Vol III Issue II August 2013

Impact Factor : 1. 2018

ISSN No :2231-5063

Monthly Multidisciplinary Research Journal

Golden Research Thoughts

IMPACT FACTOR : 1. 2018

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Golden Research Thoughts

ISSN 2231-5063
Volume-3, Issue-2, August-2013

Trend Of E-commerce Technology & Its Security Issues

Anil M. Tirkar
Assistant Professor Smt. L.R.T. College of Commerce, Akola

Abstract: In the present era, it is not possible to live without internet for a single day. Internet makes its applications as a primary need for the person in different generations by providing a different technology of E-Commerce. E-Commerce is a most important application of Internet. It is cheaper and faster to carry out business transactions within an organization and among organizations electronically using the network connection. Thus it is important to understand how business transactions are carried out electronically reliably and securely. Security is very important issue for implementing ecommerce technique.

In this paper I trying to introduce advance techniques in electronic commerce, its security issue and different technology for providing reliability and security during any transaction through the E-Commerce.

Keyword:E-Commerce, Security, Cryptography, Encryption & Decryption.

INTRODUCTION:

E-Commerce is defined as the buying and selling of products or services over electronic systems. A wide variety of commerce is conducted via e-commerce, including electronic funds transfer, supply chain Management, online transaction processing, electronic data interchange (EDI) and automated data collection systems. It also pertains to any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact. E-Commerce is very widely used in the developed countries to enhance productivity, efficiency, accuracy and security.

E-COMMERCE CAN BE APPLIED IN ALL INDUSTRY VERTICALS INCLUDING:

Government, all sectors e.g. Health, Finance, Defense, Industrial.. etc
Banking, investment and finance
Manufacturing, Retail, Logistics
Telecommunication
Transport
And many more.

ADVANTAGES OF E-COMMERCE

In present era, ecommerce is widely used in different field mentioned above. E-Commerce can increase sales and decrease costs. 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, because the web can provide competitive bid information very efficiently. 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.

TYPES OF E-COMMERCE:

There are different types of E-Commerce according to a business and it consumers. There are five generally accepted types of E-Commerce:

Business to business (b2b)
Business to consumer (b2c)
Consumer to consumer (c2c)
Business to government (b2g)

1) B2B E-Commerce:

B2b E-Commerce is simply defined as E-Commerce between companies. This is the type of E-Commerce that deals with relationships between and among businesses.

ISSN 2231-5063
Volume-3, Issue-2, August-2013

2) B2C E-Commerce:

Business-to-consumer E-Commerce, or commerce between companies and consumers, involves customers gathering information; purchasing physical goods (i.e., tangibles such as books or consumer products) or information goods (or goods of electronic material or digitized content, such as software, or e-books); and, for information goods, receiving products over an electronic network. It is the second largest and the earliest form of E-Commerce.

3) C2C E-Commerce

Consumer-to-consumer E-Commerce or c2c is simply commerce between private individuals or consumers. This type of E-Commerce is characterized by the growth of electronic marketplaces and online auctions, particularly in vertical industries where firms/businesses can bid for what they want from among multiple suppliers.

4) B2G E-Commerce:

Business-to-government E-Commerce or b2g is generally defined as commerce between companies and the public sector. It refers to the use of the internet for public procurement, licensing procedures, and other government-related operations.

Why Security in E-Commerce ?

When you uses any application in E-Commerce , It will flow a very important information through the world wide web, so security is very important issue during the use of ecommerce application so that the your transaction should be secure, therefore ecommerce system must meet four integral requirements:

Privacy – information exchanged must be kept from unauthorized parties,
Integrity – the exchanged information must not be altered or tampered with,
Authentication – both sender and recipient must prove their identities to each other
Non-repudiation – proof is required that the exchanged information was indeed received.

These basic maxims of ecommerce are fundamen tal to the conduct of secure business online. Further to the fundamental maxims of ecommerce above, E-Commerce providers must also protect against a number of different external security threats, most notably Denial of Service (Dos). Security is an eternal concern for organizations as they face the dual problem of protecting stored data and transported messages. Organizations have always had sensitive data to which they want to limit access to a few authorized people. Historically, such data have been stored in restricted areas (e.g., a vault) or encoded. These methods of restricting access and encoding are still appropriate. Electronic commerce poses additional security problems. First, the intent of the Internet is to give people remote access to information. The system is inherently open, and traditional approaches of restricting access by the use of physical barriers are less viable, though organizations still need to restrict physical access to their servers

Second, because electronic commerce is based on computers and networks, these same technologies can be used to attack security systems. Hackers can use computers to intercept network traffic and scan it for confidential Information. They can use computers to run repeated attacks on a system to breach its security (e.g., trying all words in the dictionary for an account's password). Since the main goal of EDI is to provide a standardized message format which can be used by all trading partners to communicate transactions such as purchase orders, shipping information, and payment, security was not included in the EDI message translating and transmitting process and was left to the application or the underlying transport protocol to handle. Since EDI mostly use.

To satisfy these all the requirement mention above developer should take care of these and he must have to implement application by adding a different security mechanism so that the user can do secure and reliable transaction.

Overview of a Methods to add Security in E-Commerce

There are different techniques which can be used to provide security in during transferring a data through World Wide Web while using ecommerce applications. Cryptography is one of the techniques to provide reliable data transferring through the web.

Cryptography:

Cryptography is the science of writing in secret code using mathematical technique. Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. The cryptography includes two main process, the first one is encryption and second is decryption.

Encryption and Decryption:

Data that can be read and understood without any special measures is called plaintext or clear cipher text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption.

TYPES OF CRYPTOGRAPHY

a) Conventional Cryptography:

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government. Figure 1. is an illustration of the conventional encryption process.

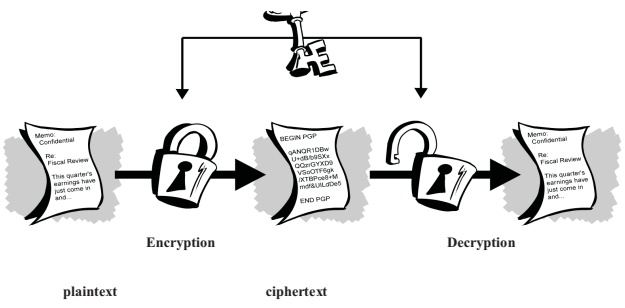

Figure 1. Conventional encryption

There are different algorithms to implement conventional cryptography technique. Some of these are
1) Data Encryption Standard
2) Advance Encryption Standard
3) CAST-128/256
4) International Data Encryption Standard
5) Rivets Cipher etc……

b) Public key Cryptography:

The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975. Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.

It is computationally infeasible to deduce the private key from the public key.

Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

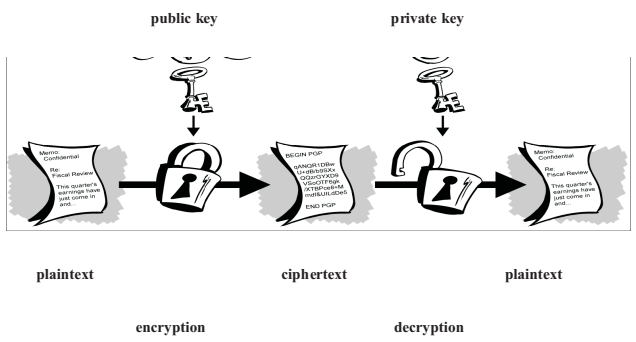

Figure 2. Public Key Cryptography

There are different algorithms to implement public key cryptography technique. Some of these are

1) RSA
2) Diffie Hellman
3) Digital Signature Algorithm
4) ElGamal
5) Public Key Cryptography Standard.
6) Key Exchange Algorithm etc…..

All these secrete key cryptography algorithms and public key cryptography algorithms are vary according to key size they generate, security they provide, and no of steps perform during key generation. We can use any one of these algorithm to secure our data while it transform through World Wide Web.

CONCLUSION

In this paper we discuss an E-Commerce applications, need of security while using ecommerce application. As well as we discuss different security issue while transferring a data through world wide web and methods, helps to successfully encoded a message by using cryptography. These all techniques provide reliable transformation of an information trough the World Wide Web.

REFERENCES

a) Dr. C.S.Rayudu, "E-Commerce E-Business", Ist edition, Himalaya Publishing House Mumbai, 2004.
b) Dr. Milind M.Oka, "E-Commerce", Ist edition, Everest Publishing House Pune,2000.
c) Prof. P.T.Joseph, "E-Commerce – An Indian Perspective", IIIrd edition, PHI Learning Private Limited New Delhi, 2010.
d)William Stallings, "Networking Security Essentials Applications & Standards", IIIrd edition, Pearson Education, 2011.
e) William Stallings, "Cryptography and Network Security – Principles & Practice", IIIrd edition, Pearson Education, 2004.
f) Andrew S. Tanenbaum, "Computer Networks", IVth edition, Pearson Education, 2011.
g) Garry C. Kessler (2012) : "An Overview Of Cryptography".