International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 2; Issue 5; September 2017; Page No. 45-49

Study of major security challenges and solutions in ecommerce model

[1] Hiral D Patel, [2] Dr. Kamaljit I Lakhataria, [3] Dr. Pravin H Bhathawala
[1] Research Scholar, Calorx Teachers' University, Ahmedabad, Gujarat, India
[2] Professor, Gujarat University, Ahmedabad, Gujarat, India
[3] Professor, Calorx Teachers' University, Ahmedabad, Gujarat, India

Abstract
Internet age changes the business exchange style and conveys numerous business chances to the e-commerce. Ecommerce is characterizes as the purchasing and offering of item and service on the web. However, the security likewise turns into the most basic issues of ecommerce framework all ecommerce exercises dependably include client individual information and exchange data [7]. This enormous increment in the uptake of Ecommerce.
Has prompted another generation of related security dangers, in this paper we will concentrate on the most imperative security confronts that any E-Commerce framework needs [9]. However, any online business must have four essential necessities. in the first privacy security the information traded must be kept from unapproved gatherings, second Integrity the traded information must not be modified or messed with, third Authentication both sender and beneficiary must demonstrate their characters to each and fourth Non-revocation evidence is required that the traded data was for sure gotten. Additionally we will talk about e-commerce segment and security dangers and solution about e-business.

Keywords: DDOS, e-commerce, privacy, security threats, SSL

Introduction
The rapid evolution of online and mobile channels has carved out new markets and brought huge opportunities for emergent and established organizations alike. However, unfortunately the past decade has also witnessed significant disruption to ecommerce payment processes and systems [6]. The interconnected, anonymous and instantaneous nature of these channels has inevitably led to the development of malicious threats targeting ecommerce and retail services firms, their people and their customers. These e-crime and digital fraud threats continue to evolve rapidly, with attackers utilizing increasingly sophisticated techniques to target vulnerabilities in people, processes and technologies. The e-crime threats, if successfully realized, can undermine essential digital services, cause significant damage to brand reputations, and result in considerable financial and operational pain for organizations and their customers. In order to achieve the security objectives, it is necessary to recognize that the security of the services and the protection of the customers' data are essential. To this end, and specifically to support the current security equation, it is necessary to have an enterprise wide target customer security model. This should be designed to deliver enhancements to both customer- facing and back office security capabilities, and in particular to improve existing security defenses for remote online, telephone and mobile banking channels [2].

E-commerce in India
India has an internet user base of about 354 million as of June of 2015. Despite being the second largest user base in world, only behind China (650 million, 48% of population), the penetration of e-commerce is low compared to markets like the United States (266 M, 84%), or France (54 M, 81%), but is growing at an unprecedented rate, adding around 6 million new entrants every month. The industry consensus is that growth is at an inflection point. In India, cash on delivery is the most preferred payment method, accumulating 75% of the e-retail activities [6]. Demand for international consumer products (including long-tail items) is growing much faster than in-country supply from authorized distributors and e-commerce offerings. Largest e-commerce companies in India are Flipkart, Snap deal, Amazon India, Paytm. India's e-commerce market was worth about $3.9 billion in 2009, it went up to $12.6 billion in 2013. In 2013, the e-retail segment was worth US$2.3 billion. About 70% of India's e-commerce market is travel related. According to Google India, there were 35 million online shoppers in India in 2014 Q1 and is expected to cross 100 million mark by end of year 2016.CAGR vis-à-vis a global growth rate of 8–10%. Electronics and Apparel are the biggest categories in terms of sales. By 2020, India is expected to generate $100 billion online retail revenue out of which $35 billion will be through fashion e-commerce. Online apparel sales are set to grow four times in coming years.

Related works
Security is one of the principal and continuing concerns that restrict customers and organizations engaging with commerce [9]. The aim of this paper is to explore the perception of security in e-commerce B2C and C2C websites from both customer and organizational perspectives. With the rapid development of E-commerce, security issues are arising from

people's attention. The security of the transaction is the core and key issues of the development of E-commerce. This paper about the security issues of E-commerce activities put forward solution strategy from two aspects that are technology and system, to improve the environment for the development of E-commerce and promote the further development of E-commerce. Web applications increasingly integrate third-party services [13]. The integration introduces new security challenges due to the complexity for an application to coordinate its internal states with those of the component services and the web client across the Internet. E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Still, its definition is a complex endeavor due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions [11].

Review of Literature

Thomas L. Mesenbourg (2002) Digital Point is one of the biggest forums in the world, and the ecommerce section is filled with threads for chatting with folks on what your next step should be when scaling up your store.

William Stallings (1999) when viewed from the perspective of motivation intersecting with opportunity, risk management can be driven not only by the techniques or sophistication of the attackers and threat vectors, but also by their motives.

Khalid Haseeb (2002) the best time to start is at the very beginning, and use threat modelling for system design. But since the methodology is attack-oriented, it is never too late to start.

D. Berlin (1985) The tremendous increase in online transactions has been accompanied by an equal rise in the number and type of attacks against the security of online payment systems.

S. R. S. Kesh, and S. Nerur (2003) the threats of mobile devices motive the development of protections on mobile devices. Main methods now in use for mobile banking information security are: implementing encryption technology to protect data privacy, density authentication, and digital signature.

Schmid. B, (1990) "Elecktronische Markte. E-commerce based on data processing, including text, sound, image. The business includes various activities such as the electronic exchange of goods and services, instant delivery of digital content,

QIN Zhiguang, LUO Xucheng, GAO Rong, (2006) E-commerce has undeniably become an important part of our society. The World Wide Web is and will have a large part in our daily lives.

Abdullah M. Jaafar and Azman Samsudin (2001) Internet and e-commerce are closely wrapped towards developed countries. But they can achieve tremendous benefits to developing countries if it is applicable as an ideal business purpose.

Research Methodology

E-Commerce: Security Challenges and Solutions Six Security Needs in E-commerce are

- Access Control
- Privacy/Confidentiality
- Authentication
- Non Repudiation
- Integrity
- Availability

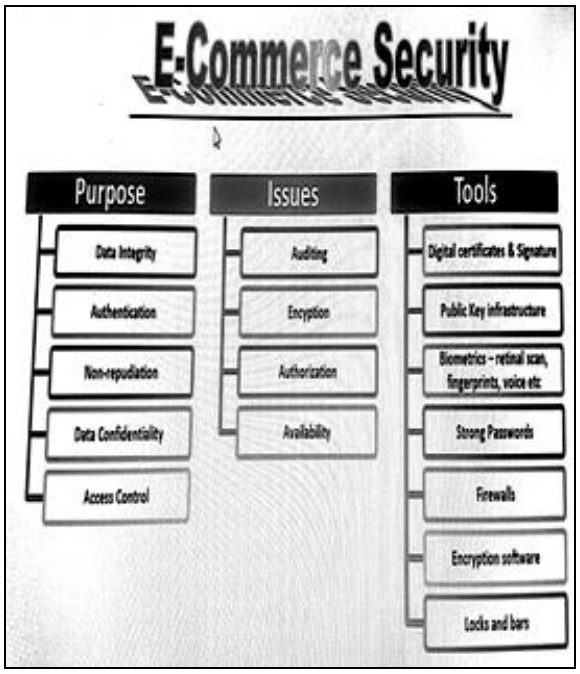

Fig 1: The Confidentiality, Integrity and Authentication Triad

1. Access control ensures only those that legitimately require access to resources are given access.
2. Confidentiality is concerned with warranting that data is only revealed to parties who have legitimate need, while privacy ensures that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure. Issues related to privacy can be considered as a subset of issues related to access control.
3. Authentication provides for a sender and a receiver of information to validate each other as the appropriate entity. This means having the capability to determine who sent the message and from where and which machine.
4. Non-repudiation is a property of the transaction that positively confirms that a particular client did indeed request the transaction in question without having the ability to deny making the request.
5. Integrity ensures that if the context of a message is altered, the receiver can detect it. It is possible that as a file, electronic mail, or data is transmitted from one location to another, its integrity may be compromised.
6. Availability as defined in an information security context ensures that access data or computing resources needed by the appropriate personnel are both reliable and available in a timely manner.

Security Challenges to E Commerce

Many companies offering their products and services online face security threats to their business. Many threats to E

Commerce could potentially occur from within the company or externally. The following are key threats businesses and consumers may encounter.

Malicious Programs

Malicious codes or malware can take the form of software designed to cause damage to a computer, server or computer network. Malware comes in a number of different forms and variations of attack. A computer virus is a computer program which can copy itself and infect a computer. The virus can also spread from one computer to another by means of executable codes when one user inadvertently transfers the program using removable storage devices such as a USB drive or CD. In other cases a virus can be transferred via email attachment to other users who may download or execute the attached program file.

A worm is a program which uses a computer network to send copies of its program to other computers on a given network and might do so without any computer user initiating the activity. Worms generally cause harm to a company's network by consuming bandwidth.

Trojan horses are programs that look legitimate from the outset to perform a desirable function for a computer user. However when the program is executed the Trojan horse orchestrates unauthorized access of the user's computer system.

Spyware is a type of program installed on computers and collects information over time without the user's knowledge. The spyware is usually hidden from the user and can be very difficult to detect.

Adware is a software program which automatically plays, displays or downloads advertisements to a computer. The advertisements can be in the form of a pop-up as their objective is to generate revenue for the program's author.

Finally root ware is a program hackers use to give them privileged access to a computer by actively hiding its presence from IT administrators. Once the root ware is installed the hacker can circumvent the standardized authentication and authorization mechanisms built into E Commerce software. Based on the most recent report released by Computer Economics (2007),malware cost businesses $13.3 billion worldwide. Fortunately financial losses from malware have gradually declined from prior years as a result of better anti-malware technology. Businesses encounter IT security threats in other ways. Stolen or lost hardware can affect businesses as they contain data vital to the business.

Crimeware is a program designed to conduct identify theft on a user's computer while consumers use online bank accounts and retailer sites. Recent trends point towards greater emphasis on IT security to combat the criminal activity of phishing. Phishing is a process of criminals attempting to acquire from users sensitive information such as usernames, passwords, and credit card details by pretending to be a trustworthy entity. Communications may come in the form of social web sites, auctions, online payment processors or IT administrators who target unsuspecting users. This type of activity is usually carried out by e-mail or instant messaging and directs users to enter details at a bogus website whose look and feel are almost identical to the legitimate website. Fraudsters often target consumers of banks, online retailers, and payment services. Wireless networks which are not secured also pose a threat to consumers and businesses using E Commerce. Fraudsters can gain entry into a company's network through an open wireless network and potentially steal client and proprietary information. Most businesses do not take precautions to protect against this threat. One example in 2007 involved a major security breach affected a large U.S. retailer (TJX Companies) resulting in a loss of $ 46 million customer credit and debit card numbers due to having an unsecured open wireless network.

Distributed Denial of Service Attacks (DDOS)

Businesses that trust on web based exchanges are and can keep on being helpless against Denial of Service (DoS) assaults. DoS assault scripts are the chief basic, powerful and best to execute assaults accessible on the on the web. No actual harm is finished to the victim site. The entrance systems to that are only frail with approaching bundles. it may be every representative's fantasy to be amid this situation if the approaching bundles were real customer requests. On the other hand, it will be their most noticeably bad dream in the event that they are the objectives of a DoS assault. Early DoS assaults were activated by one inward machine against another. The Distributed Denial of Service (DDOS) assaults are the latest development of DoS assaults and their prosperity relies on upon the absence of moderate locales to find, contain and destroy the infiltration of their network.

Security Technologies

Two types of encryption methods offer reliable protection to E-commerce businesses. They are symmetric and asymmetric.

a. Symmetric Encryption

Symmetric encryption [4, 10] may also be referred to as single key or shared secret encryption. In symmetric encryption, a single key is used both to encrypt and decrypt messages. Common symmetric encryption algorithms include AES, DES, 3DES, and RC4. Symmetric encryption algorithms can be extremely fast, and low complex which allows for easy implementation in hardware. However, they require that all hosts participating in the encryption have already been configured with the shared secret key through some external means.

b. Asymmetric Encryption

Asymmetric encryption [4, 10] is also known as public-key cryptography or two- key encryption. Asymmetric encryption differs from symmetric encryption primarily in that two keys are used: one for encryption and other for decryption. The most common public key encryption algorithm is RSA. Compared to shared key encryption, asymmetric encryption imposes a high computational burden, and tends to be much slower. its major strength is its ability to establish a secure channel over a non- secure medium (for example, the Internet). This is accomplished by the exchange of public keys, which can only be used to encrypt information. The complementary private key(non shared) is used to decrypt.

c. Secure Socket Layer

The E-commerce business is all about making money and finding ways to make more and more money. But that's hard

to if the consumers don't feel safe executing a transaction on your Web site. Secure Socket Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. When you have SSL, you are protected as well as your customer [10]. The server – which is basically another name for a computer that stores information about your website for viewing by the customers and others – must have a digital SSL certificate. SSL provides these certificates and is able to read them. SSL certificates come from a trusted third party that can guarantee encryption process. The SSL certificate is a proof that the server is what it says it is. Having a SSL makes it harder for fraudsters to pretend to be another server.

d. Digital Signature

Based on the public-key cryptographic method combined with data hashing functions such as MD-5 and SHA-1, digital signatures are implemented to verify the origin and contents of the online transaction, translating to consumers proving their identity to vendors in the transaction and providing non-repudiation features [4].

A digital signature functions for an electronic document like a handwritten signature does for printed documents. The hand written signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached [8]. A digital signature actually provides a greater degree of security than the handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been modified either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated, this means the signer of a document cannot later disown it by claiming the signature was forged. In other words, digital signatures enable "authentication" of digital messages, assuring that the recipient of a digital message of both the identity of the sender and the integrity of the message.

e. Digital Certificates

Digital Certificates provide a means of proving a persons identity in electronic transactions, much like a driver license or a passport does in face-to-face interactions. With a Digital Certificate, you can assure business associates, friends and online services that the electronic information they receive from you are authentic. Digital Certificates bind an identity to a pair of electronic keys that can be used to encrypt and sign the digital information [6]. A Digital Certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent users from using phony keys to impersonate other users. A Digital Certificate is issued by a Certification Authority (CA) and signed using the CA's private key. Digital Certificates can be used for a variety of electronic transactions which includes e-mail, electronic commerce, groupware and electronic funds transfers.

f. Smart Cards

A smart card [11] can generally be defined as a plastic card with dimensions similar to traditional debit/credit cards, into which an electronic device has been incorporated to allow information storage. Frequently, it also has an integrated circuit chip with data processing capacity. Smart cards are normally separated into two categories: microprocessor cards and memory cards, commonly named smart cards for their capability to do data processing and the sophisticated algorithms embedded in them [11]. The lack of security and a fear of hackers are some of the reasons that have caused the slow growth of the online interactive commercial transactions among individuals and enterprises, generally called consumer–to-business (C2B) e-commerce [7, 1]. In spite of the number of these breaches, credit cards are being used as one of the payment mechanisms over the Internet [4]. As long as commercial transactions over the Internet are not too great in the number and have a small individual economic value, the actual threat could be considered at a low or acceptable risk level. Once this type of transaction gains more consumer confidence and the volume increases, it will attract more and more fraud activities, thus increasing the level of risk exposure. One of the techniques that has begun to be used in France and other countries is the smart card with a C-SET (Chip-Secure Electronic Transaction) protocol for online authentication. This authenticates both the card as well as the customer, and therefore offers a payment guarantee without customer non-repudiation [3].

g. Electronic Money

Electronic money or digital cash (DC) [6] is an electronic method of payment on the Internet with the result that money is transferred from one account to another. One can visualize a DC transaction as a foreign exchange market, in the sense that money is converted to DC before it can be spent. When making a purchase, a buyer will send a 'digital coin' message encrypted with its private key containing his identity, the amount of the coin, Internet address, its serial number and expiry date. A record is kept of that transaction to ensure that the coin is not double spent. The digital coin is also encrypted with the merchant's public key [12]. The merchant decrypts the digital coin with his private key and verifies the message. The issuer must verify the serial number of the digital coin to confirm that it is still current and has not been already spent. The issuer then credits the merchant's bank account with the currency and then cancels the serial number.

Conclusion

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. Day by day E-commerce and M-commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction [9].

Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data source. Confidentiality: protection against unauthorized datadisclosure. Privacy: provision of data control and disclosure.

References

1. Abdullah M. Jaafar, Azman Samsudin**.** A New Public-Key Encryption Scheme Based on Non-Expansion
2. An Introduction to Cryptography found in the documentation of PGP® Desktop 8.1. 2004, 17.
3. Cetin K. Koc, Next Generation E-Commerce Security Information Security Laboratory 2, 1999
4. D. Berlin, Information Security Perspective on Intranet, presented at Internet and E-Commerce Infrastructure, 2007.
5. Jagdev Singh Kaleka, E-Commerce: Authentication & Security on Internet, Deptt. of Technical Education and Industrial Training, Govt. of Punjab
6. Joel Weise, Public Key Infrastructure, Sun PSSM Global Security Practice Sun BluePrints™ On Line August 2001
7. Khalid Haseeb Secure E-commerce Protocol, International Journal of Computer Science and Security IJCSS, 2011; 5(1):742-751
8. PCO A. J Menezes, and S.A. Vanstone, Handbook of Applied Cryptography: CRC Press, 1996.
9. QIN Zhiguang, LUO Xucheng, GAO Rong, A survey of E-commerce Security, School of Management, University of Electronic Science and Technology of China Chengdu, Journal of Electronic Science and Technology of China 2004; 2(3).
10. SRS KESH, NERUR S. A Framework for Analyzing E-Commerce Security, Information Management and Computer Security, 10(4)149-158.
11. Schmid B. Elecktronische Markte. 1993; 465-480.
12. Thomas L. Mesenbourg, An Introduction to E-commerce, Philippines: DAI-AGILE, 2000
13. William Stallings, Cryptography and Network Security, 3rd edition, Prentice