Learning Paradigm to Develop Secure E-Commerce System

Amit Garg*, Aman Gupta**, Rahul Bansal**

**Department of CSE, Kurukshetra University, Kurukshetra, amit.indus86@gmail.com,*

*** Management Department ,Kurukshetra University, Kurukshetra, amangupta5000@gmail.com*

**** Department of CSE, Maharshi Dayanand University, Rohtak, rahulbansal1612@gmail.com*

ABSTRACT

From people's attention security issues are arising with the rapid growth in the field of E-commerce. Security issues & threats in E-commerce environment are varied and can be caused intentionally and unintentionally by both insiders & outsiders. Transaction security in business management is the key issue of e-commerce so as to improve the environment for the development of E-Commerce and promote the further development of IT.

***Keywords*- E-commerce, Security issues, Cryptography, public and private key,message digest**

I. INTRODUCTION

E-Commerce is a modern business methodology that addresses the needs of organizations, merchants and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery.

E-Commerce came into a progress of networking and multimedia feels with the development of internet technology. It is through open complete network to handle online transactions that helps in implementing a variety of business process. This process may be servicing of goods like advertising, purchasing, consultancy financial services, commodities payment etc. As a result E-Commerce is an open trade on the internet (public network).

II. SECURITY ISSUES IN E-COMMERCE SYSTEM

E–Commerce business transactions are the security issue that exists in two aspects which are the security of information and security of the system. The security of informal can be tempering with and loss information, denial and forgery information etc. the security problems of system may be hacking, damaging of system with virus activities and so on.

A. Computer Network Problems:

Those are great dangerous in security management and difficulty to defend against hackers attack.

i. Anti- Virus Problem:

Now days, new virus are rapidly increasing due to internet technology. These viruses directly transmit in the networks that result in the big economic loss.

*ii. The Security issues of information***:**

The unauthorized users malicious temper the network data that interrupted such as increase, reduce or remote data which cause the information rise; the authenticity and integrity. Some illegal users sent again intercepted data from the web to malicious attack the other's hardware and software in the public network.

B. The Security issue of servers:

The core issue of E- Commerce system is business servers that is basically name of information about business related software/hardware a lot of information about clients and products like cost, price etc. There are some ways to attack the servers: The authorized users can send a large no. of invalid request to host computers to consume the basic resources of server that results in the blockage of normal service of the server.

C. Business Transaction Security Issue:

i. *The problem of the uncertainty of identity:* The attacker through illegal ways can steal the authorized user identity, and then use these identity to obtain illegal revenues by transacting with others.

ii. *The problem of denial of transaction:* E-Commerce transactions none repudiate as same as traditional trade. Some users to shirk their responsibilities send malicious message by their own sending.

iii. *Other Aspects of Security issues:*

The E-Commerce security threats come from all possible potential aspects. They are deliberate or unintended. E-Commerce transaction results in a series of legal issues such as lease problems of network deal, the operator leak information, the media waste lead to leak information and so on. All of this is necessary to provide legal protections to E-commerce transaction.

III. HOW CAN CONTROL E-COMMERCE SECURITY

Here we are preparing some security control requirements at the E- Commerce transaction process:

A. Information Validation

E-commerce is basically related to organizations, entire reputation, coordination, product prices, and secure interrelated data and overall to the country. So we should control these threats that can affect the E-Commerce secure system in the form of application, program error, hardware failure, operator error, network failure etc. only then, our E-Commerce transaction system will be more efficient at a certain time and place.

a) Information transaction confidentially.

b) The integrity request when store data should prevent illegal destruction or change on site.

c) Repudiation of information should not be occurred.

d) The authorization and authenticity of trader identity.

e) The message sent over network cannot be modified.

B. Development of Security mechanism to E-Commerce

i. *The security mechanism strategies adopted by E-Commerce:*

E-Commerce security technology is divided in to two categories that are data encryption and authentication technology.

ii. *Data Encryption Technology:*

It is the one of the important technology is implant secure E-Commerce system. First change the original message into cipher text (encoded form), second send the cipher text to original message. Encryption technology is based upon key-exchange. So, it is divided in to symmetric key encryption, asymmetric key encryption and hashing encryption.

iii. *Symmetric Key Encryption*:

In this technology we use single key to encrypt and decrypt the message of information. This is fast but not effective because distribution of original key is a big issue that results in periodic change of key for security. Fig.1 shows this procedure.

iv. *Asymmetric Key Encryption:*

In this technology, two keys (public key, private key) are being used to encrypt or decrypt the message of the original message is encrypted by private key; then it is decrypted by public key and vice versa. It is difficult to find out the public key for a private key and vice- versa, so this encryption technology is much effective. Fig 2 shows the asymmetric key to encryption.

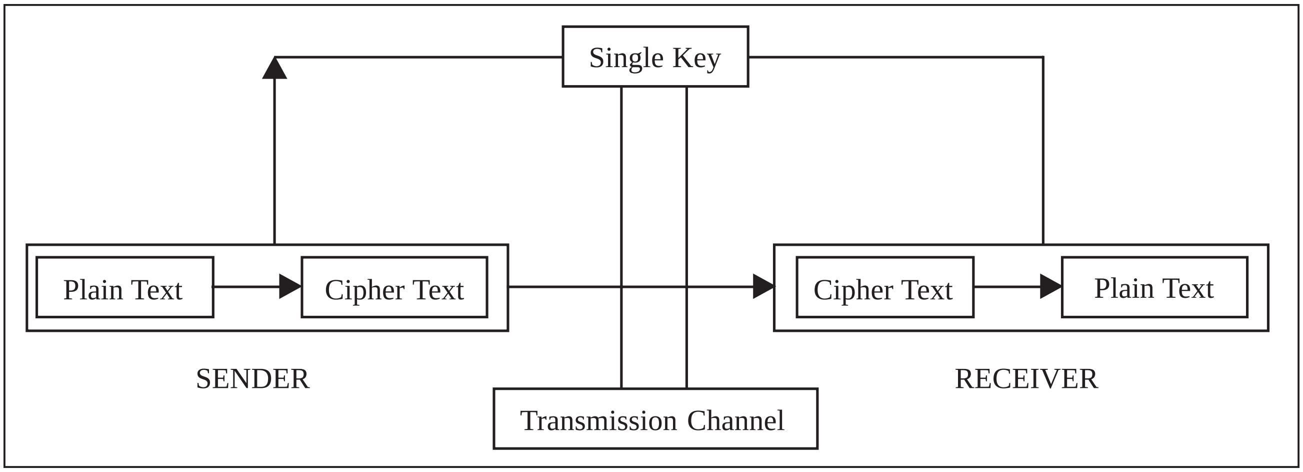

Fig.1: Symmetric Key Encryption Technology

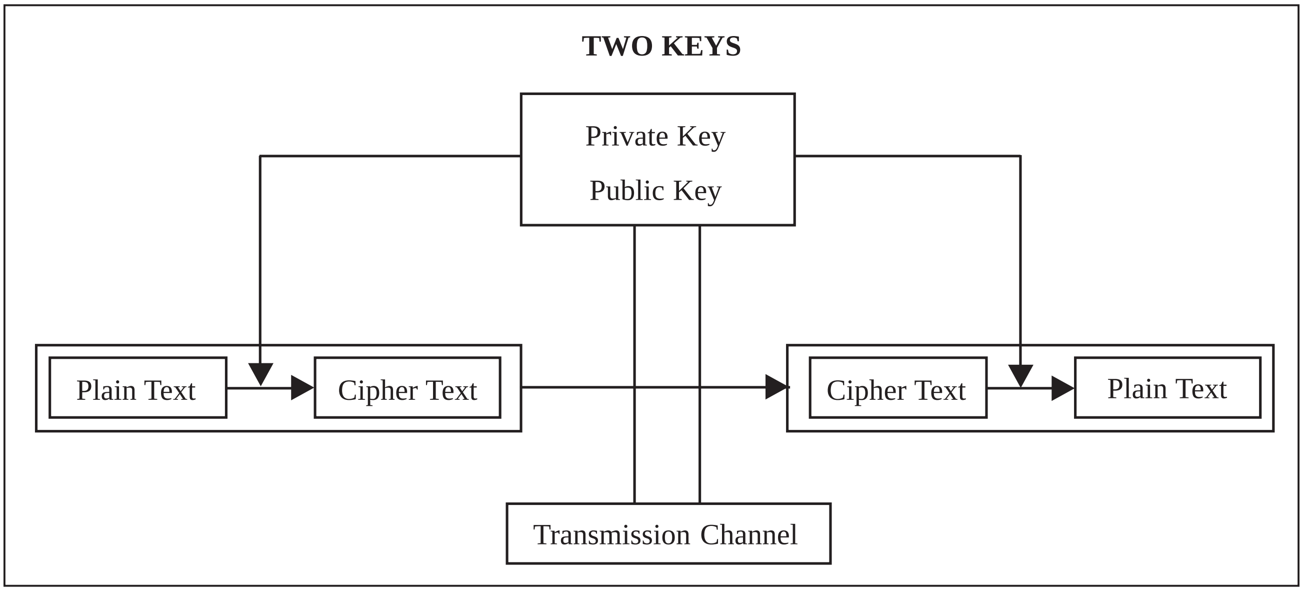

Fig.2: Asymmetric Key Encryption Technology

V. HASH CODE ENCRYPTION:

In this technology hash algorithm (i.e. hash function) is used to drive the hash value of message to check whether the original message is modified or not. If the sender and receiver hash value do not match, it means message is intercepted and modified.

a) *Authentication Technology:*

It uses one way hash function to compute a number of elements in the Document. Then the document with the abstract code regards complete information sends to recipient. The receiver uses some method on that element of the document and calculates abstract code. If this code matches, it means message has not changed.

b) *Digital Signature Technology:*

Digital signature takes the concept of traditional paper- based signing and turns it into an electronic "fingerprint". This "fingerprint" or coded message is unique to shoots the document and the signer and birds both of them together. It ensures the document after it is signed invalidate the signature, here by protecting against signature forgery and information tampering.

C. *Digital envelope:*

The following explains what happens at each step:

1. The message is encrypted using symmetric encryption. Typically, a newly generated random message key (secret key) is used for the encryption. Symmetric encryption means that the same key is used for both encryption and decryption (a secret key). Anyone wanting to decrypt the message needs access to this key.
2. To transfer the secret key between the parties, the secret key is encrypted using the recipient's public key.
3. The encrypted document and the encrypted message key are packed together in a single data packet to save or send to the intended recipient.

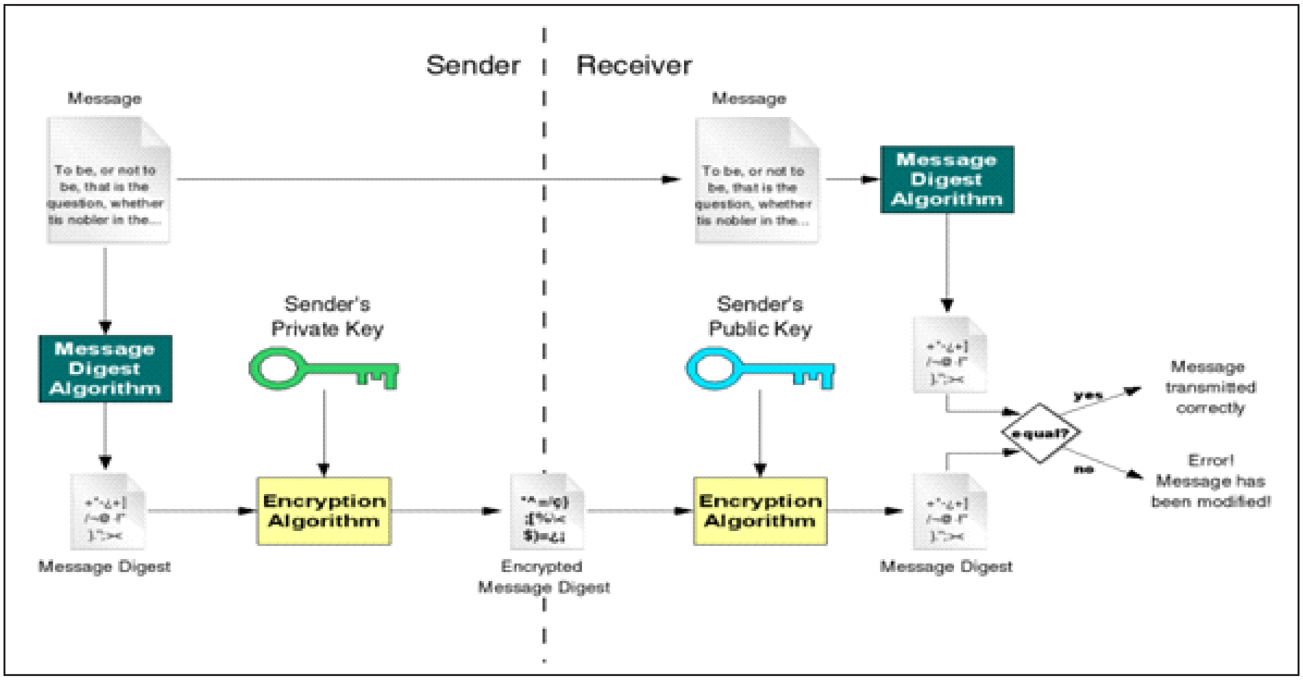

Fig 3 - digital signature security procedure

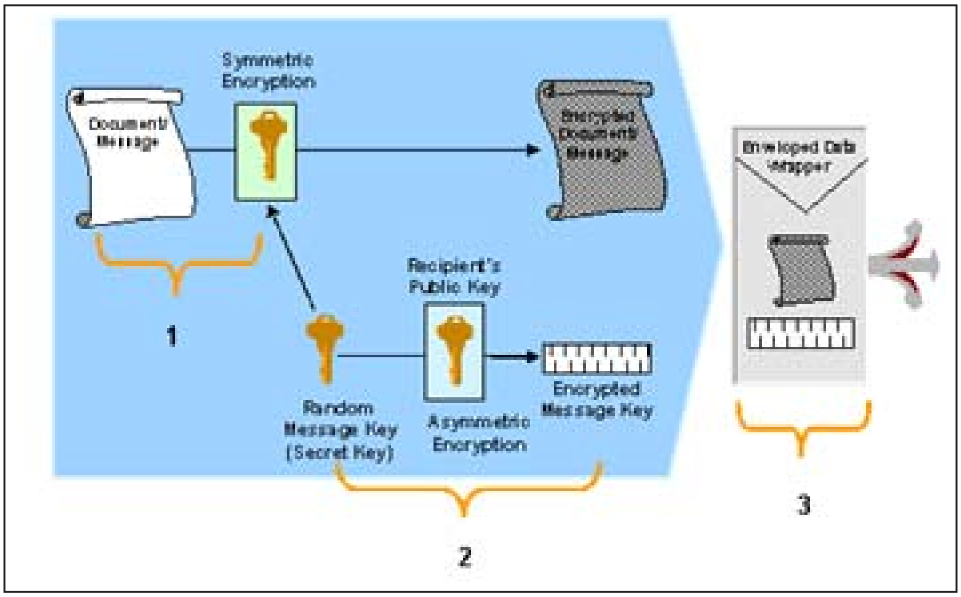

Fig 4 - digital envelope security procedure

VI. CONCLUSION

In conclusion the e-commerce industry faces a challenging future in terms of security risks it must avert with the rapid growth in technological knowledge and internet availability; criminals are becoming more sophisticated and dangerous in deception and attacking. In saying this there are multiple security strategies (already discussed) which any E-Commerce provider can instigate to reduce the attack risk and compromise significantly. Risk awareness, detailed and open privacy cilices strong authorizations and authentication and encryption technologies will go on long way such that risk of compromise should be kept minimal.

REFERENCES

[1] Wang Li, "*The Safeguard of EC Security Technology*", Peking University Journal (Special), 2000, pp. 115-120.

[2] Zhao Jing, Hu Yunfa, Li Liyan, "*Online Shopping Security Protocol of EC—SSL and SET*", Computer Engineering, 1999,25 (12),pp.90-91,103.

[3] China Internet Network Information Center, The Eighteenth Statistics Reporter of the Development Chinese Internet, Jan. 2006.

[4] CCID Consulting Co., Ltd, The Review and Expectation of 2005 China EC Market, Nov.2005.

[5] Hu Shuixing, Yu Lifan, " *Research of E-commence Performance Assessment*", Group Economics Research 2006.

[6] Lv Feng, Zhou Liang, Research on Framework of EC Wuhan University of Technology Journal, Apr.2004.

[7] A good introduction to computer security. Pfleeger, Charles P., *Security in Computing*, Second Edition, Prentice-Hall, Inc., 1996.

[8] Low level tips for writing secure code. Howard, Michael and LeBland, David, *Writing Secure Code*, Second Edition, Microsoft Press, 2003.

[9] The state of e-commerce security. http://www.newsfactor.com/perl/story/19462.html

[10] The house of secure e-commerce. http://www.istart.co.nz/index/HM20/PC0/PV21902/EX24014/AR2505