ISSN:0975-9646

Secure Authentication Based E-Payment with Intermediate Entities

B.Ratnakanth

Assoc. Professor, VITS,HYDERABAD

Abstract: **With the rapid development of information highway, especially that of Internet, E-commerce, as one of the frequently used words, enjoys high popularity in modern society. As increasing number of business conducted via Internet, E-commerce gradually evolves as a new model for business activities. The continuous update of modern password technique make E-commerce, especially Epayment in the aspects of security algorithm and protocols well-developed. The E-payment system brings users with higher efficiency, credibility and speeding-up transactions settlement, which reduce the pay risks caused by time lags in handling the bills. However, it also comes with new risks, i.e. security problem of transactions. Additionally, the transaction and their data about clients are enormously sensitive, security production and privacy is exceptionally crucial. In order to address the security issues, in this study proposed a stylized transaction for online commerce using an intermediary in the e-payment field. This proposed model of intermediary not only settles payments, but it also takes care of such needs as confirming seller and buyer identities, authenticating and verifying ordering and payment information and other transactional requirements lacking in virtual interactions.**

Keywords : E-payement system, security, Encryption, Electronic commerce

INTRODUCTION

The role of e-commerce electronic payment systems is pivotal for future of e-commerce, whose further growth depends on the timely development of EPSs. The development of new types of e-commerce purchasing relationships and business models has created the need for new ways of money exchange and new EPSs. For instance, online auctions, (Ribbers & Heck, 2004), has spurred the necessity forperson-to-personpayment systems to allow online money exchange between individuals. Certain types of information products and services require small payments and micropayments. Businesses would like to sell information content that costs very little, accumulating revenues with high turnover. E-commerce EPSs can be designed for selling specific types of products, for example for trading copyrighted online content, such as music. Another unforeseen earlier requirement is conducting e-commerce using wireless mobile devices, such as mobile phones or Personal Digital Assistants (PDA). The need for paying with mobile devices has urged the development of payment systems for mobile electronic commerce, (Laudon & Traver, 2002). In addition, e-commerce provides the possibility to enhance current payment systems or substitute them with online variants(Abrazhevich, 2004).

Electronic commerce is now one of the widest applications in Internet since it helps businesses to expand their marketing strategy and to reduce their costs. This growth has motivated the development of research to improve electronic services. Security, as one of these research topics, constitutes a critical point in the implementation of new business models because the process of traditional business such as paper-based contracts, personal purchases, etc. must be adapted to flows of information inside an unreliable network like the Internet. Payment should be the process with the highest security level in e-commerce operations because it is the step where the customer legally ends the business by making the money transference. Many secure electronic payment solutions have been proposed. Some of them describe online payment with a cash payment model, like e-Cash, DigiCash, NetCash, and Cybercash. Others, such as NetBill, NetCheque and BankNet, present a cheque payment model(Carbonell *et al*., 2009).

At the present time, internet has become a platform for social interaction and collaboration. It allows people and organizations to communicate, exchange ideas and trade goods and services more efficiently (Tan *et al*., 2007). In Pakistan, like other developing countries of the world, internet has already been established and accepted warmly for information and social interaction. But role of internet in commerce and trade (ecommerce) is still very limited. E-Commerce plays vital role in economic development by reducing cost of products and services. It promotes Small and Medium size Enterprises (SMEs) and allows them to compete with giants in same marketplace. Small business organizations in Pakistan are suffered badly due to political instability in the country especially after 9/11. In this situation, ecommerce has become very important solution for their growth. Pakistan is among those few countries that made remarkable performance in Information and Communication Technologies (ICTs). Banking and Information Technology industries also made excellent advancements in past decade. Country is producing thousands of IT professionals every year(Khan *et al*., 2013).

2.0 Significance of the study

E-Commerce plays a vital role in economic development by reducing the cost of products and services. It promotes Small and Medium-size Enterprises (SMEs) and allows them to compete with giants in the same marketplace (Khan *et al*., 2013). Online applications require a strong security feature to protect user confidential data. Security is a major issue on the internet based online payment system. There are various internet threats which affect the security system of the internet and increase the risk for an electronic transaction. Most of the authentication system relies on passwords, personal identification numbers, and keys to access their personal account information. This type of authentication system cannot verify or authenticate the identity of the users who he or she claims to be (Tiwari, 2007). Security of electronic transaction over an insecure communication channel is a challenging task that includes many critical areas as a secure communication channel, strong data encryption technique and trusted a third party to maintain the electronic database(Gupta & Sharma, 2011).For overcoming these issues in the e-payment field, we proposed a stylized transaction for online commerce using an intermediary. In this model, the intermediary not only settles payments, but it also takes care of such needs as confirming seller and buyer identities, authenticating and verifying ordering and payment information and other transactional requirements lacking in virtual interactions.

3.0 Related work

An online payment system using visual cryptography and steganography is proposed in Roy and Venkateswaran (2014) but the customer's share generated using visual cryptography is not secured during transmission, As a result of that an eavesdropper can masquerade as customer by hacking customer's share. In Wang, Wu and Duan (2004) an off-line electronic cash scheme using partial blind signature is proposed but it is not meant for online payment. An electronic payment using quantum blind signature is proposed in Khodambashi and Zakerolhosseini, (2014) but it requires account in same bank for both customer and merchant and it is not an online payment method

Ismaili *et al*. (2014) proposed three-domain (3D) security schemes, including 3-D Secure and 3D as ways of improving ecommerce transaction security. Based on this about SSL, SET, 3D security schemes and the requirements of electronic payment, designed a secure and efficient E-Payment protocol. The new protocol offers an extra layer of protection for cardholders and merchants. Customers are asked to enter an additional password after checkout completion to verify they are truly the card holder; the authentication is done directly between the card holder and card issuer using the issuer security certificate and without involving the third party (Visa, Master Card).However this study needs focus analysis the security and the performance of proposed protocol.

4.0 Electronic Payment System

The electronic payment system is the alternative to the coin or paper-based cash payment system to easy the user to make payment for their purchased goods or services over the network or internet and in the absence of the physical (entity) presence. Initially cheque in bank payment systems are used to serve the purpose of the same but now in the era of internet and e-commerce paying securely over the internet is an important task for the electronic payment system. Currently, a credit card is also in use for the payments over the network but still users doubt about trustworthy and the security of their money because of the increase in the frauds which ultimately causes loss of value(money) either of users, merchant or participating banks (Raghuwanshi *et al*., 2009).

Present electronic payment system are to far from ideal payment system because of the higher transaction cost, more fraudulent activities, and multiple parties are involved in the payment processing simultaneously lacks users acceptance, proper application plans and incompatible standards/ specifications. The good payment system should satisfy the user's acceptance and merchants in the mass scale.The present electronic payment system can be divided in two group electronic cash and credit/ debit system or token based and account based system. Tokens or electronic cash are like the physical cash which represent the value and credit/debit, or account based system does not carry value but a message to transfer value (Raghuwanshi *et al*., 2009).

4.1 Security Requirements of E-Payment

In this research, the issues regarding payment transactions are considered. Based on what is designed, implemented and tested, some potential points of development for essential security enhancement could be detected. The most sensitive part of the application, the payment function as a mobile payment operation, is the process of exchanging financial values done by two or three parties using mobile devices (Khan *et al*., 2013).

The following security services are required to establish a secure, comprehensive and smooth payment. There are potentials where the security is an essential property.

- Authentication of all parties and objects involved in a transaction.
- Confidentiality of messages and information transferred in a transaction.

- The integrity of messages and transactions.

Authentication: User identification verification and approval is essentially required in system design and must be efficiently provided (Yung, 2008).

Integrity: In this context transaction must be created or modified only by authorized parties or only in authorized ways to assure all participants that the received messages have not been altered in any way from the original message(Bishop, 2005).

Confidentiality: ensures that the transaction contents are accessed only by authorized parties. Basically access can be reading, viewing, printing or knowing that a particular asset exists. In this context, encryption and decryption are the methods to achieve confidentiality (Bishop, 2005).

Privacy: The function of protecting the collected information of the participants of transactions that were performed over the Internet. This information can be useful outside of the transactions so that any of that information may be linked in a way the participants without their knowledge or consent.

Availability: as an integral requirement each security infrastructure needs the complete security design in order to provide expected services available enough for its intended users.

5.0 Methodology

In this research, propose a stylized transaction for online commerce using an intermediary in the e-payment field. This proposed model of intermediary not only settles payments, but it also takes care of such needs as confirming seller and buyer's identities, authenticating and verifying ordering and payment information and other transactional requirements lacking in virtual interactions.

5.1 Conduction of the study

- Initially, technical, business and user requirements should be considered for a payment system presenting an interoperable, modular, integrated, and extensible with payment architecture that provides the potentials for deploying security extensions.

- Secondly, according to the specified system requirements, a financial system evaluated and interactions between internal components and external components of the system.

- The third step will identify potentials of the payment model of the system for security enhancement along with preserving system behavior including protocols, services, transactions, and message structure.

- Next, an interface has been designed which is used to interact with the adopted financial system.

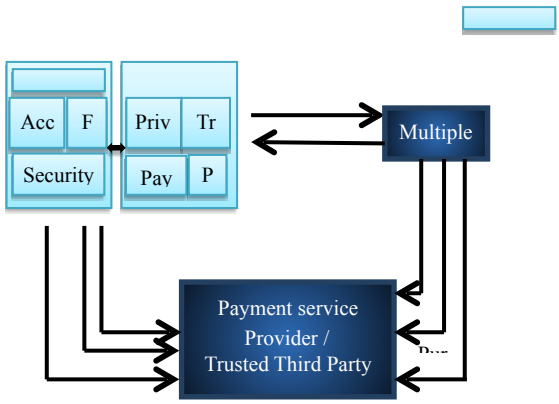
- Identifying potentials points of interactions between mobile applications and backbone system in applying security constraints was the starting point to employ security arrangements.

- According to all information related to evaluating system security potentials, security requirement specifications will be determined, so that the system can proceed persistently along with predicted security circumstances.

- Based on possible security requirement specifications, some of them should be adopted which are feasible in terms of design, implementation, and deployment in an efficient way.

- Finally, a methodology for security design and implementation will be planned.

1: Proposed System



The proposed model comprises with three entities Customer, Merchant and the Payment authority. Payment Authority is the one who initiates the process of message verification after receiving the transaction request. A process started from the order placement by the customer then merchant verifies the identity of the customer through payment authority and confirms the order. Following the sequence of events are occur during the transaction process.

1. The customer open an account and get its digital credentials.

2. The merchant acquires his/her digital credentials.

3. Customer opens the web of merchant and places the order to the merchant.

4. Merchant verifies the customer with its digital signature through payment authority.

5. Payment Authority checks the integrity of Payment order information using our protocol model and authorize the customer.

6. Merchant verifies the purchase and confirm the order.

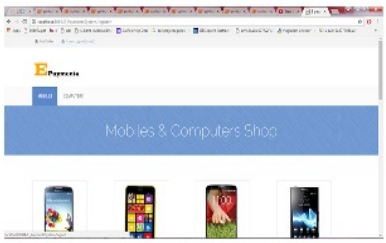


Fig1. Mobiles and C omputers

6.0 Results and discussion

6.1 privacy protection

In the proposed solution, another important aspect is protecting customer privacy. The proposed protocol guarantees that the customer and the merchant can maintain anonymity under any possible situation even when there is collusion by any 2 parties**.**

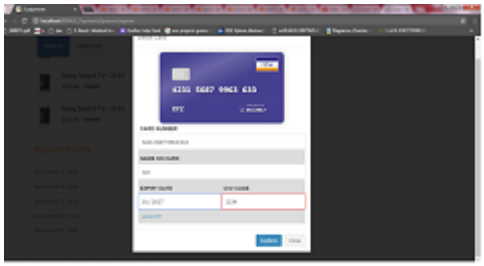


fig2. Creditcard Details

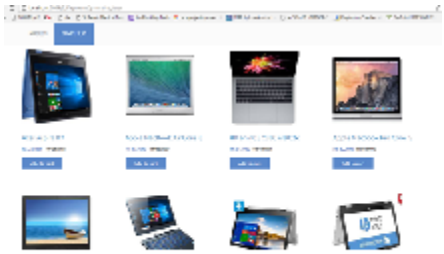


fig3.Lap Tops

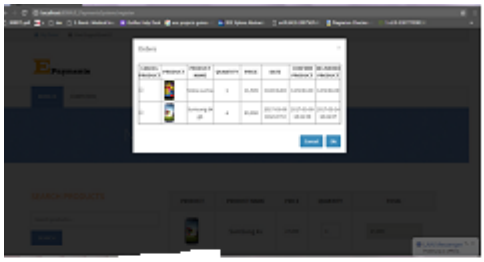


fig 4.Product Selection

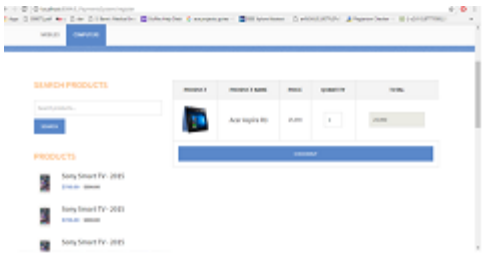


fig 5. computers

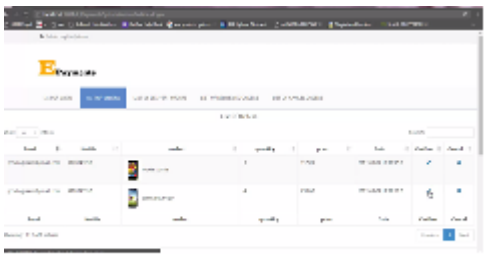


fig6 Epayments

6.2 Customer role and behavior Customer can create purchase order and authenticate payments. Customer usually initiate purchase request and provides personal details only to service provider. He provides only order related details to merchant. On the other hand merchant accepts order, generates sales invoice. He will have no access to customer's mobile number. Bank has key role in payment process. It will provide merchant account facility and normal customer account as well.

6.3 Analysis Payment order integrity is an important aspect of online shopping because both Customer and merchant can not be assumed honest. So before the confirmation of payment from payment authority it also necessary to check the customer merchant agreement on the payment order information. There are two possibilities in the transaction. Customer may claim for different order or payment. If he tries he will change m to m' which results that the two value

$$aY = a \log_b m$$

$$bx = b \log_a m'$$

will not be the same and transaction fails. Similarly merchant can also claim with different payment order information if he is dis-honenst. He has to make the change in m to m'. Again the two unit will not be same and payment authority can check the wrong payment order message.

$$a Y = a \log_b m'$$

$$bx = b \log_a m$$

6.4 Security

In our model, can able to protects private information from unauthorized access. Also, guarantees that the information is reliable; in transaction, it guarantees that the data received is equal to the data sent. Both are reached using combinations of cryptography functions (symmetric encryption algorithm for confidentiality and digest functions for the integrity). With a public key infrastructure (PKI), these security requirements can be reached. In this proposed model assumed that there is a PKI established in the system.

7.0 Conclusion

Online payment is the biggest challenge for ecommerce industry in Pakistan. World's famous e-payment service providers like PayPal, Google Checkout, and Moneybookers are not providing their services to local entrepreneurs. Available solutions are either not secure or impose very high amount of payment overhead. For sustainable developments in ecommerce, suitable e-payment system is required. Apart from technical requirements, system must be cost effective. Moreover, this model is only designed to verify the integrity of communication message between the two units by the third party. The system has the advantage of its simplicity and low cost implementation.

Reference

Abrazhevich, D. (2004). *Electronic Payment Systems: a User-Centered Perspective and Interaction Design*. Eindhoven, The Netherlands: Technische Universiteit Eindhoven.

Bishop, M. (2005). *Introduction to computer security*. Boston: Addison-Wesley.

Carbonell, M., Sierra, J.M. & Lopez, J. (2009). Secure multiparty payment with an intermediary entity. *Computers & Security*. [Online]. 28 (5). pp. 289–300. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0167404808001351.

Gupta, H. & Sharma, V.K. (2011). Role of Multiple Encryption in Secure Electronic Transaction. *International Journal of Network Security & Its Applications*. 3 (6). pp. 89–96.

Ismaili, H. El, Houmani, H. & Madroumi, H. (2014). A Secure Electronic Transaction Payment Protocol Design and Implementation. *International Journal of Advanced Computer Science and Applications*. 5 (5). pp. 172–180.

Khan, W.A., Yousaf, S., Mian, N.A. & Nawaz, Z. (2013). E-commerce in Pakistan: Growth potentials and e-payment solutions. In: *Proceedings - 11th International Conference on Frontiers of Information Technology, FIT 2013*. 2013, pp. 247–252.

Khodambashi, S. & Zakerolhosseini, A. (2014). A quantum blind signature scheme for electronic payments. In: *2014 22nd Iranian Conference on Electrical Engineering (ICEE)*. [Online]. May 2014, IEEE, pp. 879–884. Available from: http://ieeexplore.ieee.org/document/6999660/.

Laudon, K.C. & Traver, C.G. (2002). *E-commerce: business, technology, society*. London: Addison Wesley.

Raghuwanshi, S., Pateria, R.K. & Singh, R.P. (2009). A new protocol model for verification of payment order information integrity in online E payment system. In: *2009 World Congress on Nature and Biologically Inspired Computing, NABIC 2009 - Proceedings*. 2009, Coimbatore: IEEE, pp. 1665–1668.

Ribbers, P.M.A. & Heck, E. V. (2004). Introducing electronic auction systems in the Dutch flower industry - a comparison of two initiatives. *Wirtschaftsinformatik*. 4 (3). pp. 223–231.

Roy, S. & Venkateswaran, P. (2014). Online payment system using steganography and visual cryptography. In: *2014 IEEE Students' Conference on Electrical, Electronics and Computer Science*. [Online]. March 2014, IEEE, pp. 1–5. Available from: http://ieeexplore.ieee.org/document/6804449/.

Tan, J., Tyler, K. & Manica, A. (2007). Business-to-business adoption of eCommerce in China. *Information and Management*. 44 (3). pp. 332–351.

Tiwari, A. (2007). *A Multifactor Security Protocol for Wireless Payment-Secure Web Authentication using Mobile Devices*. Indian Institute of Information Technology, Allahabad.

Wang, C., Wu, J. & Duan, H. (2004). A fair off-line electronic cash scheme based on restrictive partially blind signature. *Tsinghua Science and Technology*. [Online]. 9 (4). pp. 441–443. Available from: http://ieeexplore.ieee.org/document/6075707/.

Yung, M. (2008). On the Evolution of User Authentication: Non-bilateral Factors. In: *Information Security and Cryptology*. Berlin Heidelberg: Springer.