An Overview of Online Transaction Technologies in E-Commerce

K. Vishvalingam, T.C. Sandanayake
Faculty of Information Technology
University of Moratuwa, Katubedda, Moratuwa, Sri Lanka

Abstract - **Trust has been accepted as a critical element in electronic commerce due to the fact that online transactions are characterized as a process that involves uncertainty and risk. Trust also has been thought of as the most effective means of reducing uncertainty and risk. The effect of measures to build and maintain trust in e-commerce is subject to person-specific and situation related factors that cannot be controlled by web vendors. This study has explored a factor that influences trust during online transaction. And it need to address a number of security issues in order to be an effective and secure means of transferring payments across the Internet. To be accessible to a wider audience, they also need to be easy to use for their end-users. This research paper address these issues about the technologies in Online Transaction System. This paper contains the study area of the Online Transaction System and its Security issues.**

Index Terms: **Online Transaction, Security, E-commerce**

I. INTRODUCTION

The Internet has become an essential tool for commerce and financial services. With the help of new communication technologies, these services have experienced tremendous growth. They are becoming more and more accessible to customers, regardless of their location. An inhibiting factor for this growth is the fear of fraud and sensitive data theft, which is widespread among the general public due to lack of such security a significant portion of the customers are feel uncomfortable to send their respective identity over the Internet. In traditional business, customers accept the security risks in places like departmental stores because they can see and touch the products and make judgments about the store, which is almost absent in case of an e-commerce system [1]. In order to win customer's trust, the e-commerce transaction system should be competent enough to avail of the advantages of the appropriate technology to combat the Internet security threats caused by hackers. Thus, to get the opportunity of expanding the businesses by the firms an e-commerce system must be earn the confidence of the customer. The risk and the challenges of the trust that discourage the customer to participate in the e-commerce system are spoofing, interception of sensitive data, data alteration, and denial of services and overcharge. In order to offer solution to the above problems, I have to learn about online transaction system technologies in e-commerce. And also various attempts have been made earlier, which include in digital certificates for web and online transaction system [1].

The present research paper has been organized as follows: overview of the technologies in online transaction system in E-commerce, Major researches in Online Transaction System of our study, Securing Mobile platform, the Discussion of the study area and finally, contribution and discussion.

II. OVERVIEW OF ONLINE TRANSACTION

The Online Transaction Systems are essential for the growth of e-commerce. Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the Internet and other computer networks. Electronic commerce draws on such technologies as electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange(EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web at least at one point in the transaction's life cycle, although it may encompass a wider range of technologies such as e-mail, mobile devices and telephones as well [2].

Online Transaction Processing (OLTP)

OLTP (Online transaction processing) is a class of program that facilitates and manage transaction oriented applications, typically for data entry and retrieval transactions in a number of industries, including banking, airlines, mail-order, supermarkets, and manufacturers. Probably the most widely installed OLTP product is IBM's CICS (Customer Information Control System).

Today's online transaction processing increasingly requires support for transactions that span a network and may include more than one company. For this reason, new OLTP software uses client/server processing and brokering software that allows transactions to run on different computer platforms in a network.

Online transaction processing (OLTP) is transaction processing that occurs interactively Online transactions have a small amount of input data, a few stored records accessed and processed, and a small amount of data as output, immediate response time, usually less than one second, large numbers of users involved in large numbers of transactions, Round-the-clock availability of the transactional interface to the user and assurance of security for transactions and user data. In a bank branch office, for example, customers use online services when checking an account balance or making an investment [3,4].

Transaction Processing Activities

Data Collection is the process of capturing and gathering all data needed to complete one or more transactions. Can be done manually or using devices like scanners and point-of-sale equipment. Data Editing is the process of checking data for validity and completeness. Data Correction is the process of reentering miss-keyed or miss-scanned data that was found during the data editing. Data Manipulation is the process of performing calculations and other data transformations like classifying data and sorting files. Data Storage is the process of placing transaction data into one or more databases. Document Production is the process of creating reports and outputting records [4].

Methods of Transaction Processing

Batch Processing is the method that collects transactions in groups, called batches, and processes them together (i.e., old CSUS registration). On-line Transaction Processing is the method that completes business transactions as they occur (i.e., airline reservation or bank withdrawal). On-line Delayed Processing is a compromise of the batch and on-line transaction processing when transactions are entered in the computer as they occur, but are not processed immediately (i.e., ordering over the phone) [2].

III. MAJOR RESEARCHES IN ONLINE TRANSACTION SYSTEM

Wireless

The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy (WEP), is not very effective. WEP is built into all standard 802.11 products, but its use is optional. Many users neglect to use WEP security features, leaving them unprotected. The basic WEP specification calls for an access point and all of its users to share the same 40-bit encrypted password, which can be easily decrypted by hackers from a small amount of traffic. Stronger encryption and authentication systems are now available, such as Wi-Fi Protected Access 2 (WPA2), but users must be willing to install them [5].

Malicious Software

Malicious software programs are referred to as malware and include a variety of threats, such as computer viruses, worms, and Trojan horses. Computer virus is a rogue software program that attaches itself to other software programs or data files in order to be executed, usually without user knowledge or permission. Worms are independent computer programs that copy themselves from one computer to other computers over a network. Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system [6].

Spoofing and Sniffing

Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake e-mail addresses or masquerading as someone else. Spoofing also may involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination. A sniffer is a type of eavesdropping program that monitors information traveling over a network [1].

When transaction information is transmitted through the Internet, hackers can intercept the transmission and obtain customers' sensitive information like credit card number, username, password etc [1].The content of a transaction may not only be intercepted, but also may be altered en route, either maliciously or accidentally. Customer names, credit card numbers, and amounts sent through the Web all are vulnerable to such alteration [1].

Denial-of-Service Attack - In a denial-of-service (DoS) attack, hackers flood a network server or Web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests [7].

Overcharge - The fraudulent activities may include charging the customers at a higher than the agreed prices for the good or service ordered by the customer[1].

Security Controls in E-commerce Transaction System.

Sufficient security controls are required to reduce the associated risk in E-commerce transaction system. However, these controls should not be so restrictive that the overall performance of the system is degraded. Some of such controls are as follows [1]:

Authentication- This is the most primitive method of using a username and password combination for protecting contents of a Website from being accessed. Username and password combination are easy to detect, therefore it is not a good approach for Website protection [8]. New authentication technologies, such as tokens, smart cards, and biometric authentication, overcome some of these problems. Token is a physical device, similar to an identification card that is designed to prove the identity of a single user. Tokens are small gadgets that typically fit on key rings and display pass codes that change frequently [9]. Smart card is a device about the size of a credit card that contains a chip formatted with access permission and other data. (Smart cards are also used in electronic payment systems.) A reader device interprets the data on the smart card and allows or denies access [9].

Biometric authentication uses systems that read and interpret individual human traits, such as fingerprints, irises, and voices, in order to grant or deny access. Biometric authentication is based on the measurement of a physical or behavioral trait that makes each individual unique. It compares a person's unique characteristics, such as the fingerprints, face, or retinal image, against a stored profile of these characteristics to determine whether there are any differences between these characteristics and the stored profile. If the two profiles match, access is granted. Fingerprint and facial recognition technologies are just beginning to be used

for security applications, with many PC laptops equipped with fingerprint identification devices and several models with built- in webcams and face recognition software [10].

Access Control - This restricts different groups of authorized users to access subsets of information and ensures that only the intended user could access data and services offered by the system. Access control could only be a part of entire security system and therefore is not a full-fledged security control mechanism [11].

Encryption - During the initial stage of digital data protection encryption is used, based on cryptographic algorithms. Cryptography is implemented by transforming the digital information into encrypted digital information, which is thereafter inaccessible. Two major categories of encryption systems are symmetric key encryption and asymmetric key encryption.

Encryption can be a way of protecting transmitted data over the Web based on cryptographic algorithms, but this is not sufficient. It doesn't prevent someone from copying a file but it prevents access to the content of a file. Encryption works only when a person holding a key is the one who wants to protect the digital file. Giving the key to anyone else negates the purpose of the encryption [12].

There are two alternative methods of encryption: symmetric key encryption and public key encryption. In symmetric key encryption, the sender and receiver establish a secure Internet session by creating a single encryption key and sending it to the receiver so both the sender and receiver share the same key. Its bit length measures the strength of the encryption key. Today, a typical key will be 128 bits long (a string of 128 binary digits).

The problem with all symmetric encryption schemes is that the key itself must be shared somehow among the senders and receivers, which exposes the key to outsiders who might just be able to intercept and decrypt the key. A more secure form of encryption called public key encryption uses two keys one shared (or public) and one totally private.

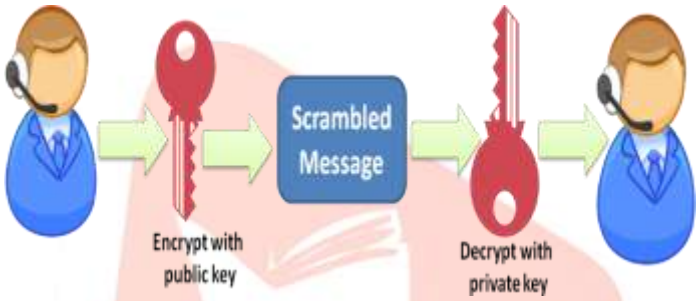

Figure 1: Public key Encryption

The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key. To send and receive messages, communicators first create separate pairs of private and public keys. The public key is kept in a directory and the private key must be kept secret. The sender encrypts a message with the recipient's public key. On receiving the message, the recipient uses his or her private key to decrypt it [12].

A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message (Figure 1).

Firewall - Firewalls are software or hardware security measure that filters information passing between an internal and external network. A firewall controls access to the Internet by internal users, and also prevents outsiders from access to the systems and the information stored on the internal network. A firewall typically could be one of the two forms: Software firewall and Network firewall (Figure 2).

It is generally placed between the organization's private internal networks and distrusted external networks, such as the Internet, although firewalls can also be used to protect one part of a company's network from the rest of the network .[13]. The firewall acts like a gatekeeper who examines each user's credentials before access is granted to a network. The firewall identifies names, IP addresses, applications, and other characteristics of incoming traffic. It checks this information against the access rules that have been programmed into the system by the network administrator. The firewall prevents unauthorized communication into and out of the network.

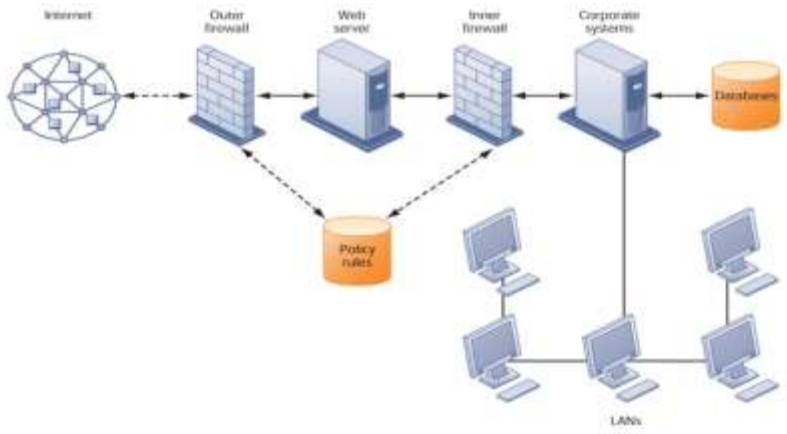

Figure 2: Corporate Firewall

In large organizations, the firewall often resides on a specially designated computer separate from the rest of the network, so no incoming request directly accesses private network resources. There are a number of firewall screening technologies, including static packet filtering, stateful inspection, Network Address Translation, and application proxy filtering. They are frequently used in combination to provide firewall protection. [14]

Packet filtering examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet, examining individual packets in isolation. This filtering technology can miss many types of attacks.

Stateful inspection provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver. It sets up state tables to track information over multiple packets. Packets are accepted or rejected based on whether they are part of an approved conversation or whether they are attempting to establish a legitimate connection.

Network Address Translation (NAT) can provide another layer of protection when static packet filtering and stateful inspection are employed. NAT conceals the IP addresses of the organization's internal host computer(s) to prevent sniffer programs outside the firewall from ascertaining them and using that information to penetrate internal systems.

Application proxy filtering examines the application content of packets. A proxy server stops data packets originating outside the organization, inspects them, and passes a proxy to the other side of the firewall. If a user outside the company wants to communicate with a user inside the organization, the outside user first "talks" to the proxy application and the proxy application communicates with the firm's internal computer. Likewise, a computer user inside the organization goes through the proxy to talk with computers on the outside [15].

Protecting from Viruses and Spywares

Both individuals and businesses must include antivirus protection for every computer. Antivirus software is designed to check computer systems and drives for the presence of computer viruses. Often the software eliminates the virus from the infected area. However, most antivirus software is effective only against viruses already known when the software was written. To remain effective, the antivirus software must be continually updated. Antivirus products are available for many different types of mobile and handheld devices in addition to servers, workstations, and desktop PCs [6].

Digital Signature - In an E-commerce system, digital signatures are used to sign licenses between participating users for transmitting digital content over the Web. The licenses are thereafter used as a proof of usage rights. At the client side such licenses are verified for the verification of the usage rights. Digital signature has the limitation of distribution, i.e. once a customer purchases the usage rights he can distribute the rights over the Internet, which causes a violation of the copyright [1].

Digital Certificates - Digital certificates are data files used to establish the identity of users and electronic assets for protection of online transactions. A digital certificate system uses a trusted third party, known as a certificate authority (CA), to validate a user's identity (Figure 3).

The CA verifies a digital certificate user's identity offline. This information is put into a CA server, which generates an encrypted digital certificate containing owner identification information and a copy of the owner's public key. The certificate authenticates that the public key belongs to the designated owner. The CA makes its own public key available publicly either in print or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it was issued by the CA, and then obtains the sender's public key and identification information contained in the certificate.

Using this information, the recipient can send an encrypted reply. The digital certificate system would enable, for example, a credit card user and a merchant to validate that an authorized and trusted third party issued their digital certificates before they exchange data. Public key infrastructure (PKI), the use of public key cryptography working with a CA, is now widely used in e-commerce [14].

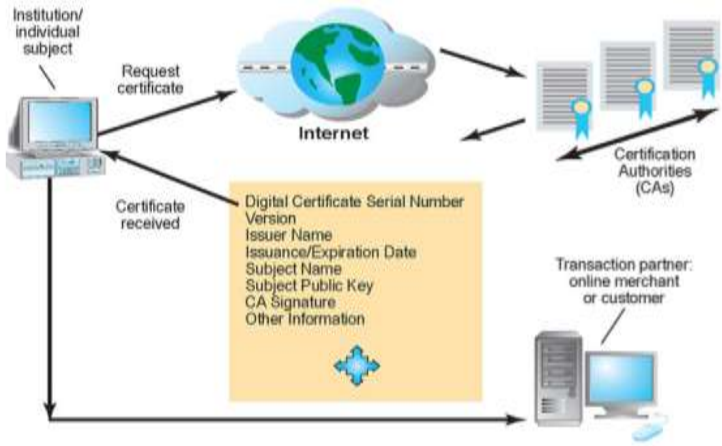

Figure 3 - Digital certificates

Secure Transaction Protocols used in current E-commerce

Electronic transactions are the main activities of e-commerce. Electronic transactions here are nothing more than exchanging information or messages between parties involved in transactions. Messages can be anything such as order form, confirmation messages, credit card numbers or documents. Since transactions are actually the main activities of e-commerce, then it is important to secure the transactions from any kind of threat. As stated by Cameron that the most critical factor in success of electronic commerce is transaction security [1].

The Internet offers no security whatsoever to business transactions. Information travels over the Internet through series of routing, which means information can be routed through many computer systems before it reaches the trusted server. Any one of these computer systems can represent an opportunity for the information to be accessed or even changed. To support secure information exchange (including e- commerce transactions) currently there are several security protocols based on encryption methods discussed in the previous section. In this section, we will discuss two security protocols commonly used in the Internet to support Internet-based e- commerce, namely Secure Socket Layer (SSL) and Secure Electronic Transaction (SET).

Secure Socket Layer - Secure Socket Layer (SSL) is a security protocol developed by Netscape Communications to protect communication over the Internet. SSL works to protect the Internet communication by server authentication, encryption [16].

Secure Electronic Transaction - A protocol designed to ensure the security and integrity of online communications and purchases, Secure Electronic Transaction (SET) uses digital certificates, issued to merchants and other businesses and customers, to perform a series of security checks verifying that the identity of a customer or sender of information is valid. SET provides the basic framework within which many of the various components of securing digital transactions function. Digital certificates, digital signatures, and digital wallets all function according to the SET protocol [16].

IV. SECURITY ISSUES FOR CLOUD COMPUTING AND THE MOBILE DIGITAL PLATFORM

Although cloud computing and the emerging mobile digital platform have the potential to deliver powerful benefits, they pose new challenges to system security and reliability. We now describe some of these challenges and how they should be addressed.

Security in the Cloud

When processing takes place in the cloud, accountability and responsibility for protection of sensitive data still reside with the company owning that data. Understanding how the cloud computing provider organizes its services and manages the data is critical. The Interactive Session on Technology details some of the cloud security issues that should be addressed.

Cloud users need to confirm that regardless of where their data are stored or transferred, they are protected at a level that meets their corporate requirements. They should stipulate that the cloud provider store and process data in specific jurisdictions according to the privacy rules of those jurisdictions. Cloud clients should find how the cloud provider segregates their corporate data from those of other companies and ask for proof that encryption mechanisms are sound. It's also important to know how the cloud provider will respond if a disaster strikes, whether the provider will be able to completely restore your data, and how long this should take. Cloud users should also ask whether cloud providers will submit to external audits and security certifications. These kinds of controls can be written into the service level agreement (SLA) before to signing with a cloud provider [17].

Securing Mobile Platforms

If mobile devices are performing many of the functions of computers, they need to be secured like desktops and laptops against malware, theft, accidental loss, unauthorized access, and hacking attempts. Mobile devices accessing corporate systems and data require special protection.

Companies should make sure that their corporate security policy includes mobile devices, with additional details on how mobile devices should be sup- ported, protected, and used. They will need tools to authorize all devices in use; to maintain accurate inventory records on all mobile devices, users, and applications; to control updates to applications; and to lock down lost devices so they can't be compromised. Firms should develop guidelines stipulating approved mobile plat- forms and software

applications as well as the required software and procedures for remote access of corporate systems. Companies will need to ensure that all smart phones are up to date with the latest security patches and antivirus/anti- spam software, and they should encrypt communication whenever possible[17].

V. DISCUSSION

The online transaction system technologies in e-commerce is an important and useful studied area. Most of the people who are using this system in the transaction side they have some sort of hesitation. This study has covered areas related to the transaction systems, its characteristics and functionalities and the technologies that used for the security controls. Those are some issues in the transaction security are vital in e-commerce, hesitation in transaction security over the Internet. However, when it comes to decide to buy a product/service over the Internet many people worry about the transaction security. Similarly, firms worry about online frauds. Encryption technology discussed in this paper is key technology to make online transaction over the Internet secure. Of course no one can guarantee 100% security Fraud exists in current commerce systems: cash can be counterfeited, checks altered, credit card numbers stolen. Yet these systems are still successful because the benefits and conveniences outweigh the losses. Similarly fraud will still exist in e- commerce even though encryption technology is good enough to protect electronic transactions, but at least a good encryption technology can reduce fraud significantly.

REFERENCES

[1] Innovative Systems Design and Engineering ISSN 2222-1727/ISSN 2222-2871, Vol 3, No 6, 2012

[2] Wikipedia, Electronic Commerce, http://en.wikipedia.org/wiki/Electronic-commerce

[3] IBM Knowledge Center,Main frame computers, http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp?topic=/com.ibm.zos.Zmainframe/zconc_onlinetrans.htm

[4] K. Wrona, M. Schuba, G. Zavagli, Mobile payment state of the art and open problems., Proceedings of 2nd International Workshop WELCOM, volume 2232 of Lecture Notes in Computer Science, Springer-Verlag, 2001, pp.88-100.

[5] The Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology, Volume 298, 2009, pp 119-134

[6] Trend Micro, Addressing Big Data Security Challenges :The Right Tools for Smart Protection, http://www.trendmicro.com/cloud-content/us/pdfs/about/wp_big-data-security-challenges.pdf

[7] Wikipedia, Denial-of-service attack, http://en.wikipedia.org/wiki/Denial-of-service_attack

[8] *Cameron, D.* , Security Issues for the Internet and the Web, Computer Technology Research Group Corp, Report,1997

[9] SWITCH, Authentication and Authorization Infrastructure (AAI) in a nutshell https://www.switch.ch/aai/docs/AAI-Flyer_en.pdf

[10] Network Authentication, Authorization, and Accounting Protocols: Part Two - The Internet Protocol Journal - Volume 10, No. 2, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-2/102_aaa-part2.html

[11] Barbara Carminati, Elena Ferrari, "Access control and privacy in web-based social networks", International Journal of Web Information Systems, Vol. 4 Iss: 4, pp.395 – 415, 2008

[12] Majdi Al-qdah& Lin Yi Hui. International Journal of Computer Science and Security, Volume (1) : Issue (1). 33. Simple Encryption/Decryption Application, 2003

[13] Avolio, F.M., Ranum, M.J., A Network Perimeter With Secure External Access http://www.avolio.com/papers/isoc.html, 1993

[14] Bellovin SM., Cheswick WR., Network Firewalls, IEEE Communications Magazine September 1994 , http://people.scs.carleton.ca/~soma/id/readings/bellovin-firewalls.pdf

[15] Feruza s., Tao-hoon Kim IT Security Review: Privacy, Protection, Access Control, Assurance and System Security, International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007

[16] Bella, F. Massacci, L.C. Paulson, An overview of the verification of SET.International Journal of In formation Security, 2005, 17-28.

[17] Arora p., Singh A., Tyagi H., Evaluation and Comparison of Security Issues on Cloud Computing Environment, World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741,Vol. 2, No. 5, 179-183, 2012