International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 1, January 2017

ISSN: 2394-4404

Online Transaction Security Issues In A Digitally Enabled Business Environment

Dr. Mushthaq Ahammed K.

Assistant Professor and Course Coordinator of Commerce,
School of Distance Education, University of Kerala,
Thiruvananthapuram

Abstract: ***Digital and Electronic Business based on internet and web can lead to competitive advantage and can increase profitability. But, there are several ethical factors that are substantial on the success of web based digital business. Security is one of such key factors to the success of online shopping and lack of security is the significant problem on the way to web based digital business success. In every business transactions, the parties involved should feel privacy and trust with the people and the companies. Organizations must give due concern on the issues relating to the security and privacy in web services of electronic business. Security services offering protection from security threats such as identification, confidentiality, authentication, integrity, access control, and non-reputation. The present study, therefore, analyses the issues relating to problems and prospects augment of the trust, privacy and security in Online Business Transactions and also addressed security concerns in web bases business services.***

Keywords: Digital Business, E-Commerce, Online Transactions, Security Issues, Web Based Business

I. INTRODUCTION

Web Based Digital Business is the ability of a company to have a dynamic presence on the Internet which allowed the company to conduct its business electronically, in essence having an electronic/ digital shop. Products can be advertised, sold and paid for all electronically without the need for it to be processed by a human being. Due to the vastness of the internet advertising and the website will be exposed to hundreds of people across the globe for almost zero cost and with information being able to be changed almost instantly the site can always keep up to date with all the most recent products to match with customers demands. The major advantage of online based business is the ability to provide secure shopping transactions via the internet and attached with almost instant verification and validation of debit/credit card and online banking transactions. This has caused Web based business sites to explode as they cost much less than a store front in a town and has the ability to serve many more customers. In the broad meaning web based business or Web based business is a means of conducting business using one of many electronic methods, usually involving telephones, computers (or both). Web based business is not about the technology itself, it is about doing business using the technology

The arrival of internet-based electronic business over the last decade has given businesses an unparalleled marketing opportunity. As the Internet-using population has grown, so too has the potential market size for any business that sets up a shop on the Web. An increasing number of Indians are shopping online. India has an internet user base of about 463 million as of June 2016 that represents 34.8% of the Indian population (Internet World Stats 2016). The number of people who have purchased a product or engaged in banking online more than doubled in the past year, growing from 3.7% of the Indian population in 2007 to more than 29% in 2015 (Internet World Stats 2015). This increased Web Based Business activity has translated in growing online sales revenue in India. . The continuing raise of Internet users in general, and in particular use for product explore and online shopping, has not gone unobserved by firms in India. It is evident from this that firms are using the internet to reach clients in some way,

with partially reporting that they in fact sell products and services over the Internet. In such a backdrop the security, privacy and trust are very often befallen as constraints ahead of web based business transactions.

II. BACKGROUND OF THE STUDY

Web based business is the utilization of information and communication technology to conduct business activities such as buying and selling, servicing customers and collaborating with business partner on the internet. E- Commerce practices enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers. Trust is the key to the success of web based business and lack of trust is the significant problem on the way to web based business success. In every business transaction, the parties involved should feel privacy and trust with the people and the companies. Security services offering protection from security threats such as identification, authentication, confidentiality, integrity, access control, and non-reputation. Today, online shopping applications are doing more than ever to increase efficiency and improve relationships with partners and customers.

The Security and policy facet is another important contemplation in web based business. The development and implementation of policies that would support the security, privacy, trust and other ethical side of web based business activities that need should be explored. While web based business has witnessed extensive growth in last decade, consumers concerns regarding security issues also continue to increase. Even many consumers and businesses are beveling in web based business; consumer problems related to online selling and purchasing become the dark side of the issue. Security and privacy are concerned with the numerous ethical questions that managers must confront as part of their daily business decision-making.

In relation to trust in internet technologies, consumers are concerns about two main things which are privacy and security. This study is focusing on the issues relating to web based business, such as its importance, issues and the solutions in order to overcome related to the security, privacy and trust issues in web based business.

III. RESEARCH ISSUES

The following are the major issues under the purview of the present study:

- ✓ Lack of practical knowledge on online transactions and web based business operations and procedures
- ✓ Lack of awareness regarding the privacy and security involved in online transactions and internet shopping.
- ✓ Lack of confidentiality relating to web based business and online transactions.

IV. STATEMENT OF PROBLEM

Many companies implemented web based business extensively in order to simplify purchasing processes by customers. Almost all trading and business activities including banking can be performed online. These trends provide a lot of advantages both to customers and business organizations. However, the bad side about web based business also cannot be ignored. The bad side we mean is about the ethical issues and the issues connected with security and trust in web based business. These issues involve the irresponsible parties who always give threats both to consumers and business organization. There is almost an uncountable number of ways that a web based business setup could be attacked by hackers, crackers and disgruntled insiders. Common threats include hacking, cracking, eavesdropping, spoofing, sniffing, masquerading, Trojan horses, bombs, viruses, wiretaps, etc. Therefore the present study analyses the security problems and challenges in online transactions in a digitally enabled business environment.

V. RESEARCH OBJECTIVES

The important objectives of the present investigation are:

- ✓ To understand the awareness regarding security and privacy issues in web based business transaction.
- ✓ To analyze the confidentiality and issues of security and privacy relating to web based business.
- ✓ To give a better understanding on how businesses and consumers can be safe from online threats.

VI. RESEARCH DESIGN AND METHODOLOGY

Present Study is descriptive in nature and Descriptive approach of research is used for the study. Since the study is qualitative and analytical in nature, the literature and data required were gathered from various secondary sources consist of journals, newspapers, books, magazines, annual reports, online search database, library websites, and online data bases like jstore, Pro Quest, Scince Direct etc. Some of the information and data were also obtained from the Internet search engines like Google, infospace, Yahoo, mywebsearch etc.

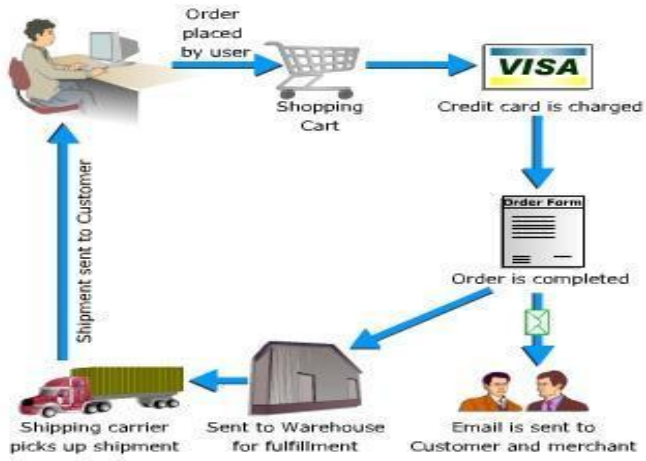
VII. ONLINE TRANSACTIONS AND DIGITAL BUSINESS

Digital Business/ E-Business/ E-Commerce is not simply a new distribution channel, or a new way to communicate. It is many other things: a marketplace, an information source, a tool for manufacturing goods and services. It changes the way managers run their everyday business, from locating a new supplier to coordinating a project, to collecting and managing customer data. Each such activity have an effect on the corporation in diverse ways, with the result that Electronic Business brings changes that are more pervasive than whatever thing we have seen from communication and information technology. E-Business can be defined as

business transactions, customer service, and intra-business operations that make use of digital communications. Electronic Business, broadly, is "The use of electronic networks to exchange information, products, services and payments for commercial and communication purposes between individuals (consumers) and businesses, between businesses themselves, between individuals themselves, within government or between the public and government and between business and government." The essential infrastructure for Digital Business and the new economy is a digitally networked computing setting that links firms, entities and individuals in business, industry, non-profit institutions, government, and the home.

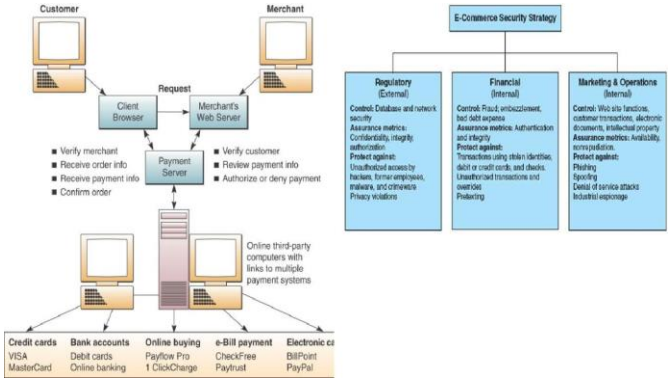
Businesses can have two types of existence on the Internet, a partial presence, and an absolute presence. Majority of business firms have partial Internet presence that it is done by having a straightforward marketing site. The purpose of the website is to supplement traditional marketing activities, perhaps give supplementary information, and generally promote the company. There is often a reluctance to give entire product details because the objective is to encourage visitors to call or write to the firm for more information and thus establish contact. Digitally enabled businesses have a complete Internet presence that is implemented by having a selling website in addition to the marketing and advertising site. Its objective is to close the sale electronically with payment made over the Internet. This type of site will be designed to consist of comprehensive product and services information as visitors may be expected to make a purchasing decision based on the information presented. Such websites usually have three different sections. The opening section is for attracting customers and containing marketing and added value information. The second section is for giving detailed information including prices about the products and services. The last section is for online shopping cart and order processing.

WEB BASED DIGITAL/ ELECTRONIC BUSINESS CYCLE



Source: Niranjanamurthy M and Dharmendra Chahar 2013, E-Commerce Security Issues and Solutions

Figure 1



Source: Niranjanamurthy M and Dharmendra Chahar 2013, E-Commerce Security Issues and Solutions

Figure 2

VIII. ANALYSES AND INTERPRETATIONS

A. ONLINE TRANSACTION SECURITY ISSUES IN DIGITAL BUSINESS ENVIRONMENT

Internet only became the platform, at the early ages of its emergence, to search information and to communicate by each other. But now, it has been commercialized and almost all trading and business activities including banking can be done online. This trend gives a lot of benefits both to consumers and business organizations. However, the bad side of web based business also cannot be ignored. The security and privacy issues in web based business have to be seriously analysed and these issues engross the irresponsible parties who always give intimidation and threats to consumers as well as business organization. However, the security and privacy issues in web based business are analysed and interpreted one by one hereunder.

a. PRIVACY INCURSION

Privacy incursion issue is related to customer. The privacy incursion occur when the personal information belong to customers are exposed to the unauthorized party. It may occur in three ways.

- ✓ Web based business buys information about individuals such as their personal details, shopping habits and web page visitation listings. This can be done with or without the knowledge of individuals by using diverse computing technologies. A huge number of web pages/ web sites that require users to create name of members, also ask for personal details. These details are often sold to companies to support in the marketing and selling of their products and services.
- ✓ Consumers' personal information of being transmit may be intercepted by anyone other than the person whom it is intended. Protecting the communication privacy is a great problem and challenge, by reason of the nature of the online medium and the open network of digital telecommunications. It is technically and economically impossible to patch all the cracks through which unauthorized intruders may get access.

- ✓ The Malicious programs delivered through web pages could reveal debit card or credit card numbers, online transaction usernames and passwords that are recurrently stored in special files called cookies. Internet is stateless and cannot memorize a response from one web page view to another. Cookies help to solve the problem of remembering customer order information, usernames or passwords.

b. UNAWARE OF ONLINE BUSINESS TRANSACTIONS

Web based business has made an organization to run their business more efficient where the customers can get their products just in time. Through online shopping like by using extranet, the suppliers are capable to access to the database of organizations when they want to receive what they have ordered and that enable them to make the products and services available to a particular company without delay. Moreover, with the collaboration and cooperation from suppliers or sellers, a company can send their products to the clients' residence on the time. But, there are still some of the customers who are unaware on how online transaction takes place. Some of the customers have the perception of buying things in shops is much more faster and easier than buying through online shops as they can be handed over the products immediately where they thought that purchasing through online might have to wait for another days in order to arrived to the products to their house residence.

c. CYBER-SQUATTING

Cyber-squatting is an activity which a person or firm register, purchase and uses the existing domain name belongs to the well-known organization for the purpose of contravening its trademarks. These types of person or firm are usually called cyber-squatters they infringed the trademarks to extort the payment from original owner of the trademark. The extortion of payment happens when they offer the prices far bigger than they had purchased. Some of the cyber-squatters put up derogatory remarks about the person, firm or company which the domain is meant to represent in an attempt to encourage the subject to repurchase their domain.

d. WEB SPOOFING

Web spoofing is an electronic deception relates to the online transactions. This is happening when the attacker sets up a fake website which almost same with the original website in order to entice customers to give their debit/ credit card number or other personal information. Users might find themselves in a situation where they do not become aware of they are using a bogus web-site and give their debit/ credit card details or other information.

e. ONLINE PIRACY

The online piracy can be defined as unlawful copyright of electronic intellectual property such as videos, music or e-books. This unethical and illegal activity occurs when the users of Internet use the software and hardware technology in an illegitimate manner to transport the electronic intellectual property over the Internet. Software that is available for free of charge on the Internet permit the transfer of music and videos without the authorization.

f. EMAIL SPAMMING

Email spamming, also known as unsolicited commercial e-mail (UCE) involves sending or broadcasting of unwanted advertisement, correspondence or messages over the Internet. The individual who spam their e-mail usually called spammer. Many spammers broadcast their e-mail for the purpose to get financial information of individuals such as credit card or bank account numbers in order to deceive them. The content of spam emails often directs the consumers to the fake website or web pages in order to lure them to type their personal information such as debit/ credit card or bank account details. This technique is called phishing.

g. OUTDATED LAW AND REGULATION

Internet and websites facilitate people to discover new opportunities in running their business but at the same time, criminals have found their innovative ways to crime others. Criminals nowadays tend to make use of cyberspace for crimes and wrong doings. There are numerous factors that are recognized to be the probable factor in the growth of crimes where one of such factors is outdated law and regulation. Technologies are changing repeatedly and the changes of new technology is highly advanced and faster enough till the criminal laws of various jurisdiction have not caught up with the challenge of new technologies. Some countries may have address the threat and some of these laws are already in need of amendment to address the new kinds of cyber-crimes, but there are still many countries from developing and less developed areas are under the condition of not seeing cyber crimes as an vital issue that must be addressed and there are only diverse countries that have attempted to tackle the issue of prosecuting cyber-crimes committed from another jurisdiction by criminals.

B. MAJOR THREATS IN WEB BASED BUSINESS

Web Based Business Security also has some main issues. They are interception of data, redirection of data, identification of parties, exploitable program errors, and being the weakest point in security. When administrating a secure Web Based Business site, it is important to remember that you are part of a link of systems. If the security is weak, it may be possible that are allowing criminals access to information they may not have had access. This leads to ethical problems and issues where weak security on system led to awful consequences for other people or companies.

The Threats Posed to web based business servers online shopping tends to be at a higher echelon for risk and attacks. Because web based business is the transaction of goods and services and the payment for those goods and services are over the Internet. Therefore, the physical place where all of these transactions occur is at the Server level. The server is

considered as the central repository for "Web Based Business Place of Business" consists of the actual website which displays the products and services, customer database, and payment mechanism. Any attacks to this server could lose everything. Threats to Web Based Business servers fall into two general categories i.e. Threats from an actual attackers and secondly technological malfunction. In terms of the former the motivation and enthusiasm is primarily psychological. The intent is to gather personal information from people for the purpose of exploitation such as obtaining Debit Card, Credit Card and Bank Account information, Phishing schemes, obtaining usernames and passwords, etc. with the latter, anything related to the Internet can grounds problems. This can be everything from a network system not configured properly to data packets being lost, especially in a wireless access environment. Even poorly written programming code upon which your Web Based Business site was developed can be very susceptible to threats. Most Web Based Business Servers utilize Windows Operating systems and a Web Server Software to host the Web Based Business Site such as Internet Information Services (IIS) and a database which contains customer information and transaction history.

These platforms had a variety of security flaws linked with them, which has made them wide open to issues, threats and attacks. Consequently, there have been various moves in the business community to adopt more robust and protected platforms. The direct threats to Web Based Digital Business servers can be classified as: a) Malicious Code Threats; and b) Transmission Threats. With the former, spiteful, malicious or rogue programming code is set up into the server in order to gain access to the system resources. Very often, the intent of Malicious Code Attacks is to cause large scale damage to the Web Based Business server. With the latter, the threats and risks can be classified as either as active or passive. With passive threats, the main objective is to listen or eavesdrop to transmissions to the server. With active threats, the objective is to alter the flow of data transmission or to create a rogue transmission meant directly at the Web Based Digital Business server.

a. MALICIOUS CODE ATTACKS

VIRUSES AND WORMS

The most common threats and issues under this kind are the worms and viruses. A virus needs a congregation of some sort in order to cause damage to the system. The accurate definition is "a virus attaches itself to executable code and is executed when the software program begins to run or an infected file is opened." For example, a virus needs a file in which to attach itself to and when that file is opened, the virus can then cause the damage. This type of damage can range from the deletion of some files to the total reformatting of the hard drive or disk. The important thing to remember about viruses is that they cannot by themselves spread but they require a host file.

However, worms are very much different. A worm does not need a multitude or host to duplicate. Rather the worm replicates itself through the Internet, and can literally infect millions of computers on a global basis in just a matter of hours. Worms by themselves do not cause damage to a computer system like a virus does. But worms can shut down parts of the Internet or Web Based Business servers, because they can use up most valuable resources and database of the Internet, and the memory and processing power of servers and other computers.

TROJAN HORSES

A Trojan horse is a part of a set of programming code that is layered behind another program, and can execute covert, malicious functions. For example, Web Based Business server can display a cool-looking screen saver, but behind that could be a part of hidden code, cause for damage to the system. In order to get a Trojan horse attack is by downloading software and applications from the Internet. This is where you need to be very careful. There will be times, it could be often, that patches and other software code fixes will need to be downloaded and applied onto Web Based Business server. Make sure that whatever software is downloaded comes from a genuine, authentic and verified source, and that all the defense mechanisms are activated on the server

LOGIC BOMBS

A Logic Bomb is a description of a Trojan horse however it is event of time specific. For example, a logic bomb will release malicious or rogue code in a Web Based Business server after some particular time has over and done or a particular event in application or processing has occurred.

b. TRANSMISSION THREATS

DENIAL OF SERVICE ATTACKS

With a Denial of Service Attack, the main intention is to deny your customers the services provided on your Web Based Business server. There is no actual intent to cause damage to files or to the system, but the goal is to literally shut the server down. This happens when a huge amount of invalid data is transported to the server. Because the server can handle and process so much information at any given point of time, it is not capable to keep with the information and statistics overflow. As a result, the server becomes perplexed, and subsequently shuts down.

PING OF DEATH

When we surf the Web, or send E-Mail, the communications between our computer and the server takes place via the data packet. It is the data packet that contains the data and information and the request for information so as to send from one computer to other computers over the Internet. The communication protocol which is used to oversee the flow of data packets is called Transmission Control Protocol/Internet Protocol or TCP/IP for short. The TCP/ Internet protocol (IP) allows for data packets to be as large as 65,535 bytes. However, the data packet dimension that is transmitted across the Internet is about 1,500 bytes. With a Ping of Death Attack, a substantial data packet is sent i.e.

65,536 bytes. As a result, the memory buffers of the Web Based Business Server are totally overloaded, thus causing it to crash.

SYN FLOODING

When it opens up a Web Browser and type in a Web address, or click "Send" to transmit that E-Mail from the client computer, a set of messages is exchanged between the server and the client computer. These set of interactions is what establishes the Internet connection from the customer or client computer to the server, and vice versa. This is also known as a "handshake." To initiate this Internet connection, a SYN (synchronization) message is sent from the customer or client computer to the server, and the server replies back to the client computer with a SYN ACK (synchronization acknowledgement) message. To complete the Internet connection, the client or customer computer sends back an ACK (acknowledgement) message to the server. At this point, since the Web Based Business server is waiting to receive the synchronization acknowledgement message from the client. Computer, this is considered to be a half-open connection. It is at this point in which the Web Based Business server becomes vulnerable to attacks. Counterfeit messages, which appear to be lawful, could be sent to the Web Based Business server, thus overloading its memory and processing power, and causing it to crash.

IX. RECOMMENDATIONS

A. CONFIDENCE OF TRUST

In order to solve the major problem of trusting in Web Based Business, a large amount of trust will be very important to prove to the users that the certain website which the customers and users are accessing are trust worthy. The trust makes a website in a superior condition and all the users who are using it will feel comfortable dealing any type of business with them. As the issue of trust occurs in everything in the internet and Online shopping, it is very important that the value of trust is big and it is able to gain the trust and the loyal and faithfulness of the users and making certain that they stay loyal to the particular website. This trust can be achieved by taking few steps which can help gain this trust. The steps are making certain that all private data about the user are kept safe, well maintained and kept up dated. By doing this we can prevent and protect the lack of trust a user puts towards the particular website. When we have enough conviction amongst the users, an E-Biz website can execute well and at full speed and ensure that all the information are kept safe and making sure that no hackers go through the website and steal users information.

B. UPDATING THE LAW & REGULATION

Cyber crime is a serious issue and hackers are the real threats to web based business transactions. All this threats can give severe break down on Web Based Business websites if proper care is not given. Sometimes users may think that the law and regulation in the internet are lousy. We have to prove them wrong by giving updated law and regulations which will help keep Web Based Business transactions safe and secure. Laws and Regulation are very important to prevent the users to miss use their main concern and their freedom and to not do useless things such as hacking to account of others and getting away with it. Frauds in Web Based Business can be punished and jailed if all this laws & regulation are kept well and updated regularly and repeatedly. These laws must be strict and the people who regulating the laws should be honest and punish all who misuse the system. Any misuse and misconduct of the system have to pay the penalty.

C. DEGREE OF CONFIDENTIALITY

Making sure that degree of confidential is reached Organizations have to keep secured of clients' personal information and stored in a method that it is unable to be accessed by other unauthorized users. In order to build the confidence of users, the system has to be secured and tight so that no bugs or viruses could enter the website or the transaction system. This prevention of this system can enlarge the safety and can ensure the safety of the users using the system and this confidentiality is essential because of the fear towards forgery and hacking. Confidential are privacy of data and safety of an individual's property and assets. In E-Biz, hackers always are on the wait for any loophole to enter the system and hack information about the user's confidential folders. In these folders, there may be a lot of important information which can be useful and harmful to others. By using this powerful system, hackers will find it difficult to hack the system, and due to these users will have more confident on the E-Biz website and they will certainly cash in their money and deal their businesses thru the internet.

D. MAKE AWARE HOW WEB BASED BUSINESS OPERATIONS WORK

The issue of being unaware of not knowing about how online transaction works can lead to a lot of issues as stated above. This problem is a threat to users who don't seem to understand that their money can be blacked out if hackers hacks their account. To prevent this problem, the Web Based Business has to make sure that they have enhanced versions of security and good transaction system for the users to cash in their money. By making this transaction system secure, we can no longer be afraid of hackers. In the mean time, Web Based Business needs to teach the users about the online transaction system. By teaching them how the system functions, users can learn and they too can be aware of the system's processes. All this learning will alert the users to be more caution on their online transaction. Web Based Business websites with online transaction systems should list down all the possibilities of doing online transaction and all the misuses possible.

X. CONCLUSION

The concepts and theories on Web Based Business trust and security can guide the managers and companies to develop

ISSN: 2394-4404

their own unique customer retention strategies. While developing trust between companies and customers in Web Based Business, managers should understand that different service qualities might lead to different level of customer buying behavior and customer retention. The security systems are strongly needed to handle the process of developing the customer retention strategies in Web Based Business transaction process in an attempt to capture the relationship within organization and with the customers. The benefits of applying trust and build up security in online shopping is quite obvious. To develop a better relationship between customers and online shopping, there are certain steps that could be considered for future preferences such as the attitudes of employees towards the customers, the usage of technologies in developing security in Web Based Business transaction, and protect customers during business transactions. Researchers have caused executives to think on what do exactly customers want? And it was concluded that companies have to find best solutions in improving service quality and develop trust in relation between Web Based Business and customers.

REFERENCES

[1] Suh, B and Han I., 2003, The Impact of Customer Trust and Perception of Security Control on the Acceptance of Web based business, International Journal of Web based business, Vol 7, No. 3, pp. 135-161

[2] Gehling, B. & Stankard, D. 2005 „ eCommerce Security" in Information Security Curriculum Development Conference, September 23-24 2005 pp32-38,

[3] Alan, D. S. and William, T. R., 2002, "E-Lending: Foundations of financial and consumer marketing in an information intensive society," Journal of online shopping and Information Technology, Vol. 3, No. 1, pp. 5-19.

[4] Mukherjee, A. and Nath, P., 2007, "Role of electronic trust in online retailing: A re-examination of the commitment-trust theory," European Journal of Marketing, Vol. 41, No. 9/10, pp. 1173-1202.

[5] Salo, J. and Karjaluoto, H., 2007, "A conceptual model of trust in the online environment," Online Information Review, Vol. 31, No. 5, pp. 604-621.

[6] Shalhoub, Z. K., 2006, "Trust, privacy, and security in electronic business: The case of the GCC countries," Information Management and Computer Security, Vol. 14, No. 3, pp. 270-283.

[7] So, W. C. and Sculli, D., 2002, "The role of trust, quality, value and risk in conducting online shopping," Industrial Management and Data Systems, Vol. 102, No. 9, pp. 503-512.

[8] Srinivasan, S., 2004, "Role of trust in online shopping success," Information Management and Computer Security, Vol. 12, No. 1, pp. 66-72.

[9] Vasilis, K., 2006, "Dealing with internet risk," Journal of Internet Security, Vol. 3, No. 1, pp. 1-4.

[10] Internet World Stats: http://www.internetworldstats.com/stats.htm

[11] Niranjanamurthy M and Dharmendra Chahar (2013) *E-Commerce Security Issues and Solutions*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7