation in the delivery/acceptance of products. It involves the use of a handheld device that has two important functionalities:

- It should be able to read a finger print of any recipient and verify it against the fingerprints stored in the MyKad. This is to make sure that the card is used by its rightful owner.
- It should be able to read the private key that is stored in the MyKad, generate and affix a digital signature on the electronic Delivery Acceptance Form (DAF).

Description of the Process:

- A courier personnel will carry a handheld device that has two readers attached. A thumbprint reader is used to scan the thumbprint of the person accepting the package. Another reader is a smart card reader, used to read data from the MyKad.
- Each recipient is required to have already applied for a keypair from a certificate authority and stored their private key in the MyKad.
- Upon agreeing to inspect and eventually accept the package, the recipient is asked to insert his/her MyKad into the smart card reader and place his/her thumb on the thumbprint scanner.
- The thumbprint will be verified against the thumbprint data that is stored in the MyKad. If they match the recepeint is verified.
- If the recipient is not the addressee, his/her identity is compared with a list of authorized recipient. (Specified in the order form by the customer himself).

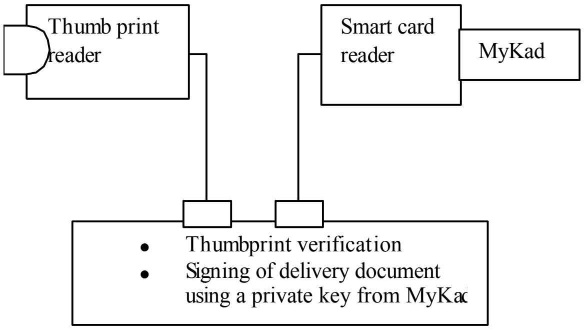

Fig. 3: Handheld terminal for courier personnel

- If the recipient is authorized to receive on behalf of the addressee, he/she will inspect the package and decide whether to accept or reject the product(s).
- In both cases he/she is required to digitally sign acceptance/rejection form using the private key that is stored in his/her MyKad.
- Delivery process is considered completed after the signature has been attached to the acceptance/rejection document.

The system is limited to produce legally binding receipt if all of the following conditions are met, namely: (a) the intended recipient (or anyone authorized by the recipient) is available and possesses a valid identity card, (b) the recipient/authorized person has a private key installed in his/her identity card and (c) the recipient/authorized person is the rightful owner of the identity card presented to the courier personnel.

In Malaysia, however, all necessary infrastructures are already in place. Every citizen has an electronic identity card (MyKad) that is capable of storing the private key. Almost every household will constitute of at least one income tax paying citizen. With the Malaysian government determination on setting up an electronic government, it has already distributed to all income tax paying citizen, a digital certificate and a pair of private and public key that is legally binding. This keypair can be used for the purpose of this project if the customer is not willing to purchase a new certificate.

In case the intended recipient do not have a valid private key, he or she can specify in the order form that another person will be signing the delivery receipt of his/her behalf. This other person can be a member of the family or a neighbour. This will not pose any problem since the digital signature that will be affixed to the delivery receipt is legally binding.

CONCLUSION

This paper has described the process flow of current online businesses as they are practiced mostly by Malaysian entrepreneurs. A number of problems in the ordering process, delivery process and payment process have been identified. An online business model has been introduced with some additional security mechanisms that will benefit both the consumers and the merchants. A system prototype has also been successfully implemented to prove the feasibility of the design. It is suggested that the entire proposed model is to be implemented in a pilot project to evaluate its robustness and efficiency.

REFERENCES

1. Hanzaee, K.H. and T. Sadeghi, 2010. Measuring Banks' Automated Service Quality: A Re-Examination and Extension in an Islamic Country, World Applied Sciences J., 8(7): 874-880.
2. Leung, A., Z. Yan and S. Fong, 2004. On designing a flexible e-payment system with fraud detection capability, IEEE International Conference on e-Commerce Technology, Beijing, China, 13-15 September 2004, pp: 236-243.
3. Sung, W.T., L. Yugyung, K.P. Eun and J. Stach, 2001. Design and evaluation of adaptive secure protocol for E-commerce, Computer Communications and Networks, Scottsdales, Arizona, USA, 15-17 September 2001, pp: 32-39.
4. Blundo, C., S. Cimato and A. De Bonis, 2002. Advertising and Security for E-Commerence: A lightweight protocol for the generation and distribution of secure e-coupons, Eleventh International Conference on World Wide Web, Honolulu, Hawaii, USA. 7-11 May 2002, pp: 542 - 552.
5. Peha, J.M. and I.M. Khamitov, 2003. PayCash: a secure efficient Internet payment system, The Fifth International Conference On Electronic Commerce, Pittsburgh, Pennsylvania, USA, 30 September-3 October 2003, pp: 125-130.
6. Ruiz-Martínez, A., C.I. Marin-Lopez, L. Bano-Lopez and A.F. Gomez Skarmeta, 2006. A new fair non-repudiation protocol for secure negotiation and contract signing, Fourth International Conference on Privacy, Security and Trust, Markham, Ontario, Canada, 30 October - 1 November 2006, pp: 1-11.
7. Elahi A., S. Shayan and B. Abdi, 2008. Designing a Framework for Convergent Information Security Management among Federated Organizations, World Applied Sciences J., 4(Supplement 2): 21-32.

8. Hashemian, S.M., M. Behzadian, M. Ranjbar-Bourani and F. Zabihy, 2009. Information Access Level Control in Electronic Supply Chain, World Applied Sciences J., 6(Supplement 1): 97-105.

9. Hamzehei, A., 2008. Digital Rights Management using RFID in an E-Commerce Environment, World Applied Sciences J., 5(3): 324-331.