2014 Fourth International Conference on Communication Systems and Network Technologies

# E-commerce Security Through Asymmetric Key Algorithm

Ankur Chaudhary
Department of CSE/IT,
Swami Vivekanand Subharti University, India
ch.ankur.402@gmail.com,

Khaleel Ahmad
Department of CSE/IT,
Swami Vivekanand Subharti University, India
khaleelamna@yahoo.co.in

M.A. Rizvi
Department of Computer Engg. & Applications
NITTTR, Bhopal, India
marizvi@nitttrbpl.ac.in

***Abstract*— E-commerce provides low transaction costs and more convenient business mode to all over world customers. We describe many asymmetric approaches which use in E-commerce transaction and other supported cryptography algorithms which are essential in working setup of E-commerce. In this paper, we propose a model of E-transaction based on PGP. It will show that how much secure payment and customer order of information will be efficiently handled by PGP based on dual signature. Along with, we also derive a comparison table of all asymmetric algorithms in which we analysis all the properties of algorithms.**

***Keywords—Digital Signature, Encryption, E-commerce, Pretty Good Privacy, Secure Socket Layer, Secure Electronic Transaction.***

## I. INTRODUCTION

With the enhancement of Internet technology, a setup also in existence now that is E-commerce which is based on network and multimedia technology. It conducted transaction through Internet also called open public network which is effective to implement a variety of e-business process [1] [2]. E-commerce is an online business trade on the Internet. To provide secure trade in the form of E-commerce web service security plays an important role in such business processes. In E-commerce, more and more security issues are increasing day by day on the open Internet like client information leakage, credit card clowning etc. So, it is the cause that people's interest using of E-commerce decreasing day by day. They feel panic when they want to pay on Internet [3]. To develop the E-commerce, security is the main issue on the Internet. So, to avoid the security issues we should have some secure conditions that should provide the adequate protection to the transaction information for each and every entity in E-commerce transaction. Customers are cautious to take participate in e-commerce due to security problems like hacking customers' information and many other attacks exist in the open network which is dangerous to the customer information[4]. Internet is full of security threats viz. DOS attack, integrity violation, sabotage, access control and infrastructure attacks. So, all of these threats becomes as cyber war or cyber terrorism collectively. Cyber war is corrupting the web and host system and its entire component and collapse it.

## II. LITERATURE VIEW

This paper describes important security issues in E-commerce. Through the analysis, the customers and the organization to join those in a single phenomenon with respect to E-commerce security. By such analysis of information, it generates a "holistic" view. It will reduce the gap between organization and the customer's objectives and their perceptions. By the holistic view of analysis, information about customer and the open Internet organization implement such solution which aligned the customer needs more effectively [5].

### *A. Security Issues In E-commerce At Various Levels:*

*1) Transaction level:* This level focuses on transaction participants that are legal. These threats are arises from the following three factors reply attacks, mutual authentication and no record of transaction [5] [6].

*a) Reply Attacks:* It is a network attack in which attacker want to cheat the cryptographic protocol by the re use transmission of a message again and again. The data will be valid and maliciously repeated according to the attacker benefit. This attack is carried out either by source or by the adversary who wants to intercepts the information and retransmits it. Session token is the method to handle this type of attack.

*b) Mutual Authentication:* It is also called two way authentications. If any intruder (unauthorized user) comes between the communicating party (authorized user) and mutually authenticated by them, then this creates problem to authorized users.

*2) Network and Transport Level*: It is hard to manage the security management because there are great danger in security management and also much difficulty to protect from malicious attack. There are several viruses with high transmission speed on the web, which may cause economic loss. Unauthenticated user use improper techniques to block session data to attain the effective information from authenticated users. Business server is the like a kernel to the E-commerce which has large number of business software and save lot of information and record of client information. So, the servers may cause the leakage of client information.We describes some issues of E-commerce security at network and transport level in below [7].

*a) Eavesdropping:* Eavesdropping is an attack in which unauthorized user in real time intercept on private communication network, information which is communicated between authorized users such as listening telephone conversation of two communicating parties.

*b) Illegal Access:* This problem is created when an unauthorized user access the system information or system resources.

*c) Server Problem:* Server is the main part of E-commerce. Server is a combination of softwares and

978-1-4799-3070-8/14 $31.00 © 2014 IEEE
DOI 10.1109/CSNT.2014.163

hardwares which are installed in CPU and it stores many type of sensitive data (cost, quality etc.). Server problem means that the information is not available to the clients or server does not give response of users' request. This is the major security issues in communication network as denial of service attack [8].

*d) Security Agreement:* Security agreement is the document in which we write the statement that they do not interfere one another business security. Till now, security agreements do not have global standards or norms, so that the cause of restrictions in the activity of International e-business. In E-commerce, security management is more dangerous and difficult to defend against hackers or attackers.

*3) Business Integration Level*: E-commerce transaction is the same as trade with non–repudiation. Many users may maliciously deny to message that they send himself in order to shrink their responsibilities [9] [10].

*a) Identity Uncertain:* There is a need of virtual network platform to the E-commerce transaction process in which no need of both side meeting. This becomes major problem in E-commerce transaction because an attacker can steal the identity of authorized user and then do the transaction in order to receive benefit.

*b) Deny Transaction:* E-commerce transaction is same as a trade with non–repudiation problems. Many users may deny for any message which is send or receive by them.

*c) Amend Transaction:* E-commerce shares the similar concept of traditional business in which the transaction time cannot be modified.

*B. Security Approaches in E-commerce At Various Levels:* Followings are the various security approaches at various levels:

*1) Application System Level:*

*a) Confidentiality:* It tells that only authorized users can access the information in the system.

*b) Integrity:* It tells that only authorized users can modify any information over the network.

*c) Anonymity:* Only for few E-commerce applications, it is essential to develop techniques which provide receiver anonymity services, sender anonymity services and transaction anonymity services.

*d) Non-repudiation:* This ensures that the sender cannot deny after the sending or receiving (sender non –repudiation and receiver non-repudiation).

*e) Availability:* Almost all E-commerce applications requires availability of trusted party such as Key Distribution Center (KDC) for Distribution of public key, Availability removes the problem of denial of service attack

*2) Security Protocol Level:*

*a) Secure Socket Layer:* It is a protocol layer which exists between the connection oriented layer (TCP/IP) and application layer (HTTP).TCP provide the end to end reliable service which is used by the SSL.TCP established a secure communication between client and the server by allowing mutual authentication. To provide such secure services between client and the server it uses encryption for privacy and digital signature for integrity. It consist four sub protocols

- SSL handshake
- SSL change cipher spec protocol
- SSL alert protocol
- SSL record layer

*b) Secure Electronic Transaction (SET)*: Secure Electronic Transaction is communication protocol standard and an encryption and security specification protocol for securing credit card transactions in open network called Internet during E-commerce transactions. SET is not a payment system but it is security standard and a combination of security protocols and formats. This enables the users to online transaction through their credit card in open network. SET is a secure communication open standard which provides privacy and protection to ensure the authenticity of electronic transaction. Privacy is more important for consumer protection. Without privacy, any consumer can never be authenticated as consumer and without authentication, neither the merchant nor the consumer can not be sure that a valid transaction is being made. SET is an important part of E-commerce [11]. There are several components of SET which are cardholder application (digital wallet), merchant server component, Payment gateway component and Certificate Authority component. SET provides three services which are given below

- SET gives a secure communication network among all the different communication parties involved in e-transaction.
- SET also provides trust by the use of X.509 version three digital certificates.
- It ensures the privacy because in a transaction the information is only available to parties when and where necessary.

*3) Security Authentication Level:*

*a) Message Digest:* Message digest is a hashing function of all the bits of the message in which comparison of sender's and recipient message digest take place to detect the error when message pass from the open network. Any change in any bit or bits in the message, changes the result of hash code. A variable size message M as input to the hash function and it accepts and provides a fixed size output message digest or hash code.

*b) Digital Signature:* To remove the problem of public key encryption (public key is known to all person in public key encryption in communication networks, so anyone can transmit a forge message to the receiver end by the use of receiver public key), we use digital signature for authentication. Before sending data content in the form of a message, sender encrypts message content with her own private key (digital signature), which authenticate the sender because in network no one has anyone's private key. This is the property which creates a prepared message which is authenticated its contents and its data integrity.

*4) Encryption Technology Level:* This technology encodes the plain text in to unreadable form which helps to protect the data from being viewed, and it also provides a technique to detect whether the receiving data is modified or not. Encryption technology provides secure communication over unsecured networks. We classify encryption techniques in two ways according to the used key.

*a) Symmetric Key Encryption:* This is also called the private key cryptography or private key encryption. In this, we use same key for message encryption and decryption. This key (k) is also called secret key. This encryption technology have two problems first is Simple symmetric encryption used so not provides better data security and second is Problems to exchange secrete key [12].

*b) Asymmetric Key Encryption*: It is also called public key encryption. In asymmetric key cryptography, we use two keys, one for encryption method and other key for decryption method. One key is Public and second one is private. Public key is known to all communication party in networks and private key is secret. Every participant has their own pair key (one for encryption and second for decryption) [13].

## III. PREETY GOOD PRIVACY (PGP)

PGP is also a security which provides confidentiality and authentication. It is used in electronic mail and storage applications. PGP have no Certificate Authentication (CA). In PGP, the sender and receiver have good faith in communication of data transfer. Sender introduces itself without any CA to the receiver by the web of trust [14].

- It is algorithm based it survived according to public feedback and considered extremely secure.
- It has wide field of applicability to maintain security in electronic mail and file storage applications.
- It has no interfere of government in development. There is no control on it by any standard organization.

## IV. PROPOSED MODEL

*Commerce Transactions and Volumes:* To design an E-commerce set up with effected security steps, we need define the E-commerce transactions. By definitions, we can easily measure the volume and growth of E-commerce transactions. There are some steps which are followed by the E-commerce system to use for online exchange of fund and the goods and services first. In E-commerce there are some steps [15] [16] [17]:

*a) Collecting information*: e.g., goods, services and price information from different sources.

*b) Product discussion:* a describe discussion takes place about product features, price, configuration, and many others.

*c) Agreement*: online commitment to purchase a product or service through online shopping and the order representing and responsibility to transfer money in exchange.

*d) Payment information:* buyers provide payment information to the seller.

*e) Delivery:* seller gives the goods and services to buyer and they receive them.

### *A. Working of Proposed Model:*

We designed a model to merge the payment order and the customer order information under the secure algorithms like RSA. You know that SET is secure for transaction purpose in the E-commerce but it is not successful in the E-commerce environment because it has a lot of drawback.

*1)* SET overhead is very heavy for E-commerce simple purchase transaction:

*a.* Four message are exchanged between merchant and the customer

*b.* Two message are exchanged between merchant and the payment gateway

*c.* 6 digital signature are computed

*d.* There are 9 RSA encryption cycles and 9 RSA decryption cycles

*e.* There are 4 DES encryption/decryption cycles and

*f.* Four certificate verification.

*2)* It has been argued by the merchants that they have to expand lot of money in order to process SET transaction from consumer's point of view, and also need to install the appropriate software.

*3)* Inter-operability problems is not solved.

*4)* Using SET, payment information is secure but goods' order information is not secure.

Due to this, we proposed a model for secure E-commerce transactions. In proposed model, we reduced the 4 DES encryption/decryption cycles and the third party CA interference also reduced from the E-commerce purchase transaction. Now, our model is based on the PGP and dual signature method. We merged both methods which gives the best result. Till now, PGP is used only for e-mail purpose but we used it in E-commerce first time. Suppose, we have two orders, one is goods order and other is payment order. We encrypt the goods order and payment order by RSA algorithm and send the encrypted customer and payment order information parallel to Internet open network. RSA is the most secure and the reliable algorithm in the asymmetric key cryptography. These encrypted messages of payment and the customer order information is merged with each other and then encrypted by RSA. Now, we have one merged message and encrypted three times.

The most important part of this model is the certificate authentication of introducer or the customer but in PGP there is no third party who provides the X.509 certificate to the authenticate the customer. In PGP, there is no CA. The customer will also an introducer of his authentication. Now, on the other side recipient will decrypt the received messages contents by RSA algorithm and the private key of the recipient will decrypt the encrypted content. In such manner, receiver gets information of merged payment order customer order information (POCOI). Our proposed model fulfill the deficiency of the SET by which we can achieve the secure e-transaction.

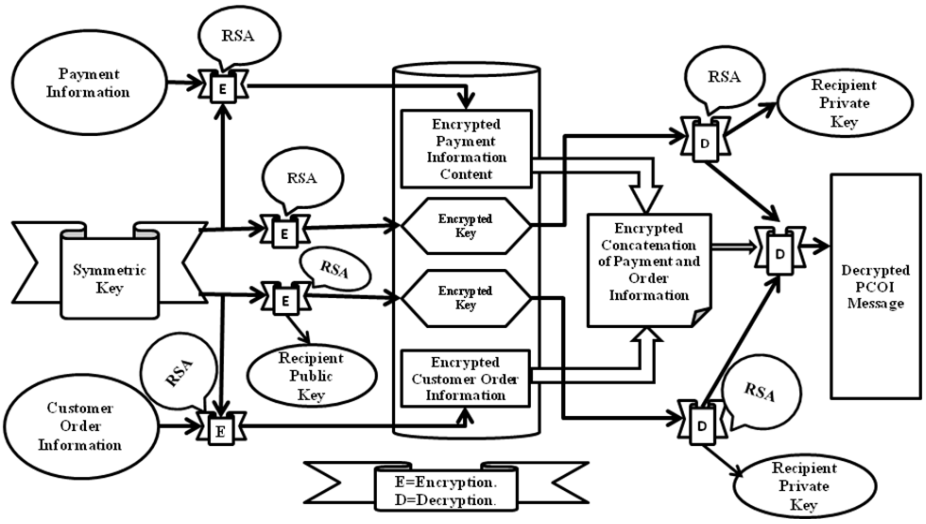


Fig. 1. Proposed PGP E-commerce Model

### *B. Flow Chart of the Proposed Model:*

It is the flow chart of proposed model; it depicts that how the customer sends the goods order and payment order to the merchant to buy the products online through E-commerce setup. First, customer select the goods from the available goods' list on the online shopping web portal and then customer sends the customer order and the payment order parallel to the merchant. Both payment order and the customer order are encrypted by RSA algorithm and then concatenate the both encrypted messages and send to merchant. Merchant decrypts the both encrypted messages by his private key and customer's public key and then deduct the payment from the account of customer. Merchant delivers the product to the customer.

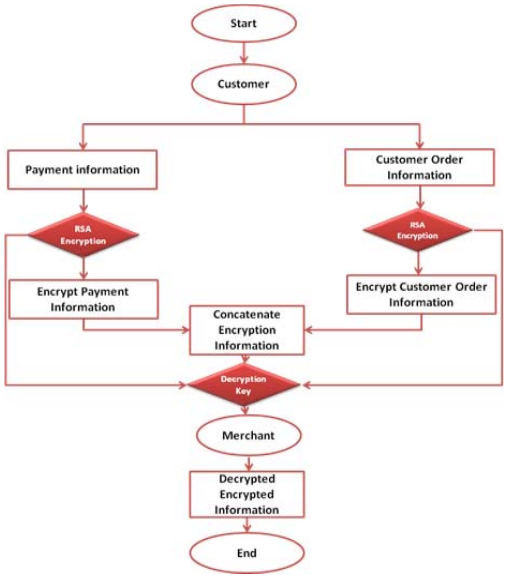


Fig. 2. Flow Diagram

### *C. Mathematical Simulation:*

Suppose customer wants to buy some products through online. There are two components need to buy the products online, one is customer order and the other is payment order. Every product has own id in the database of the online shopping web portal. Firstly, customer will fill the online form on web portal and select the product by the product id. Now, customer sends the customer information order to the merchant from online shopping web portal through Internet. The other component is payment order which is compulsory to buy any product online.

For product id encryption, we use RSA algorithm. To generate the public and private key, we have two prime numbers. Suppose product id is 7. The following steps show how the message encrypt and decrypt by the RSA algorithm.

*STEP1 Select two prime numbers r=11, s=3*
*STEP 2 Calculate n=r.s=11.3=33*
*STEP 3 Phi= (r-1) (s-1) =10.2=20*
*STEP 4 Select e randomly e=3, calculate the value of gcd(e,phi)=gcd(3,20)=1*
*STEP 5 Compute the value of d such that ed=1(mod phi) d=e-1mod phi=3-1mod 20 Calculate the value of d in a way that phi divides(ed-1) Find d such that 20 divide 3d-1. (d=1,2….) gives d=7*
*STEP 6 Public key=(n,e)=(33,3) Private key=(n, d) = (33,7).*

This is actually the smallest possible value of the modulus n for the RSA algorithm works. We want to encrypt the message *m=7,c=me mod n=73mod 33=343 mod 33=13.* The cipher text *c=13.* To test decryption we compute, *m= cd mod n=137mod 33=7.* We have a method to break down a potentially large number into its component and then calculate the value of all its components then again combine them for final result. To compute the value of 137, here we can use a simple step as follows -:

*STEP 1.Calculate the value of a=bc mod n*

*STEP 2.We can easily calculate the value of m: m=137 mod 33.*
*STEP 3. m = 13(3+3+1) mod 33.*
*STEP 4. m = (133 mod 33)*(133 mod 33)*(13 mod33) mod 33.*
*STEP 5. m = 19*19*13 mod=4693 mod 33 =7.*

For payment order information encryption, we use RSA algorithm with two prime numbers. Here the card number is 688, how it can be encrypted by the RSA algorithms. See the following steps:

*STEP 1 randomly choose two prime numbers r =47, s =71*
*STEP 2 Calculate the value of n = r.s = 47.71 = 3337*
*STEP 3 Phi = (r-1) (s-1) = 3220*
*STEP 4 Randomly select the exponent e = 79, compute the d =79-1 mod 3220 = 1019.*
*STEP 5 n and e is public key, d is private key, so p and q can be discarded.*
*STEP 6 encrypted message in the form of payment order text (c) will be C = 68879 mod 3337 = 1570.*
*STEP 7 decrypted message c = 1570 then original message (m) will be m = 1570^1019 mod 3337 = 688.*

That is the whole mathematical simulation based on the RSA algorithm. Both encryption and the decryption used the RSA algorithms to handle the online process of proposed model on the basis of dual PGP method.

## V. COMPARITIVE ANALYSIS

We have analyzed important algorithms related to asymmetric cryptography. We designed a comparative table with following attributes in table 1:

- Algorithms Name
- Features
  - *a) computational problem.*
  - *b) Encryption key size.*
  - *c) Applications*
- Drawback and Attack

TABLE 1: COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS

| S.No | Algorithm | Features | Drawback and Attacks |
|---|---|---|---|
| 1 | RSA | 1) Computational problem- integer factorization problem.<br>2) Encryption key size-1024 bit.<br>3) Application- Used in all worlds banking circle for security purpose and the transaction. | 1) Drawback- Key size is large, so it is 15 times slower than ECC/ Need more memory and computing power and more battery in RSA use.<br>2) Attacks- Chosen-cipher text attack, Discrete- Logarithm-Attack, Men-In-The-Middle-Attack. |
| 2 | Diffie Hellman | 1)Computational problem- Discrete Logarithm Problem, Decision Problem<br>2) Encryption key size-1024 bits.<br>3)Application- Key Exchange | 1)Drawback- The value of private key K is smaller in size which can be easily understood and decoded.<br>2) Attacks- It used only in key exchange only |
| 3 | DSA | 1)Computational problem- Discrete Logarithm Problem<br>2)Encryption key size- No Encryption key in DSA<br>3 )Application- DSA is used for digital signature. | 1)Drawback-<br>a) Vulnerable DSS design.<br>b) The second complaint regards the size of prime 512 bits.<br>2) Attacks-In known message attack, attacker given valid signatures for many types of messages which is known by attacker but not chosen by attacker. In an adaptive chosen message attack, the attacker first understands and learns signatures on arbitrary messages of the attacker's needs. |
| 4 | NTRU Encrypt | 1)Computational problem- Closest vector problem in lattices<br>2) Encryption key size- The table shows the required sizes of NTRU key strength. NTRU 251, NTRU 347 and NTRU 503 provide roughly equivalent security to RSA 1024, 2048 and 4096. Key Strength Pre-master Secret Size NTRU 25 120 bytes, 347 32 bytes and 503 48 Bytes3)<br>Application- Digital signature | 1) Drawback-"Shor's algorithm" is quantum algorithm used to integer factorization and would be able to break ECC or RSA of any practical size in negligible time period. So NTRU's security is slightly vulnerable through quantum computers.<br>2) Attacks- Security issues-Elementary (why N should be prime), Standard(men-in-middle attack), Implementation(choosing-cipher attack, hashing and padding issues) |
| 5 | ElGamal | 1)Computational problem- Discrete logarithm problem<br>2 )Encryption key size-512 bits.<br>3) Application- It used in PGP Key exchange, Authentication, encryption and decryption of small messages. | 1) Drawback-The encrypted message becomes very big in size, it becomes the twice the size of original message m.ElGamal's need large amount of space to store the three part public key and two part encrypted message.<br>2) Attacks- Low-Modulus attack, Known-plaintext attack |

| | | | |
|---|---|---|---|
| 6 | Rabin cryptosystem | 1)Computational problem- The complexity of System is same level as factoring large number n into 2 primes<br>2) Encryption key size-1024 bit.<br>3) Application- The Rabin cryptosystem can also be used to create a signature through exploiting inverse mapping. | 1) Drawback-The problem is its decrypt into four possible messages.<br>2) Attacks- CCA attack. Algebraic attack The Hastad Attack. Algebraic Attack. Desmedt Odlyzko Attack. Related Message attack. |
| 7 | ECC | 1)Computational problem- Discrete logarithmic problem<br>2) Encryption key size-160 bits<br>3) Application- Digital signature, key exchange, Authentication. | 1) Drawback- It increase the size of encrypted message/It is more complex than RSA<br>2) Attacks- General-DL attack by SPH, Software attack estimator, Explicit attack(Hardware attack estimate, Anomalous attack, |

## VI. CONCLUSION

The motive of this paper has to extend the E-commerce security through PGP with dual signature. Our proposed model focused on some point like the SET security and its cost and the time consumption. In our model, some of the algorithms are removed like DES. It generates many cycles and takes too much time to process the data in the verification but we used RSA algorithm which is most secure and less time consuming. It will control all the encryption and the decryption with the help of private and public key of sender and the receiver. In this paper, we also analyzed some important algorithms which is used in Internet banking, ATM machine, biometric system, digital signature, key exchange etc.

## REFERENCES


[1] Yu Xin, Xia Ming Ping &Bai Yu, "Research on the Security Model for E-business Process Management," Published in IEEE computer society, 2008, pp.369-371.

[2] LI Yuewen, "Research on E-commerce Secure Technology," Published in IEEE computer society, 2010.

[3] Yuanqiao Wen, Chunhui Zhou, Kezhong Liu, "Research on E-commerce Security Issues," published in International Seminar on Business and Information Management, 2008, pp.186-189.

[4] He Y, Jiang Jian, "E-commerce Security Payment System Research and Implementation," Published in IEEE Computer Society, 2010, pp.559-562.

[5] [online] http://www.ecommerce-digest.com/7_8.html. (Accessed 23 Sept 2013).

[6] Geng Li-xiao, Zeng Zhen-xiang, Zhang Xue-min, "Research on PKI based E-commerce security Mechanism," Published in IEEE conference, 2007, pp.3545-3547.

[7] [online] http://ijns.femto.com.tw/contents/ijns-v11-n3/ijns-2010-v11-n3-p121-127.pdf (Accessed 20 Sept 2013).

[8] [online] http://www.ijcaonline.org/icvci/number9/icvci1377.pdf. (Accessed 26 Sept 2013).

[9] Dai Wei, Ji Wei, "Research on the Security of an improved E-commerce Model," Published in International Conference on E-Business and E-Government of IEEE, 2010, pp. 2534-2537.

[10] E-commerce and Development Report By United Nations Conference on Trade and Development, 2002.

[11] Christoph Kern, Anita Kesavan, and NeilDaswani, Foundations of Security: What Every Programmer Needs to Know.

[12] Richard Gay, Alan Charlesworth, Rita Esen, Online Marketing: A Customer-Led Approach, 2007.

[13] Seyyed Mohammad Reza Farshchi, Study of Security Issues on Traditional and New Generation ofE-commerce Model IPCSIT vol.9, IACSIT Press, Singapore, 2011.

[14] MohanadHalaweh, Security Perception in E-commerce: Conflict between Customer and Organizational Perspectives, Computer Science and Information Technology, ISBN 978-83-60810-14-9. 2008, pp. 443 – 449.

[15] ThulasimaniLakshmanan and MadheswaranMuthusamy, "A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes" The International Arab Journal of Information Technology, Vol. 9, No. 3, 2012.

[16] Dr. Nada M. A. Al-Slamy, "E-commerce security" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, 2008.

[17] Rhavani Chris Clifton, "Directions for Web and E-commerce Applications Security" IEEE, ISSN 0-7695-1269-0101 1- 2001, 2001.

[18] Jones, Privacy and Security Issues in E-commerce, New Economy Handbook.

[19] Co. John Daly, Roseann Day, and Charles Kolodgy, Secure ecommerce Transactions The Volume, the Requirements, Path to a Solution An IDC White Paper Sponsored by ValiCert.

[20] ShaziaYasin., "Cryptography Based E-commerce Security: A Review" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, 2012.

[21] Randy C. Marchany, "E-commerce Security Issues" Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.

[22] Dr. Qingxiong Ma., A Review of Emerging Technology Trends in E-commerce, International Technology Management Review Volume 1 Number 2, 2008.

[23] Deffiehellmen[online], www.ijcta.com/documents/volumes/vol3issue4/ijcta2012030402.pdf+&cd=5&hl=en&ct=clnk&gl=in (Accessed 09 November 2013).

[24] NTRU [online] http://tools.ietf.org/html/draft-ietf-tls-ntru-00/, (Accessed 14 Sept 2013).

[25] NTRU [online] https://github.com/NTRUOpenSourceProject/ntru-crypto/blob/master/README.md (Accessed 17 Oct 2013).

[26] Elgamal[online] http://www.iusmentis.com/technology/encryption/elgamal/ (Accessed 14 Sept 2013).

[27] Elgamal-[online] http://webcache.googleusercontent.com/search?q=cache:9ZLPbHQuArsJ:www.morris.umn.edu/academic/math/Ma4901/Sp2010/Prop/Missy-Helgeson prop.pdf+&cd=6&hl=en&ct=clnk&gl=in (Accessed 14 Sept 2013).

[28] Digitalsignature [online] http://simple.wikipedia.org/wiki/Digital_signature (Accessed 12 Sept 2013).

[29] [online] http://Programmingpraxis.com/2010/11/22/rabins-cryptosystem (Accessed 5Sept 2013).

[30] [online] https://www.google.co.in/?gws_rd=cr&ei=fzYzUtqAonZrQfUyIDICA#q=use+of+rabin+cryptosystem (Accessed 13Sept 2013).