Eliphas F. Tongora

E-commerce obstacles & security for online payment transaction in Tanzania

Ekonomiczne Problemy Usług nr 112, 207-218

2014

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 808 EKONOMICZNE PROBLEMY USŁUG NR 112 2014

ELIPHAS F. TONGORA
Politechnika Wrocławska[1]

E-COMMERCE OBSTACLES & SECURITY FOR ONLINE PAYMENT TRANSACTION IN TANZANIA

Summary

The rapid evolution of computing and communication technologies and their standardizations have made the boom in e-commerce possible. Lowering of the cost of operation, increase in the speed of transactions, and easy global reach to customers and vendors have been the reasons for the overwhelming popularity of this new way of commerce. However, in Tanzania many are still wary of using the internet for such transactions, unsure as to whether the security of their transactions would be guaranteed, Nature of online transaction in Tanzania is constrained by obstacles resulting from insecurity, unprotected transaction, lack of knowledge as well as trust. Online shopping could become predominant source of shopping method, if the obstacles associated with insecurity, trust and customer's protection are tackled by Tanzanian institutions or organizations. This paper highlights the obstacles and solutions related to the policy and private as well as security measures as the step toward secured online transaction payments. Since protocols like SSL, PKI and SET have proved to be effective in USA and European countries as the steps to be taken to assure efficient and effective online Payment transaction activities over the internet why not implementing these in Tanzania?

Keywords: online payment transaction/online shopping, Public Key Infrastructure, Digital Signature, Secure Socket layer, Secure Electronic Transaction, Secure E-commerce Protocol.

[1] Instytut Organizacji i Zarządzania.

Introduction

It is conceived that e-commerce is a phenomenon of developed country and new technology generally put challenges for developing countries like Tanzania that lacks the requisite capabilities, as well as the economic and financial resources to cope with the developed countries. Especially internet presents both opportunities for economic and social development and threat to further increasing the gap between developed countries and developing country like Tanzania (Paulo 2013). However, there is a concern over online shopping especially when customer's personal information and financial transactions is required to facilitate transaction through internet medium. A lack of trust is likely to discourage online consumer's intention from purchasing via online stores. However, with the existence of purchasing online, a secured system is needed to enhance online transaction since consumers cares for their privacy and security (Udo 2001).

1. Related work

An e-commerce obstacle such as security and trust is one of the principal and continuing concerns that limit customers and organizations engaging with e-commerce. The main goal of this paper is to highlights the solutions of online shopping obstacles and security strategy issues that face e-commerce for online payment transaction from both customer and organizational in Tanzania.

Due to the increasing warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers discouraged to perform online transactions and relate that to the lack of trust or fear for their personal information (Rashad, Noor 2011). The impact of security, protection and trust towards consumers as well as attitudes plays a key role in e-commerce implementation, if well implemented, instantaneous flow of goods and services internally and externally. Besides, vital information could also be simultaneously processed to match with data flowing from external e-commerce transactions which could allow for efficient and effective integration into organizational processes (Yuanqiao, Chunhui 2008). A transaction between buyers and sellers in e-commerce includes requests of information, quotation of prices, placement of orders and payment, and after sales services. The high degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain since they are exchanged over the Internet (Sengupta, Mazumdar 2005). Privacy and security can be viewed as ethical questions. At the same time the privacy and security area attracts a large amount of attention from the commercial sector because it has the potential to determine the success or failure of many business ventures, most obviously e-commerce activities (Biswajit, Jibitesh 2013).

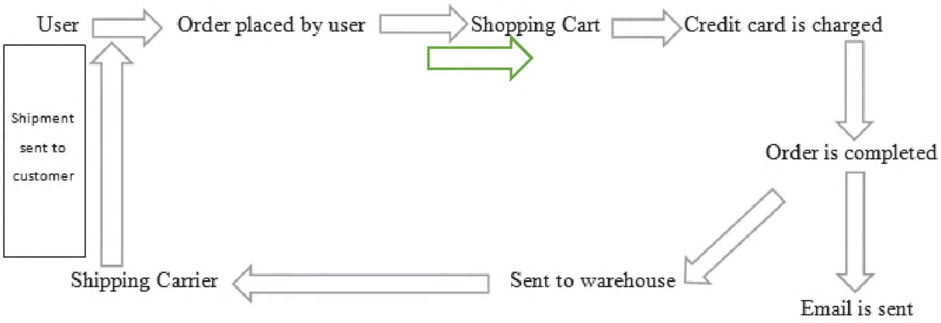

Fig. 1. Digital e-commerce cycle based on life cycle approach

Source: (Niranjanamurthy, Dharmendra 2013).

2. Major obstacles of e-commerce in Tanzania

Despite the fact that e-commerce has endless opportunities, there are numerous obstacles inhibit the successful uptake of e-commerce. One point of this presentation is to revealing the existing and prospective obstacles to e-commerce and devising their solutions in the context of Tanzania.

- Lack of sufficient Security system and reliability as a major technical limitation
- In sufficient of telecommunication bandwidth.
- The software development tools are still evolving and changing rapidly to catch up.
- The need for special web servers and other infrastructures, in addition to the network servers that means more cost.
- Possible problem of inter-operability meaning some software, hardware and other components are incompatible.
- Lack of trust and user resistance is the non-technical obstacle.
- Cost and justification is a non-technical limitation as well.

3. Study findings

Below is the studies conducted in which six major factors has been highlighted for e-commerce obstacles in Tanzania. Lack of security, lack of privacy, lack of experts.

Table 1

Main e-commerce obstacles in Tanzania

		Lac of sec	Lac of pri	Lac of inf	Lac of exp	Comp ill	Inap law
N	Valid	200	200	200	200	200	200
	Missing	0	0	0	0	0	0
Mean		2.9900	2.4500	2.7000	2.8500	2.3500	2.1500
Median		3.0000	2.0000	3.0000	3.0000	2.0000	2.0000
Std.Dev		1.1904	1.1904	1.1298	1.1723	.9550	.8551

Source: Based on the Prospects and Barriers of E-Commerce Implementation in Tanzania (Oreku, Fredrick, Mtenzi, Ali 2013).

The mean score of the variable lack of security shows that the average people to some extent agree about the fact that it has substantial contribution to the obstacles of e-commerce. The mean score of the lack of experts, computer illiteracy, and inappropriate laws indicates that the average respondents agreed that these variables have impact on the development of e-commerce in Tanzania. Security is one of the principal and continuing concerns that restrict customers and organizations engaging with e-commerce. The study collected and analyzed primary data about existing and prospective inhibitors from customers has identified critical factors toward e-commerce that is exactly the main goal of this paper trying to highlights and put forward steps to overcome this obstacle such as lack of security, privacy and policy of e-commerce in Tanzania (Oreku, Fredrick, Mtenzi, Ali 2013).

Based on that research, my opinion is still that e-commerce is not something new in this 21st century, although e-commerce in Tanzania is ta early stage. Tanzanian consumers are not well aware about online shopping due to the doubtful factors toward online shopping such security,trust and privacy when dealing with web merchants. Trust as an important obstacle factor affecting consumer behavior determines the success of online shopping in Tanzania. contrariwise, security, confidence and protection in e-commerce are determinant factors to consumer acceptance of e-commerce as an efficent business transaction strategy in Tanzania. On top of that delivery address could also raise concerns among consumers embarking online shopping in Tanzania. Government and business organiations could lift the limitations by affectively planning and implementing quality e-commerce shopping online strategy with consumers, however remains a potential strategy to boost business transaction in Tanzania.

4. The challenges of security, protection and trust of e-commerce in Tanzania

The obstacles associated with online shopping are more to consumer's protection in transaction that requires privacy and trust between different geographical locations. Also there is an increasing concern over online shopping because of the insecurity, lack of customer's protection and trust which are vital elements for a successful e-commerce online transaction in Tanzanian institutions and individuals.

Also it was pointed out that the major problem faced by consumers in an online transaction is security. From survey report, it is obvious the most reports acknowledged that transaction base on e-commerce have been constrained by security. In addition, consumers are concern about their privacy especially when their personal information are required to facilitate transaction besides, potential risks are also posed to those using credit cards to make purchase online. Secured system is needed enhance online shopping since consumers cares for their privacy and security (Udo 2001). I hereby proposed that efficient measures for effective implementation of e-commerce transaction in Tanzania economic developments should integrate web-based infrastructures so as to;

- Credit card issuance must be regulated to control and monitor fraud through predetermined security code and features.
- Transportation infrastructure through which goods and services are delivered should be enhanced through adapting good maintenance and change of outdated facilities.
- Transaction should be carried out only through secured network besides; parties embarking on online transaction should be acquainted on security-related issues to ensure reliability.
- Reduce high costs associated with internet access, such as pronounced in service connection charges, tariff on subscription and hosting charges for websites with sufficient bandwidth.
- The use of physical and residential addresses must be encouraged and to be well designed in some area.

4.1. Recommendations for solution to the problem of e-commerce obstacles in Tanzania

Tanzania still is a developing country and private organizations are not organized enough to provide with IT infrastructure, Government should initiate programs to reduce limitations:

- It is imperative that the World Trade Organization (WTO) support Limitation-free e-commerce and the WTO rules and disciplines are applied, and where necessary adapted, to ensure effective execution of e-commerce.

Adopting and implementing the WTO IT agreement on financial services and the WTO agreement on basic Telecommunications are essential for international business relating to e-commerce (Worldwide Coalition Calls for WTO Policy Agenda to Enhance Growth of E-Commerce).

- Creating effective distribution channels like postal service, direct delivery, third party delivery, and alliances with other established companies.
- Giving an education to the consumers about the easiest and advantages of online shopping.
- Careful selection of products to offer in the virtual stores in terms of nature and price of the products.
- Minimalize or removing any obstacle that hinder the effectiveness of the method in an online payment.

5. Security in e-commerce

The successful functioning of e-commerce security depends also on a complex interrelationship between several applications development platforms, database management systems, and systems software and network infrastructure.

E-commerce transaction phases			
Information phase	Negotiation phase	Payment phase	Delivery phase
Security measures			
Confidentiality Access control Integrity Checks	Secure Contract Identification Digital Signatures	Encryption	Secure Delivery Integrity Checks

Each phase of E-commerce transaction has a security measures.

Fig. 2. Security measures in different phases of e-commerce transaction

Source: (Yasin, Haseeb, Qureshi 2012).

6. E-commerce security protocols in online payment for Tanzanian

Online business organizations in Tanzania should search for high-tech security mechanism to protect itself from intrusion and also protect it customer from being indirectly invaded. There are two lines of defense for e-commerce which are technology solutions and policy solutions that can be implemented in Tanzania as a first step.

Secure Socket Layer: Secure Socket Layer (SSL) was developed by Netscape to provide secure communication between web servers and clients. The information is broken into packets, numbered sequentially, and an error control attached. Individual packets are sent by different routes (Zimmerman 2004). SSL is widely used on the Internet, especially for interactions that involve exchanging confidential information such as credit card numbers (Yasin, Haseeb, Qureshi 2012). SSL uses Public Key infrastructure and digital certificates to ensure privacy and authentication (Zimmerman 2004). SSL protects the communication between a client and a server and provides authentication to both parties to secure communication (Yasin, Haseeb, Qureshi 2012). SSL encryption is at transport layer rather than Application layer. SSL provides point to point security (Yasin, Haseeb, Qureshi 2012). Message is encrypted only during transmission over the network and other security mechanisms are required to handle security of the messages in an Application or disk. SSL is above TCP layer and below application layer. SSL allows many key exchange algorithms, but some algorithms such as Diffie-Hellman key exchange have no certificate concept (Zhiguang, Xucheng, Rong 2004). The design goal of the protocol is to prevent eavesdropping, tampering or message forgery when a data is transported over the Internet between two communicating applications (O'Mahony, Peirce, Tewari 2001).

Public key infrastructure: PKI provides a foundation for other security services. The purpose of a PKI is to allow the distribution and use of public keys and digital certificate to provide secure communication. There are some popular public-key encryption algorithms, for example, RSA, and ECC. The security of the most public-key encryption algorithms is based on discrete logarithms in finite groups or integer factorization (Yasin, Haseeb, Qureshi 2012; Amador, Green 2005; Laih, Chen 2004).

Secure Electronic Transactions (SET): A SET specification for credit/payment card transactions is required for the safety of all involved in e-commerce. It is designed to meet three main objectives. First, it will enable payment security for all involved, authenticate card holders and merchants, provide confidentiality for payment data and define protocols and potential electronic security service providers. It will also enable interoperability among applications developed by various vendors and among different operating systems and platform (Chapin, Skalka, Wang 2008; O'Mahony, Peirce, Tewari 2001).

- Digital Signatures and Certificates: Digital signatures provide the requirement for authentication and integrity. A sending message is run through a hash function and new value is generated known as message digest. The message digest and the plain text encrypted with the recipient's public key and send to recipient. The recipient decrypts the message with its private key and passes the message through the supplied hash algorithm. Digital certificate are also used for security purposes. CA issues an encrypted digital certificate to applicant that contains the applicant's public key and some other identification information. The recipient of an encrypted message can use the CA public key to decode the digital certificate attached to the receiving message that verify it as issued by the CA and then obtains the sender public key and identification information stored within the certificate (Yasin, Haseeb, Qureshi 2012).

- Availability and reliability; Apart from needing to secure, an electronic payment must be available and reliable. It must be available all the time, seven days a week, and 24 hours a day. It must also have some protection against denial-of-service attacks, or at least be able to detect them early and start recovery procedures. To ensure reliability, payment transaction must be atomic. This means they occur either entirely (i.e., completely successfully) or not all, but they never hang in an unknown or inconsistent state (Zhiguang, Xucheng, Rong 2004).

7. Strategy of e-commerce security

As e-commerce security problems caused by many factors, to solve the security problem from different aspects, offers a variety of counter measures (Yang 2009).

- Security Strategy: To ensure the safety communications must be the necessary measures to guard against them. Communications links, we can use a firewall, proxy server, Virtual Private Network (VPN) technology; in the identification and authentication, encryption and authentication techniques.
- Legal Protection: As e-commerce activities are a commodity transaction and security issues should be protected by law. Must ensure that the legal status of electronic contracts and digital signatures, electronic contracting parties to the contract approved Electronic Contract denied or modified to ensure that electronic contracts can be implemented.
- Social Moral Norms: e-commerce transactions are not direct and face-to face features transactions but often seen in the traditional process of e-commerce fraud and is bound to have security implications. Thus, the healthy development of e-commerce depends on the establishment and perfect.
- Perfect Management Strategy: As e-commerce transaction system is a highly integrated man-machine system, in addition to network security, and management is also very important, but the factors that play a decisive role.

8. Security tips to the problems of the online payment transaction for Tanzanian

- Transact to secured website; How do you say the website is secured? Encryption method is used to secure site by transferring information from one's computer to merchant computer and the information are encrypted before sending so that cannot be compromised by the hackers on its route. The only person who can unscramble the code is the one with the legitimacy access privilege. Here is how you can say the website is secured:

  - at the address bar where the website address is displayed is always shows https://. The "s" after "http" mean the website is secured in most cases appear in the order page of the site;
  - nevertheless, if the padlock displayed on the address bar of the screen is closed then it is assumed that the site is secured. It's advised to read the merchants privacy and security policy before online payment transaction for the security.

- Never reveal your password; Some online site payment require customers to login by providing username and password before proceeding the order in that case don't use your predicable information such as name, date of birth or surname and don't reuse the same password to the other website. You are strictly advised to use the password with the combination of letters and number combining at least eight characters
- Don't disclose unnecessary information during the order; Always when ordering online there is some information you must provide to the web merchant such as full name and address for deliver, but the merchant will try to get some more details about you for the market purpose that may lead to spam so you are advised not to disclose information that you feel is not required to process the order.
- Be careful with cookies; Cookies is used by online merchant and other sites to watch the surfing or online payment activities, an online tracking system attaches pieces of codes to the internet browser that tracks the site visited. Normally there are types cookies remaining stored in the computer and other type expire after turning off the computer and online merchant use cookies to recognize you and speed up the online payment process for the next site visit. Once you opt to disable the cookies the tradeoff may limit some of the functions online activities and possibly prevent from ordering online unless you enable session cookies to place the order.
- Understand the website security policy and privacy before ordering; Make sure you read and understand the website's privacy and policies. Reputable website offer details on how it processes the order. You will find out if the merchant intends to share you details with a third party or not, if happens merchant is the member of seal of approval program that sets voluntary guidelines for privacy and may change the merchant membership in web seal program and privacy policy then there is no guarantee that web merchant will always protect your privacy.

9. Future works

Residential addresses, reliability and online payment methods are still the challenges ongoing in e-commerce since Tanzania is still fresh new to this kind of business and needs to start having post codes and proper addresses because when one order product through online must be a way to deliver it to the buyer without always relying on express couriers because they're expensive. Also the Internet which is the primary medium most e-commerce transactions which is designed to encrypt data exchanges over the internet. E-commerce is evolving toward using XML (Extensible Markup Language) technology, which not only will serve as the foundation of many web services, but also will secure transactions between machines, relying on complex trust hierarchies to do so. SSL's foremost drawback is its reliance on certificate authentication at the user end, which requires users to have at least a basic understanding of the technology and processes involved in ensuring security. The same weakness is responsible for the demise of PKI (public key infrastructure) security; browser vulnerabilities and user ignorance often result in unsecured used for conducting e-commerce transactions which is not designed to handle transactions securely.

Conclusion

Despite the obstacles and insecurity to e-commerce, the future is bright. Internet is massively impacts all aspects of business and e-commerce is no longer an option for business revolution but necessity for Tanzanian. This paper has examined the existing and prospective obstacles including security to e-commerce to a successfully operation of e-commerce in Tanzania and suggest some strategies to overcome these obstacles including insecurity and trust. Furthermore; privacy integrity, confidentiality and non-repudiation are main security dimension to protect e-commerce transactions against threats. These objectives are achieved by cryptography functions and techniques. When customers and merchants perform online shopping the protection of information against security threats is a major issue. During sending the sensitive information, the data must be protected from unauthorized access to maintain its privacy and integrity. Finally the e-commerce innovation in Tanzania will help to grow small and medium enterprises to make business with the ICT utilization.

Literature

Amador J.J., Green R.W. (2005), *Symmetric-Key Block Cipher for Image and Text Cryptography*, "International Journal of Imaging and Technology", Vol. 15, No. 3, pp. 178–188.

Biswajit T., Jibitesh M. (2013), *Protective measures in e-commerce to deal with security threats arising out of social issues – a framework*, IAEME – ISSN 0976-6375 (online), Vol. 4, Issue 1, January–February.

Chapin P.C., Skalka C., Wang X.S. (2008), *Authorization in Trust Management, Features and Foundations*, "ACM Computing Surveys", August 2008, Vol. 40, No. 3, pp. 9.1–9.48.

Laih C.S., Chen K.Y. (2004), *Generating visible RSA public keys for PKI*, "International Journal of Information Security", Berlin, Vol. 2, No. 2, pp. 103–109.

Niranjanamurthy M., Dr. Dharmendra C. (2013), *The study of E-Commerce Security Issues and Solutions*, Vol. 2, Issue 7, ISSN (Print): 2319-5940, ISSN (online), 2278-1021, July.

O'Mahony D., Peirce M., Tewari H. (2001), *Electronic Payment Systems for E-Commerce*, Artech House Computer security series, Boston, Second Edition, pp. 19–69.

Oreku G., Fredrick J., Mtenzi J., Ali D. (2013), *The Prospects and Barriers of E-Commerce Implementation in Tanzania*, retrieved on 25th November 2013, http://www.zuj.edu.jo/conferences/icit11/paperlist/papers/E-Commerce/559_george_ali.pdf.

Paulo B.T. (2013), *E-Commerce readiness and diffusion: The case of Brazil*, "I-ways. Digest of Electronic Commerce policy and regulation", Vol. 26, pp. 173–183.

Raju B., Anjana J., Gulfishan F.A. (2010), *The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology*, "International Journal of Computer Science and Information Security", April, Vol. 8, No. 1.

Rashad Y., Noor E. (2011), *Security and Privacy Issues as a Potential Risk for Further E-commerce Development*, International Conference on Information Communication and Management – IPCSIT, Vol. 16.

Sengupta A., Mazumdar C. (2005), *E-commerce security – A life cycle approach*, Vol. 30, pp. 119–140.

Udo G.J. (2001), *Privacy and Security Concerns as Major Barriers for E-commerce, a Survey Study*, "Information Management and Computer Security", Vol. 9, No. 4, pp. 165–174.

Yang J. (2009), *On-line Payment and Security of E-commerce*, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), May 22–24, pp. 046–050.

Yasin S., Haseeb K., Qureshi R.J. (2012), *Cryptography Based E-Commerce Security*, "IJSCI International Journal of Computer Science Issues", Vol. 9, Issue 2, No. 1, March.

Yuanqiao W., Chunhui Z. (2008), *Research on E-Commerce Security Issues*, International Seminar on Business and Information Management, Vol. 1, pp. 186–189.

Zhiguang Q., Xucheng L., Rong G. (2004), *A survey of E-commerce Security*, "Journal of Electronic Science and Technology of China", Vol. 2, No. 3, pp. 173–179, 199.

Zimmerman P. (2004), *An Introduction to cryptography* (found in the documentation of PGP® Desktop 8.1), Page 17, June.

E-COMMERCE: BEZPIECZEŃSTWO I PRZESZKODY W TRANSAKCJACH PŁATNICZYCH ONLINE W TANZANII

Streszczenie

Szybki rozwój technologii komputerowych i komunikacyjnych oraz ich standaryzacja umożliwiły szynki rozwój e-commerce. Obniżenie kosztów pracy, zwiększenie szybkości operacji, globalny zasięg i łatwe dotarcie do klientów i dostawców przyczyniły się do wzrostu popularności nowego sposobu handlu. Są jednak kraje, takie jak Tanzania, gdzie obawy przed tego rodzaju działalnością owocują dużą ostrożnością podczas korzystania z zakupów przez Internet. Główną przyczyną takiej sytuacji jest obawa o bezpieczeństwo swoich transakcji. Zakres transakcji online w Tanzanii jest ograniczony przez przeszkody wynikające właśnie ze strachu, wątpliwego zabezpieczenia transakcji, braku wiedzy oraz zaufania do kontrahentów. Zakupy online mogą stać się głównym sposobem transakcji zakupu, o ile przeszkody związane z bezpieczeństwem, zaufaniem i ochroną klienta zostaną zwalczone przez instytucje i organizacje w Tanzanii. W artykule zwrócono uwagę na przeszkody i rozwiązania zarówno w sektorze publicznym, jak i prywatnym, a także na środki bezpieczeństwa, które mają doprowadzić do upowszechnienia bezpiecznych płatności transakcji internetowych. Skoro protokoły takie jak SSL, PKI i SET okazały się skuteczne w USA i krajach europejskich, dlaczego więc nie zastosować ich jako pierwszych kroków ku zapewnieniu efektywnych i skutecznych transakcji online w Tanzanii?

Słowa kluczowe: płatności online, zakupy online, infrastruktury klucza publicznego (PKI), podpis cyfrowy, Secure Socket Layer (SSL), bezpieczne transakcje elektroniczne, bezpieczny protokół e-commerce.

Tłumaczenie Anna Kamińska