Journal of Engineering and Applied Sciences 13 (13): 4939-4948, 2018
ISSN: 1816-949X

Internet of Things-Security and Trust in e-Business

[1]Ali Shawket Thiab, [1]Zeratul Izzah Mohd. Yusoh and [2]Abdul Samad Bin Shibghatullah
[1]Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia, Melaka, Malaysia
[2]Faculty of Business and Information Science (FoBIS), UCSI University,
Kuala Lumpur (SouthWing), Malaysia

Abstract: 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. Success of an e-Commerce rests on many factors. e-Commerce is widely considered the buying and selling of products over the internet but any transaction that is completed solely through electronic measures can be considered e-Commerce. e-Commerce is subdivided into three categories: Business to Business or B2B (Cisco), Business to Consumer or B2C (Amazon) and Consumer to Consumer or C2C (eBay) also called electronic commerce. One of the important contributors is trust. Trust is something that an e-Commerce must strive to achieve over a period of time. Acquiring customer trust depends on many things that an e-commerce controls. However, customer's trust as such is not under the control of the e-Commerce. Then e-Commerce security is viewed as an engineering management problem and a life cycle approach is put forward. How the e-Commerce systems can be made secure using the life cycle approach is outlined.

Key words: e-Commerce security, security issues, internet consumers, trust, categories, electronic measures

INTRODUCTION

Nowadays as people are gradually aware of the contributions that reverse logistics has made to environment and economy; Enterprises are paying more attention to the promotion of reverse logistics. However, reverse logistics is different from forward logistics: the difficulties in application have aroused wide attention. The reason that leads to the delay in application of reverse logistics is heatedly debated and the academy field holds different views about it but it is an acknowledged fact that collecting reverse logistics information in difficult. The reason is that reverse logistics involves uncertainty of all attributes in products and this demands diverse reverse logistics processes. If we ignore the uncertainty and use the same process to treat all products, then we will waste many recyclable, valuable products, thus, reducing the profits created by reverse logistics in a large scale. To make up for it, we need to know the information of different products in the whole close-loop supply chain promptly and accurately. After Daugherty and Jalal Ashayeri confirmed that information system and reverse logistics performance was positively correlated through empirical study in 2002 and 2005, relevant research is more than active (Ashayeri and Tuzkaya, 2011; Daugherty *et al*., 2005). Thus, in implementing reverse logistics, we must absorb reverse management information system that can both record product life cycles vertically and record product attributes horizontally, helping enterprises improve decision management and efficiency of business operations.

During the last decade, Internet of Things (IoT) approached our lives silently and gradually, thanks to the availability of wireless communication systems (e.g., RFID, WiFi, 4G, IEEE 802.15.x) which have been increasingly employed as technology driver for crucial smart monitoring and control applications (Atzori *et al*., 2010; Miorandi *et al*., 2012; Palattella *et al*., 2013). Nowadays, the concept of IoT is many-folded, it embraces many different technologies, services and standards and it is widely perceived as the angular stone of the ICT market in the next 10 years at least (Emmerson, 2010; Hersent *et al*., 2011).

Internet of Things (IoT) also known as internet of objects connects billions of objects which include buildings, air conditioners, coffee machines washers, cars, air planes, animals and people as well. According to Cisco the IoT connects things and people on an unprecedented scale; Cisco predicts that, although, so far in 2015 more than 99% of things in the physical world are not

Corresponding Author: Ali Shawket Thiab, Department of Computer Sciences, University of Technology, Baghdad, Iraq

connected by 2020 the number of internet connected devices and objects will reach 50 billion. With the mixing of physical world and information world together. The future technology can be predicted that the communication is not going to be people communicating to people; It's not going to be people accessing information. It's going to be all about using machines to talk to other machines on their behalf. We are moving towards a new era of ubiquity in terms of technology, we are entering the internet of things era in which new forms of communication among human and things and between things themselves will be recognized (Tan and Wang, 2010).

One of the biggest breakthroughs of the internet of things is transforming the physical world and information world together. Sensors play a very vital role in bridging the gap between the physical world and information world. Sensors collect data from their environment, generating information and raising awareness about context. So that, the change of their environment can be monitored at a glance and the corresponding things can make some responses when needed (Conner, 2010). According to Stankovic (2014) if our vision is correct regarding the future technology, many IoT applications will be based on a deployed sensing, actuation and communication platform (connecting a network of things). In these deployments, it is common for the devices to know their locations have synchronized clocks, know their neighbour devices when cooperating and have a coherent set of parameter settings such as consistent sleep/wake-up schedules, planned power levels for communication and pair-wise security keys (Stankovic, 2014).

From a logical viewpoint an IoT system can be depicted as a collection of smart devices that interact on a collaborative basis to fulfil a common goal. At the technological floor, IoT deployments may adopt different processing and communication architectures, technologies and design methodologies, based on their target. For instance, the same IoT system could leverage the capabilities of a Wireless Sensor Network (WSN) that collects the environmental information in a given area and a set of smartphones on top of which monitoring applications run. In the middle, a standardized or proprietary middleware could be employed to ease the access to virtualized resources and services. The middleware in turn, might be implemented using cloud technologies, centralized overlays or peer to peer systems (Grieco *et al*., 2014).

Of course, this high level of heterogeneity, coupled to the wide scale of IoT systems is expected to magnify security threats of the current internet which is being increasingly used to let interact humans, machines and robots in any combination. More in details, traditional security countermeasures and privacy enforcement cannot be directly applied to IoT technologies due to their limited computing power, moreover, the high number of interconnected devices arises scalability issues. At the same time, to reach a full acceptance by users it is mandatory to de ne valid security, privacy and trust models suitable for the IoT application context (Roman *et al*., 2013; Anderson and Rainie, 2014). With reference to security, data anonymity, confidentiality and integrity need to be guaranteed as well as authentication and authorization mechanisms in order to prevent unauthorized users (i.e., humans and devices) to access the system. Whereas concerning privacy requirement, both data protection and users personal information confidentiality have to be ensured, since, devices may manage sensitive information (e.g., user habits). Finally, trust is a fundamental issue since, the IoT environment is characterized by different devices which have to process and handle the data in compliance with user needs and rights.

Advantages of e-Commerce: The advantages of e-Commerce for business entities can be summarized thus, e-Commerce can increase sales and decrease costs. A firm can use e-Commerce to reach narrow market segments that are widely scattered geographically. The internet and the web are particularly useful in creating virtual communities that become ideal target markets. A virtual community is a gathering of people who share a common interest but instead of this gathering occurring in the physical world, it takes place on the internet. Just as e-Commerce increases sales opportunities for the seller, it increases purchasing opportunities for the buyer. Businesses can use e-Commerce in their purchasing processes to identify new suppliers and business partners. Negotiating price and delivery terms is easier in e-Commerce becausen the web can provide competitive bid information very efficiently (Shelanski, 2013).

e-Commerce increases the speed and accuracy with which businesses can exchange information which reduces costs on both sides of transactions. e-Commerce provides buyers with a wider range of choices than traditional commerce because they can consider many different products and services from a wider variety of sellers. The benefits of e-Commerce also extend to the general welfare of society. Electronic payments of tax refunds, public retirement and welfare support cost less to issue and arrive securely and quickly when transmitted via. the Internet. Furthermore, electronic payments can be

easier to audit and monitor than payments made by check which can help protect against fraud and theft losses. e-Commerce can make products and services available in remote areas. For example, distance education is making it possible for people to learn skills and earn degrees no matter where they live or what hours of the day they have available for study.

Disadvantages of e-Commerce: e-Commerce also has its disadvantages. It is difficult to conduct a few businesses electronically. For example, perishable foods and high-cost items such as jewellery or antiques may be impossible to adequately inspect from a remote location, regardless of the technologies that are devised in the future. However, most of the disadvantages of e-Commerce today are due to the newness and rapidly developing pace of the underlying technologies. Return on investment numbers is difficult to compute for investments in e-Commerce because the costs and benefits are hard to quantify. Costs which are a function of technology, can change dramatically during even short-lived e-Commerce implementation projects because the underlying technologies change rapidly (Costa, 2016).

In addition to technology issues, many businesses face cultural and legal impediments to e-Commerce. Some consumers are still somewhat fearful of sending their credit card numbers over the Internet. The legal environment in which e-Commerce is conducted is full of unclear and conflicting laws. In many cases, government regulators have not kept up with technologies. As more businesses and individuals find the benefits of e-Commerce compelling, many of these technology and culture-related disadvantages will disappear. Another important issue is security. Transactions between buyers and sellers in e-Commerce include requests for 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 where they are exchanged over the internet. The interception of transactions and in particular credit card details, during transmission over the internet is often a major obstacle to public confidence in e-Commerce.

MATERIALS AND METHODS

Security threats to e-Commerce: e-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the "Commerce chain", the assets that must be protected to ensure secure e-Commerce include client computers, the messages travelling on the communication channel and the web and commerce servers including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-Commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.

Client threats: Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the widespread use of active content has changed this perception (Bossomaier and Hope, 2015).

Active content: Active content refers to programs that reembedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio or implement web-based spread sheet programs (Kadhim and Al-Taie, 2013). Active content is used in e-Commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount including sales tax, handling and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript and VBScript. Since, active content modules are embedded in web pages, they can be completely transparent to anyone browsing a page containing them. Anyone can embed malicious active content in web pages. This delivery technique, called a trojan horse, immediately begins executing and taking actions that cause harm. Embedding active content to web pages involved in e-Commerce introduces several security risks. Malicious programs delivered quietly via web pages could reveal credit card numbers, usernames and passwords that are frequently stored in special files called cookies. Because the internet is stateless and cannot remember a response from one web page view to another, cookies help solve the problem of remembering customer order information or usernames or passwords. Malicious active content delivered by means of cookies can reveal the contents of client-side files or even destroy files stored on client computers.

Malicious codes: Computer viruses, worms and trojan horses are examples of malicious code. A trojan horse is a program which performs a useful function but performs an unexpected action as well. Virus is a code segment

which replicates by attaching copies to existing executable. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side (Nieles *et al*., 2017).

Server-side masquerading: Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient but merely accesses it) but it is usually an active attack (Sharma and Misra, 2014).

Communication channel threats: The internet serves as the electronic chain linking a consumer (client) to an e-Commerce resource (commerce server). Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure and non-hostile.

Confidentiality threats: Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs onto a website, say www.anybiz.com, that contains a form with text boxes for name, address and e-Mail address. When one fills out those text boxes and clicks the submit button, the information is sent to the web-server for processing. One popular method of transmitting data to a web-server is to collect the text box responses and place them at the end of the target server's URL. The captured data and the HTTP request to send the data to the server is then sent. Now, suppose the user changes his mind, decides not to wait for a response from the anybiz.com server and jumps to another website instead, say www.somecompany.com. The server somecompany.com may choose to collect web demographics and log the URL from which the user just came (www.anybiz.com). By doing this, somecompany.com has breached confidentiality by recording the secret information the user has just entered (Geistfeld, 2016).

Integrity threats: An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing, pretending to be someone you are not or representing a website as an original when it really is a fake was one means of creating havoc on websites. Using a security hole in a Domain Name Server (DNS), perpetrators can substitute the address of their website in place of the real one to spoof website visitors. Integrity threats can alter vital financial, medical or military information. It can have very serious consequences for businesses and people (Voeller, 2014).

Availability threats: The purpose of availability threats, also known as delay or denial threats is to disrupt normal computer processing or to deny processing entirely. For example if the processing speed of a single ATM machine transaction slows from one or 2-30 sec, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitor's web or commerce sites (Loukas, 2015).

Server threats: The server is the third link in the client-internet-server trio embodying the e-Commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

Web-server threats: Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes, security weaknesses that provide openings through which evildoers can enter (Gillman *et al*., 2015).

Commerce server threats: The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite including an FTP server, a mail server, a remote login server and operating systems on host machines. Each of this software can have security holes and bugs (Ansari, 2015).

Database threats: e-Commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were disclosed or altered. Some

databases store username/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information (Sharma and Misra, 2014).

Identification of trust: The phase of electronic payment (e-Payment) is confidential when all phases of the process are capable to satisfy the needs of participants and their security expectations. A fundamental prerequisite must be that all participants ought to have absolute trust in the system that they participate. The contraction of trust in an electronic payment system must take into consideration: data, identities and role behaviour. The adoption of e-Commerce must consider trust and risk as important determinants of adoption behaviour. Trust has been defined as ''The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor irrespective of the ability to monitor or control that other party'' (Mayer *et al*., 1995). Trust requires a party to make a rational decision based on knowledge of possible rewards for trusting and not trusting. Trust enables higher gains while distrust avoids potential loss. ''Generally an entity can be said to ''Trust'' a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects'' (Tsiakis and Sthephanides, 2005). The purpose of modelling trust is to establish a secure way to describe the decision of commerce process. A trusted environment is characterized by:

- The fact that all entities are uniquely identifiable
- That there is a minimum number of a priori trusted entities and
- That these entities have unquestionable trust to other participating entities

To design for trust, it is necessary to determine if and under what conditions trust mechanisms are brittle. Security architecture presumes that a trust model defines the trusted relationships between all involved components. Trust services are operated by sovereign organizations that are designed to protect consumers. Merchants concede to the organization's trust standards (these standards cover areas such as privacy of personal information, return policies and security policies, etc.) in order to bind to legal obligations. Trust and trustworthiness are fundamental for every security solution. The needs for these trust aspects and the means that are used to implement it, affect the security mechanism of any commercial system. But we must distinct trust form trustworthiness. Trust is an act of a trustor in which an entity places trust in some object (trust emanates from the entity). In contrast, trustworthiness is a characteristic of someone or something that is the object of trust. Trust is the enabling of confidence that something will or will not occur in a predictable or promised manner. The enabling of confidence is supported by identification, authentication, accountability, authorization and availability (Andert *et al*., 2002).

Electronic payment (e-Payment) phase: Electronic payments have been reported to be the ultimate test of security and trust in e-Business environment. The notion of payment is an inborn part in any commercial transaction. The electronic payment (e-Payment) systems do two things in particular emulate existing payment frameworks from the real world or schematize new ways to execute payment transactions. Adoption of payment mechanisms and electronic money as other forms of payment depends upon trust in the security and reliability of the system and control of the particular transaction. The electronic transaction process takes place via the internet between three participants:

- Client e every user of the internet (client) can be considered as a potential customer. It is therefore imperative to establish mechanisms, to certificate trust and security
- Merchant e the typical merchant is the entity that needs to sell his goods (products or services) to the clients. In order to achieve this it has to secure transaction processes, so that, all participants are willing to act in a transactio
- Bank e the action of bank is familiar of every financial organization to validate and authorize transactions

In a commercial context, a payment process involves a payer, a merchant and a bank. In general, the entities transacting in a payment system are appointed by the specific commercial relationship which by itself may depend on series of conditions.

Literature review: Alan and William (Smith and Rupp, 2003) have stated that one of the most important issues in e-Lending is security. In the study, there was a statement from Richard Biell of Tower Group: "It's one thing to submit a credit card number online to buy a product. It's quite another thing to put your entire personal dossier online and hope that no one intercepts it, particularly if you're not familiar with the lender". It stated that a borrower will not proceed to exchanging personal

information without a sufficient level of confidence and the impact is the customers will not peruse other products and services without being familiar with the vendor and the process. In order to improve the trust among the customers, the suggestions given are keeping the customers informed through web presences and shared database where the study was not included.

Mukherjee and Nath (2007) stated that trust and commitment are the central tenets in building successful long-term relationships in the online retailing context. This study aims to re-examine the Commitment-Trust Theory (CTT) of relationship marketing in the online retailing context. The electronic hypermedia environment posed new challenges for relationship retailing where it is in the interest of retailers to establish and maintain long-term bonds with customers. This new marketing medium and channel is now an integral part of the multi-channel strategy for most retailers. The limitation the study has not discovered is fraud may increase, since, customers might not received the goods they had ordered and sometimes the goods are not reached to the customers.

Eben (2003) presented and reviewed the impact of information security for e-Business with emphasize on the security threats and potential losses that could arise from those vulnerabilities. e-Business security is analyzed as consisting of 6 dimensions: confidentiality, integrity, availability, legitimate use, auditing and non-repudiation. This study has proposed that designing a comprehensive and systematic security policy is a need for implementing e-Business security. The main thesis of this study was that e-Business security can only be effective if it is regarded as part of an overall corporate information security risk management policy. The resarchar proposed a six-stage security management strategy in this study. The limitations of this study are that implementing the framework were lack of building blocks in place and it was very costly for a company to developing software regarding to the increasing of the security.

Winch and Joyce (2006) mentioned that the dynamic nature in building and losing trust in Business to Consumer (B2C) e-Business in an effort to better understand the casual nature of trust. The purpose of this study is not to present yet another model but to suggest how to move from the information and knowledge those models provide into a better understanding of the problem of trust in B2C. Past models are largely descriptive and static in nature. This research helps to give a new understanding of trust building and maintenance as a dynamic process within what is in significant part, a closed-loop system. The study has therefore, taken the stock-flow diagramming approach from business dynamics modeling to reflect the structure of the trust building systems. This emphasized that the management of system levels such as trust has to be through the control of the in and outflows if a company needs to build trust it has to work through the flows resulting from consumer's beliefs about how and whether problems might arise. The limitations of this study are that it did not mention that how can they reduce actual risks in the company and its process and in e-Transactions itself and how can they ensure perceived risks close to reality.

Hagi (2005) discovered that e-Business applications provide critical linkage between customers, suppliers and partners. Enterprises today have realized that their success will necessitate considerable attention to the security and privacy of their application software and particularly their e-Business applications. Vulnerabilities and threats related to e-Business application programs can be seen as occurring at all the different levels of the application system. All of these vulnerabilities and threats result in loss of confidentiality, integrity and authenticity. This study highlighted the methods and recommendations that can be utilized by organizations working through the complex maze of application security. This study has discovered that it is necessary to create security culture where employees, contractors and partners are educated on security policies, specific processes why security is important and what behavior is expected from them through training. The limitation of this study is that lack of explanation and discussion about how costly the training is since, it requires a number of experts and other resources in conducting training. Only the large corporations with sufficient resources are able to do that. Furthermore, it is hardly to ensure that their business partners will send their employees to go for training, since, it involved a large amount of cost.

Davidson (2001) proposed that having business on the internet offers potentially opportunities for increasing efficiency and reducing costs but it also offers unlimited risks. The much greater access to data will attract hackers and criminals. The resarchar identified the importance of business security will bring benefits to e-Business. The examples of security systems are virtual private database which provides a set of tools to enforce fine-gained access control within the database and oracle label security which is useful for hosting environments in which access to information can be formalized. The limitation of this article is that resarchar has not explained details about the impact of security in e-Business.

So and Sculli (2002) stated that in relation to trust and internet technologies, consumers are concern about the privacy and security. Trust must exist at all levels for the maintenance of cooperation, fundamental for any exchange and most routine of everyday interaction.

Nowadays, in uncertain and uncontrollable future, trust has become an important factor in needed in buyer-seller relationship in order to facilitate the transactions. Besides that trust is a critical factor in business is not enough, company must also build customer's trust because customers will attempt to evaluate supplier's trustworthiness before committing to business transactions. It's included appearance, performance and reputation. Combination all of these factors, e-Business will able to gain the higher return and customers will have satisfaction during a business transaction. The limitation of this study is that it did not state about the problems may occur when applying trust in business transactions.

Lord *et al.* (2002) discussed that e-Business is essential to reduce cost resulting from less overhead, greater economies of scales and increased of efficiency. The resarchars examined that the internet provides greater access to data, not only to legitimate users but also to hackers, disgruntled employees, criminals and corporate spies. But making business information accessible via. the internet increases the number of users who may be able to access the information. The internet creates challenges in terms of scalability of security mechanisms, management of those mechanisms and the need to make them standard and interoperable. It is essential to have security for e-Business but one of the limitations the resarchars did not focused is it needs highly cost to develop and maintain it. Besides, it is costly to hire an expert to develop and manage it especially if the company is only a small or medium enterprise.

Srinivasan (2004) stated that success of an e-Business rests on many factors. He defined trust is something that an e-Business must strive to achieve over a period of time. The resarchar suggested some contributing factors for gaining customer trust are: appeal of the Web site, product or service offerings, branding, quality of service and trusted seals. Trust can be viewed from many angles such as transaction, information content, product, technology and institution. This study analyses the role of trust from the transaction perspective and highlights the things that an e-Business could do for building customer trust. Factors contributing to trust are not easy to measure. It is developed over time. People trust a business based on their own past experience as well as by third party recommendations. He concluded that the e-Businesses are accessible from anywhere at any time, there are additional impediments in building and maintaining trust. The limitation of this study is that it did not focus much on how a company can enhance the security when doing online commerce.

Velmurugan (2009) analyzed the attitude of both e-Business and perspective of e-Partners toward the risks which were born by using the Internet as the communication channel. The risks were highly correlated and shape the trust of an e-Customer towards an e-Business. Starting from the organization's attitude towards risks, a number of criteria that influence the customer's trust are discussed. He has mentioned in the criteria of the characteristics which influence and shape the trust of an organization that: "the older the site, the higher the trust". But the question is if the site has offered products or services where the customers have high desired to own even though it is still new, the trust and the security of the website might be the least criteria for the customers to gain advantage, especially if the product offered is cheap. The limitation of the study is that, it did not mention that the sites those are able to offer a very useful and advanced product can also easily gain the trust from the customers. Sometimes, people will think that the site which is able to offer good product, that particular site should not have much of critical security problems, since, it needs powerful security tool or software to prevent other companies from imitate their products.

RESULTS AND DISCUSSION

Lack of trust: It is known that e-Commerce has becoming one of the most important elements in running business successfully particularly for small business. Managers have realized on how e-Commerce can benefits their business and thus, many organizations have started their business online. Internet is becoming more and more powerful tools for a film to run their business as internet helps to connect the stakeholders from all over the world which has improved the efficiency of an organization. The customers who are buying their products online will face another risky problem on dealing with the vendors where the vendors cannot be observed and sometimes they are unknown. Besides, customers not only have to receive the products which are unacceptable in quality but they have to face the risks of not receiving the items they had ordered at all after they made their payment through online. Moreover, personal information and credit card numbers of customers might disclosed to other people during or after their online trades when the vendors are incapable to protect the customer's data. Due to the reason stated above, it in impossible for customers to do their online trades safely and because of those cases happened before, it caused the customers to lost their confident in buying through online and it does make customers lost their trust towards online trading.

Solution: To solve this major problem of trusting in e-Business, a large amount of trust will be very important to prove to the users that the certain website which the users are accessing are trust worthy. The trust makes a website in a good 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 e-Business, it is very important that the value of trust is big and it is able to gain the trust and the loyalty of the users and making sure 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 sure that all private data about the user are kept safe, well maintained and kept up-dated. By doing this, we can prevent the lack of trust a user's puts towards the particular website. When we have enough trust amongst the users, an e-Biz website can perform well and at full speed and makes sure that all the information are kept safe and making sure that no hackers go through the website and steal users information.

Unaware of how e-Business: Transactions take place e-Business has made an organization to run their business more efficient where the customers can get their products just in time. Through e-Business like by using extranet, the suppliers are able to access to an organization's database on when the wan to receive what they have ordered and that enable them to make the products available to the particular company just in time. Besides with the cooperation from supplier's a company can try to have their products sent to client's house on the time. But there are still some of the customers who are unaware on how e-Business transaction takes place. Some of the customers have the perception of buying things in shops is much more faster than buying through online as they can get the products immediately where they thought that buying through online might have to wait for another days in order to get the products arrived to their house. They do not realize that a close integration between the suppliers and the company can put the clients in the way that they still can receive their order on the time they want.

Solution: 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 e-Biz 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 meantime, e-Biz 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. e-Biz websites with online transaction systems should list down all the possibilities of doing online transaction and all the misuses possible.

Degree of confidentiality involves: There is uncountable of ways that an e-Business set up will be attacking by hackers, crackers and disgruntled insiders. These have immediately decreased the degree of confidentiality of clients towards e-Business. According to Eben (2003) confidentiality is defined as making information accessible to authorized users and prevents the access from unauthorized users towards information. The problem of degree of confidentiality is always taken place in health centre. The recent surveys reported by Georgetown University Institute for Health Care Research and Policy contain statistics regarding to the people's concern for the confidentiality, there were about 63% of internet "health seekers" and 60% of all internet users oppose the ideas of keeping medical records online, even with a secure, password protected site since they worried that other people will see the detail of their records. Majority of internet users are worried about others finding out about their online activities where 89% fear that internet companies might sell or give away and 85% fear that insurance companies might change their coverage after finding out what online information they accessed.

Solution: Organizations have to keep secured of client's personal information and stored in a way 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 this 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.

CONCLUSION

The development and improvement of technologies have brought successful towards e-Business. High technologies have attracted people misuse the technologies such as hackers and cybercrime which they can access to e-Business privacy easily. Thus, e-Business companies should build trust and using security during the business transaction. To provide value to the customers through service and goods provided, research found that companies should build up trust and security to protect their customers. Benefits of application trust and security include improved customer service, build customers trust, avoid the misuse of technologies, protect customer's privacy and maintain the companie's reputation. In order to create an effective infrastructure for securing e-Business, it requires a comprehensive development of several elements including laws, policies, industry self-regulation, technical standards and law enforcement. These elements may provide positive environment and infrastructure to support the growth of e-Business and relation with customers. Therefore, governments and businesses need to work together to improve consumer trust and security are attempt to increase transactional efficiency and effectiveness in all aspects of the design, production, marketing and sales of products or services for existing and developing good relation through the utilization of current and emerging electronic technologies which will gain the more confidence in e-Business. Additionally, the government itself needs to re-examine existing regulations to ensure protection for the e-Business.

REFERENCES

Anderson, J.Q. and H. Rainie, 2014. The internet of things will thrive by 2025. Pew Research Center, Washington, USA.

Andert, D., R. Wakefield and J. Weise, 2002. Trust modeling for security architecture development. Master Thesis, Stanford University, Stanford, California.

Ansari, J.A., 2015. Web Penetration Testing with Kali Linux. 2nd Edn., Packt Publishing, Birmingham, England, ISBN:9781783988525, Pages: 312.

Ashayeri, J. and G. Tuzkaya, 2011. Design of demand driven return supply chain for high-tech products. J. Ind. Eng. Manage., 4: 481-503.

Atzori, L., A. Iera and G. Morabito, 2010. The internet of things: A survey. Comput. Networks, 54: 2787-2805.

Bossomaier, T. and B.A. Hope, 2015. Online GIS and Spatial Metadata. 2nd Edn., CRC Press, Boca Raton, Florida, USA., ISBN:9781482220162, Pages: 414.

Conner, M., 2010. Sensors empower the internet of things. Electr. Des. News, 55: 32-37.

Costa, E.D., 2016. Global E-Commerce Strategies for Small Businesses. MIT Press, Cambridge, Massachusetts, USA., Pages: 198.

Daugherty, P.J., R.G. Richey, S.E. Genchev and H. Chen, 2005. Reverse logistics: Superior performance through focused resource commitments to information technology. Transp. Res. Part E. Logist. Rev., 41: 77-92.

Davidson, M.A., 2001. Database security for E-business. Oracle Corporation, Redwood City, California, USA.

Eben, O., 2003. A systematic approach to E-business security. Master Thesis, University of New Brunswick, Fredericton, Canada.

Emmerson, B., 2010. M2M: The internet of 50 billion devices. WinWin Mag., 1: 19-22.

Geistfeld, M.A., 2016. Protecting confidential information entrusted to others in business transactions: Data breaches, identity theft and tort liability. DePaul L. Rev., 66: 385-721.

Gillman, D., Y. Lin, B. Maggs and R.K. Sitaraman, 2015. Protecting websites from attack with secure delivery networks. Comput., 48: 26-34.

Grieco, L.A., M.B. Alaya, T. Monteil and K. Drira, 2014. Architecting information centric ETSI-M2M systems. Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), March 24-28, 2014, IEEE, Budapest, Hungary, ISBN: 978-1-4799-2737-1, pp: 211-214.

Hagi, S., 2005. Engineering E-business applications for security. IBM Canada Ltd, Ottawa, Canada,.

Hersent, O., D. Boswarthick and O. Elloumi, 2011. The Internet of Things: Key Applications and Protocols. John Wiley & Sons, Hoboken, New Jersey,.

Kadhim, A.M. and M.Z. Al-Taie, 2013. Factors disrupting a successful implementation of E-commerce in Iraq. J. Econ., 1: 1-14.

Lord, P., A. Mary and B. Kristy, 2002. Managing E-business security challenges. Oracle Corporation, Redwood City, California.

Loukas, G., 2015. Cyber-physical Attacks: A Growing Invisible Threat. Elsevier, Amsterdam, Netherlands, ISBN:9780128014639, Pages: 270.

Mayer, R.C., J.H. Davis and F.D. Schoorman, 1995. An integrative model of organizational trust. Acad. Manage. Rev., 20: 709-734.

Miorandi, D., S. Sicari, F. De Pellegrini and I. Chlamtac, 2012. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10: 1497-1516.

Mukherjee, A. and P. Nath, 2007. Role of electronic trust in online retailing: A re-examination of the commitment-trust theory. Eur. J. Market., 41: 1173-1202.

Nieles, M., K.L. Dempsey and V.Y. Pillitteri, 2017. An introduction to information security. MIT Thesis, National Institute of Science and Technology, Berhampur, India.

Palattella, M.R., N. Accettura, X. Vilajosana, T. Watteyne and L.A. Grieco *et al*., 2013. Standardized protocol stack for the internet of (important) things. IEEE. Commun. Surv. Tutorials, 15: 1389-1406.

Roman, R., J. Zhou and J. Lopez, 2013. On the features and challenges of security and privacy in distributed internet of things. Comput. Netw., 57: 2266-2279.

Sharma, A. and P. Misra, 2014. A security framework for E-business applications. Intl. J. Comput. Appl., 102: 30-34.

Shelanski, H.A., 2013. Information, innovation and competition policy for the internet. Univ. Pennsylvania Law Rev., 161: 1663-1705.

Smith, A.D. and W.T. Rupp, 2003. E-lending: Foundations of financial and consumer marketing in an information intensive society. J. E. Bus. Inf. Technol., 3: 5-19.

So, M.W. and D. Sculli, 2002. The role of trust, quality, value and risk in conducting e-Business. Ind. Manage. Data Syst.,102: 503-512.

Srinivasan, S., 2004. Role of trust in E-business success. Inf. Manage. Comput. Secur., 12: 66-72.

Stankovic, J.A., 2014. Research directions for the internet of things. IEEE. Internet Things J., 1: 3-9.

Tan, L. and N. Wang, 2010. Future internet: The internet of things. Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering, August 20-22, 2010, Chengdu, China, pp: V5-376-V5-380.

Tsiakis, T. and G. Sthephanides, 2005. The concept of security and trust in electronic payments. Comput. Secur., 24: 10-15.

Velmurugan, M.S., 2009. Security and trust in E-business: Problems and prospects. Intl. J. Electron. Bus. Manage., 7: 151-158.

Voeller, J.G., 2014. Cyber Security. John Wiley & Sons, Hoboken, New Jersey, USA.,.

Winch, G. and P. Joyce, 2006. Exploring the dynamics of building, and losing, consumer trust in B2C E-business. Intl. J. Retail Distrib. Manage., 34: 541-555.