IJCSET |October 2012 | Vol 2, Issue 10, 1438-1441 www.ijcset.net | ISSN:2231-0711

E-Commerce Security using New Public Key Algorithm based on Block Cipher

[1]Prakash Kuppuswamy, [2] Dr. Gunaseelan, [3]Peer Mohammed

[1]*Department of Computer Engineering & Networks,*
Jazan University, KSA
[2,3] *Department of Computer Science,*
Jazan University, KSA

[1]varshiniprakash@rediffmail.com, kpmvellore@yahoomail.com

***Abstract*-Now a day's, E-Commerce business is very much needed for the individuals and concern. On-line business increases information sharing, a concern regarding the exchange of money securely and conveniently over the internet increases. Therefore, security is a necessity in an e-commerce transaction. The requirements for securing e-commerce transaction are privacy, authentication, integrity maintenance and non-repudiation. These are the crucial and significant issues in recent times for trade which are transacted over the internet through e-commerce channels. The efficiency of the security methods are measured and such efficiency increases as we combined more security methods with each other. A new method of security is suggested which is a based on block cipher algorithm. Block cipher algorithm used until symmetric algorithm, this is the first time we are applying in e-commerce business as a Public Key Infrastructures (PKI). The concept of this new e-commerce securing algorithm is based on modular 37.**

***Keywords*- E-commerce, Trusted Third Party (TTP), Private Key and symmetric key, Public key or Asymmetric key**

I. INTRODUCTION

Electronic Commerce (E-Commerce) is a general concept which covers any form of business transaction or information exchange executed using information and communication technologies (ICT's). E-Commerce includes electronic trading of goods, services and electronic material e-Commerce systems include commercial transactions on the Internet but their scope is much wider than this, for example, Electronic Market, Electronic Data Exchange (EDI) and Internet Commerce. It is the process of buying, sailing or exchanging products, services, and information through computer networks. It also pertains to "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact [13]. Though popular, this definition is not comprehensive enough to capture recent developments in this new and revolutionary business phenomenon. Emmanuel Lallana el al. proposed the definition of E-commerce. It is the use of electronic communications and digital information processing technology in business transactions to create, transform, and redefine relationships for value creation between or among organizations, and between organizations and individuals [14]. The three primary processes are enhanced in e-business are Production processes, Customer-focused processes and Internal management processes.

For small businesses, the best way to grow is to reach new customers. As such, the Internet presents with a tremendous opportunity. Not only can it extend the sales reach to a world of new customers in a way that was once unimaginable, but it can also be considered a great equalizer because it levels the playing field against larger competitors. Unfortunately, many small business owners are hesitant to start selling on the Internet due to concerns about costs and technology. Online transactions can be as secure, if not more secure than payments made by mail or in a store; and fraud can be avoided if consumers understand a few simple steps they should take when they enter the online marketplace [10].

The main advantages of this new trading methods is its rapidity and the two teams of the trading process can make the contract easily and in short given period of time[4].

The remainder of the paper is organized as follows: In Section 2, it has been described in brief the relative researches in public key security algorithm based on block cipher in the e-commerce industry. In Section 3 provides the method and detailed steps on the proposed public key security algorithm. An implementation and the illustration are demonstrated in Section 4. In Section 5, the design of the experimental results and performance analysis is discussed; finally, in Section6 offers conclusions.

II. RELATED WORKS

Security issues are an important topic in e-commerce. The protection in the security of e-commerce system and data are core research area. Several research papers have been analysed the security aspects in E-commerce. The e-commerce software packages are also work with Secure Electronic Transfer (SET) or Secure Socket Layer (SSL) technologies for encryption of data transmissions. SSL protocol allows the transmission of encrypted data across the Internet by running THE above the traditional TCP/IP protocols. SSL protects the communication between a client and a server and provides authentication to both parties to secure communication. SSL provides point to point security. Storage of sensitive data in repositories or databases makes e-commerce system ideal target [5].

Hackers seem any target to data repositories due to availability of data on a single place. Ecommerce has become a critical component in any business competitive strategy. Organizations are gaining opportunities and benefits such as global presence and improved

competitiveness from web-based e-commerce. Algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature [6].

The different methods and algorithms are used in order to increase the E-commerce security are listed as below.

Sung W. T. et al, proposed an adaptive secure protocol to support secure e-commerce transactions. This protocol is dynamically adapted the security level which is based on the nature and sensitivity of the interactions among the participants. The security class is incorporated the security level of cryptographic techniques with a degree of information sensitivity. It forms implements Adaptive Secure Protocol and measures the performance of Adaptive Secure Protocol. The experimental result shows that it provides ecommerce transactions with high quality of security service [7].

Ganesan R and K. Vivekanandan in the year 2009, proposed a software implementation of a digital envelope for a secure e-commerce channel. It combines the hashing algorithm of MD5 for integrity, the symmetric key algorithm of AES and the asymmetric key algorithm of Hyper Elliptic Curve Cryptography (HECC). The algorithm is tested for various sizes of files. The digital envelope is to combine AES and HECC which is better alternative security mechanism for the secure e-commerce channel for achieve Privacy, Authentication, Integrity maintenance and Non-Repudiation [8].

H. K. Pathak and Manju Sanghi in the 2010, proposed a new public key cryptosystem and Key Exchange Protocol. It is based on the generalization of discrete logarithm using Non-abelian group of block upper triangular matrices of higher order. The security of both the systems relies on the difficulty of discrete logarithms over finite fields [9]. The proposed cryptosystem is efficient in producing keys of large sizes without the need of large primes.

The new algorithm based on Hill cipher's or linear block cipher for e-commerce industry. The block cipher is susceptible to cryptanalysis and unusable in practice, but still serves an important pedagogical role in both cryptology and linear algebra. In general, the key space of the Hill cipher is precisely GL(r, Z_m) the group of r x r matrices that are invertible over Z_m for a predetermined modulus m [1].

III. PROPOSED METHOD

One of the effective tools for ensuring the safety of e-commerce transactions is the Public Key Infrastructures (PKI). It combines the digital signature and Certificate Authority (CA), which can be a public or a private-- a business is acted as its own CA is private while a public one offers its services to businesses and provides secure key management.

E-Commerce Security focuses on the data confidentiality issue. Although security mechanisms, such as Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) have been adopted in websites, catastrophic events the confidential data in the E-commerce are revealed happened more than once. The proposed method is very easy to adopt the coding of advanced language. Also it is very safe enough on the other side; Hashing, MD5, and RSA based algorithms are consumes a large amount of computing resources.

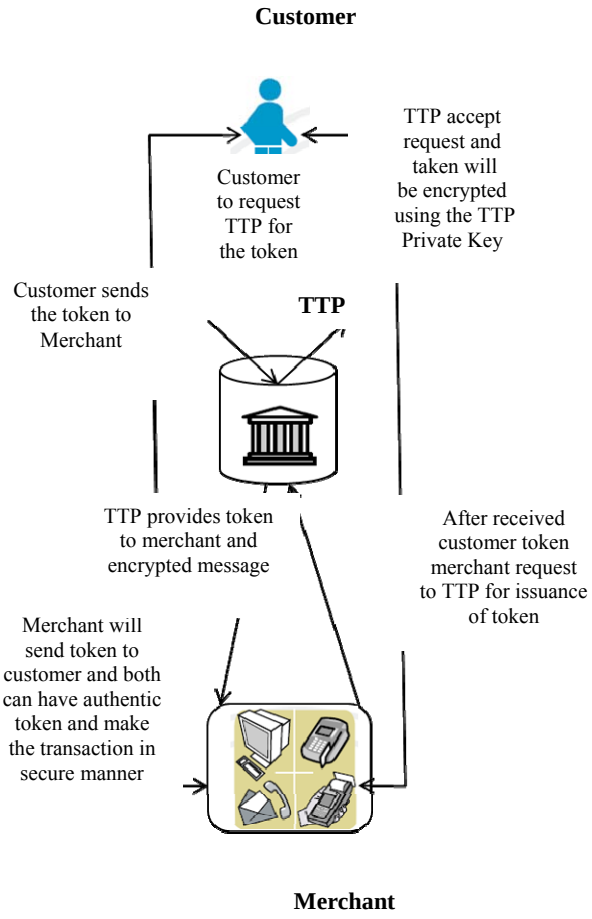

Fig.1 E-commerce transaction between Customer, Merchant and TTP

In the e-commerce industry, three parties are involved in all transactions. Firstly, the customer, secondly Trusted Third Party (TTP) and lastly the merchant. For the above transactions, we are going to apply the new public key algorithm based on the linear block cipher.

i) Customer request to TTP for token consider as a message or plain text.
ii) Randomly select linear matrix and multiply with PT as encrypted one.

A. *Square matrix:*

In the square matrix, the orders are equal, that is rows (m) and columns (n) are equal (m = n). A square matrix A = [a_{ij}] of order n × n. The components a_{ii} form the main diagonal, which runs from top left to bottom right. The cross diagonal runs from the bottom left to upper right. In the proposed linear block algorithm, it has been chosen the square matrix for the purpose of perfect calculation of determinant of matrix and invertible matrix, which we can use at the time of encrypting the plain text ….…..…..…..*(1)*

B. *Determinant of matrix:*

Every square matrix can be assigned to a real number, which is called the determinant of the matrix. If A=(a*ij*) is a

square matrix of order, then the determinant of 'A' is denoted by |A| and is defined as |A| =ϵ a_{ij} x c_{ij}, I = 1 or 2 or …….n ….....*(2)*

iii) Customer send encrypted PT to Merchant
iv) Request for an issuance of Token to TTP
v) TTP provide private key for decryption

C. Minor of an element:

The minor of an element a_{ij} is denoted by M_{ij} and is obtained by deleting the i^{th} row and j^{th} column in which the particular element a_{ij} occurred.

The resultant matrix will be a square matrix….....*(3)*

D. Inverse of a matrix:

An inverse of a function, usually written as f-1(x), is a reflection of the original function, f(x), around the line y = x. Basically, every x value is changed to a y value and every y value is change to an x value…….....……..*(4)*

E. Adjoint of a Matrix:

The adjoint of a square matrix 'A' is denoted by adj(A) and is obtained by taking the transpose of the cofactor matrix A. Therefore adj A =(c_{ij})T…….....……*(5)*

F. Modular function:

(a +b) mod n = [(a mod n) + (b mod n)] mod n….....….*(6)*
(a-b) mod n = [(a mod n) – (b mod n)] mod n…...…….*(7)*
(a * b) mod n = [(a mod n) x (b mod n)] mod n .....…..*(8)*

Now customer has one key issued by the TTP and Merchant that has one key for decryption. The customer key is a square matrix issued by the Trusted Third Party and the inverse of square matrix is Merchant key.

IV. IMPLEMENTATION

In order to provide quick and simple encryption/decryption, the bits size of the secret key has to be chosen effectively. For encrypting small amount of data, there should not be any overhead to the encrypting system as well as there should not be any compromise on the security level. Thus an optimized size of 64 bits is chosen.

i) Request for the token from TTP

Assume, the customer sending message about product and asking TTP's token

Consider here product or message or plain text is 'INDIA' i.e equivalent to 9,14,4,9,1

ii) TTP calculating customer message with key

Here we are selecting the key as

$$e=\begin{pmatrix} 2 & 1 \\ 4 & 5 \end{pmatrix}$$

Invertible is (2 * 5) – (1 *4) = 6 is no common faction in Z37. Selected invertible matrix is 2x2, so make a message as a 2 blocks i.e (9,14), (4,9), (1, 37) Note 37 used for blank space

Now we are calculating message with selected key i.e 'e'Customer Token = (m * e) mod 37

$$\begin{pmatrix} 9 \\ 14 \end{pmatrix} * \begin{pmatrix} 2 & 1 \\ 4 & 5 \end{pmatrix} \text{mod} 37 = \begin{pmatrix} 18+14 \\ 36+70 \end{pmatrix} \text{mod } 37 = \begin{pmatrix} 32 \\ 32 \end{pmatrix}$$

Therefore message (9,14,4,9,1,37) will becomes (32,32,17,24,2,4)

iii) Customer send the encrypted message i.e (32,32,17,24,2,4) to Merchant

iv) TTP generate the private key i.e inverse of 'e' is known as e^{-1}

C11 $[-1]^{1+1}$ x [5] = $[-1]^2$ x [4] = 5
C12 $[-1]^{1+2}$ x [4] = $[-1]^3$ x [3] = -4
C21 $[-1]^{2+1}$ x [1] = $[-1]^3$ x [1] = -1
C22 $[-1]^{2+2}$ x [2] = $[-1]^4$ x [2] = 2

$$e^{-1} = -6 * \begin{pmatrix} 5 & -1 \\ -4 & 2 \end{pmatrix} \text{ mod } 37 = \begin{pmatrix} 7 & 6 \\ 24 & 25 \end{pmatrix}$$

v) Now merchant will encrypt the customer message using private key issued by the TTP (32,32,17,24,2,4)

$$\begin{pmatrix} 32 \\ 32 \end{pmatrix} * \begin{pmatrix} 7 & 6 \\ 24 & 25 \end{pmatrix} \text{Mod } 37 = \begin{pmatrix} 9 \\ 14 \end{pmatrix}$$

Finally merchant will receive customer message 9,14,4,9,1,0 i.e (INDIA)

V. RESULT ANALYSIS

The proposed method in E-commerce security which is the combination of the linear block cipher, Public Key Infrastructures (PKI), a digital signature, Certificate Authority (CA) and hash algorithm. To secure transaction application, it generates tokens that are used by customer and merchant. Tokens have the different attributes like serial number, subject, hash code, issue name and public key. Customer and merchant first verify the authenticity of tokens. Then perform communication in a secure domain shown in figure 1. Application encodes the package to transmit over the network. Then, it decodes at the receiving side to achieve original data. Application also provides authentication and integrity checks to customer and merchant packages to protect against threats.

The algorithm executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core. The programs implemented using Microsoft Visual Studio 2008 (C#). It is tested with three messages and with different in length (100, 200, 300 characters).

TABLE I
COMPARISON TABLE

Message length	MD5	Hashing	SHA1 HMAC	New algorithm
100 Char.	0.03	0.04	0.04	0.03
200 Char.	0.05	0.07	0.06	0.05
300 Char.	0.07	0.09	0.08	0.07

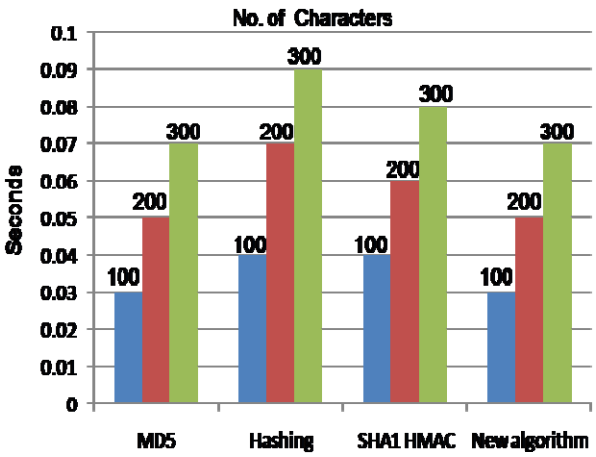

Fig.2 Comparison of e-commerce algorithm

VI. Conclusion

Satisfying security requirements is one of the most important goals for e-commerce system security designers. In the proposed paper, it has been designed for securing e-commerce transaction by using public key algorithm which is based on linear block cipher technique. The proposed method is increase the performance of E-commerce security rabidly. Also it will ensure the confidentiality, integrity and authentication. The AES algorithm provides confidentiality, the MD5 hash function provides the integrity and the modification of Diffie-Hellman will ensure the authentication. It has been tested the algorithm for various sizes of messages and parameters. The experimental results shows that the proposed method is improved the interacting performance, while providing high quality of security service for desired e-commerce transactions.

Several points can be concluded from the experimental results. It has been concluded that the proposed method consumes least encryption time (computing time) and others has taken maximum time in encryption for same amount of the data.

It can notice that as more guards added for any information system, then more secure system is resulted. It is clear from percent of efficiency of security methods shown in the table 1. So combining more security methods with each other may increase efficiency but may increase costs.

VII. Acknowledgement

The authors are extremely express gratitude to Dr. Omar Sayed Al-Mushayt, College Dean and Dr. Saeed Q Y Al-Khalidi, Vice Dean, College of Computer Science and Information Systems, JAZAN University, Kingdom of Saudi Arabia for having noble and continuous encouragement to complete this research. The special thanks also to the University President, JAZAN University, Kingdom of Saudi Arabia for inspiration and persistent support directly or indirectly for the completion of this research.

References

[1] John C. Bowman, Math 422 Coding Theory & Cryptography, University of Alberta, Edmonton, Canada.

[2] Prakash Kuppuswamy & Dr.C. Chandrasekar, Enrichment of Security through cryptographic public key algorithm based on block cipher, IJCSE, Vol. 2 No. 3 Jun-Jul 2011.

[3] Zorayda Ruth Andam ,e-commerce & e-business, 2000,Harvard Business School Press.

[4] Ashraf Abdel-Karim Abu-Ein, Hazem (Moh'd Said) Hatamleh,Ahmed A.M. Sharadqeh, As'ad Mahmoud Alnaser and Omar AlHeyasat, E-commerce: Security and applications, American Journal of Applied Sciences, 2012, 9 (11).

[5] Anup K. Ghosh "E-Commerce security: No Silver Bullet" IFIP Conference Proceedings Vol. 142, P: 3 – 16, 1998.

[6] P. C. O. A.J Menezes, and S.A. Vanstone, Handbook of Applied Cryptography: CRC Press, 1996.

[7] Sung W. T., Yugyung L., et al, Design and Evaluation of Adaptive Secure Protocol for E-Commerce, IEEE, 2005.

[8] Ganesan R. , Dr. Vivekanandan K., A Novel Hybrid Security Model for E-Commerce Channel, 2009 IEEE.

[9] Pathak H. K. , Manju S. , Public key cryptosystem and a key exchange protocol using tools of non-abelian group , (IJCSE) International Journal on Computer Science and Engineering , Vol. 02, No. 04, 2010 .

[10] www.authroize.com a cyber source solution, e-commerce, getting started.

[11] P.Ratnasingham, Trust in Web-Based Electronic Commerce Security, Information Management and Computer Security, vol. 6, no. 4, no. pp. 162-166, 1998.

[12] L. X. QIN Zhiguang, GAO Rong, A survey of E-commerce Security, Electronic Science and Technology of China vol. 2, no. 3, Sept 2004.

[13] Arun Bakshi el al. Impact of E-commerce on customers, employees, suppliers, distributors and competitors, Global Journal of Enterprise Information Systems, Vol. 1, Issue 2, July-Dec. 2009.

[14] Emmanuel Lallana, Rudy Quimbo, Zorayda RuthAndam, ePrimer: An Introduction to eCommerce (Philippines: DAI-AGILE, 2000)

Prakash Kuppuswamy Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar proceeding in 'Dravidian University'. He has been published few journals/Technical papers and participated many international conference in Rep. of Maldives, Libya and Ethiopia. His research area Cryptography, Bio-informatics, Network algorithms etc.,

Dr. D. Gunaseelan is an Associate Professor, Research Coordinator & Senior advisor for NCAAA and ABET accreditations in the College of Computer Science & Information Systems, Jazan University, Kingdom of Saudi Arabia. He has more than 25 years of teaching, research and administrative experiences in India, Oman and the KSA. He published more than 30 National & International papers and more than 20 National & International journal papers. His research interest includes Data Mining, Knowledge Discovery in Database, Biometrics, Data Compression.

Peer Mohamed Appa Lecturer, Computer Science Department in Jazan University, KSA. He has been published few journals/Technical papers and participated many national and international conference. His research area Cryptography, Bio-informatics, Network algorithms etc.,