ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

APPLYING SECURITY TO E-COMMERCE APPLICATIONS

Noureen Khatoon[1], P.M.Durai Raj Vincent[2]
[1]M.Tech (IT), VIT University, Vellore.
[2]Associate Professor, School of Information Technology and Engineering, VIT University.

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract

E-commerce has presented a different way of doing transactions all above the world using the internet. The success of e-commerce depends greatly on how its information technology is used. Over the years the rate at which e-commerce sensitive information is sent over the internet and network has increased drastically. It is for this reason that everyone wants to ensure that its e-commerce information is secured. There is aneed for e-commerce information transmitted via the internet and computer networks to be protected. There is substantial growth in the areas of credit card fraud and identity theft the exchange of some form of money for goods and services over the Internet but today, Internet is an insecure and unreliable media. Because the internet is a public network with thousands of millions of users. Amongst users are crackers or hackers that carry out the credit card fraud and identity theft in numerous ways facilitated by poor internet security; a concern regarding the exchange of money securely and conveniently over the internet increases. In this paper describes using with military applications mostly used in bordered areas equipments through e-commerce and the way of generating a public/private RSA key pair from a passphrase to overcome these problems. Although the paper's focus is on the generation of RSA keys, the process can be applied to any cryptosystem (symmetric or asymmetric) which relies on random data for generating the 100 keys and providing secure.

Introduction

E-commerce or electronic commerce is dealing in product or services conducted via computer networks such as the internet. It is measured to be the sales aspect of e-business consisting of the exchange of data to facilitate the financing, payment and security of business transactions. E-commerce refers to a varied range of online business activities for

products and services. High degree of confidentiality needed in authenticity and privacy of such transactions can be difficult

Tosustain where they are interchanged over an unsecured public network such as the Internet. E-commerce also belongs to any form of business transaction in which the parties interrelate electronically rather than by physical exchanges or direct physical contact. A security independent is aninfluence to security that a system is intended to achieve. Security has emerged as an increasingly important matter in the development and success of an E-commerce organization. Gaining contact to sensitive information and replay are some common threats that hackers execute to E-commerce systems. Privacy has become a major concern for consumers with the rise of identity theft and impersonation and any apprehension for consumers must be treated as themain concern for e-Commerce providers.

E-commerce security has its own particular gradations and is one of the highest visible security components that affect the end user through their day-to-day payment interaction with business. E-commerce shares security apprehensions with other technologies in the ground. Privacy concerns have been found, revealing a lack of trust in a multiplicity of contexts, including commerce, electronic health records, e-recruitment technology and social networking, and this has directly affects the users. Security is one of the primary and continuing concerns that restrict customers and organizations engaged with e-commerce. The e-commerce industry is slowly addressing security matters on their internal networks. There are guidelines for securing systems and networks existing for the e-commerce systems personnel to recite and implement. The data are very important to the parties involved in e-commerce, so we must declare their security completely. We need an e-payment system that would not only provide secure payments but should also have properties like an online customer and merchant authentication, unforgivable resistant of transaction authorization by the customer both to the merchant and the bank, privacy of customer and transaction data .

The asymmetric key cryptosystem includes the use of two different but related keys namely, the public key and the private key. Plaintext is converted to ciphertext using the public key. This process is known as encryption which is performed by the sender. On the other hand, the deciphering of the cipher text is performed by making use of the private key. This process is Known as decryption and is performed by the receiver. Only the receiver possesses the information of the private key. In order to maintain the confidentiality of the private key, the public key is disclosed to the public. The public key is used for authentication to confirm that the message is coming from the intended sender. Public key

cryptosystem also makes sure confidentiality. Only the receiver's private key can decipher the ciphertext originating from the sender. Communication of messages can be done in a confident manner since knowledge of the public key is not compulsory to decrypt the cipher text. When a military person buys the products through e-commerce it should be more secure and confidentially should be maintained. The products which are brought through online from the user said to use the public key. Whereas whatever bank transaction is done is keep secret by using private key with random data generation of up to 100 keys. By using public and private keys data is becomes more secure.

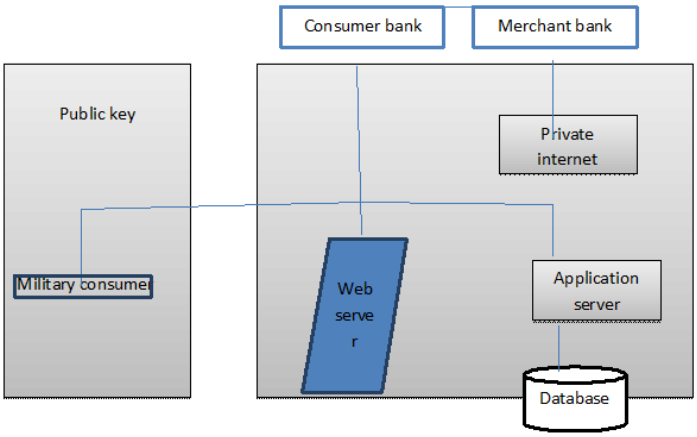

Figure 1: Structure of E-Commerce.

Literature survey

Elaine L. Render August et.al [1] RSA Cryptosystem play an important role in credit card payment application, email application and remote login for network submission by allowing security and authentication. Without using RSA cryptosystem, the growth of theinternet is not possible because the foremost goal of theuser is security. There are various attacks which are carried out and determined to recognize the effectiveness of the system. Before 15 years, Michael Wiener described the continued fraction attack which is very useful for the accomplishment of an error. Nanehkaran [2] electronic commerce is supporting of customers, supplying of services and commodities, aportion of commercial information, manages business transactions and maintaining of thebond between suppliers, customers, and vendors by devices of telecommunication networks. In this research, article paper is to theevaluation of principles, definitions, history, frameworks, steps, models, advantages, blocks and limitations of electronic commerce. Satyendra Nath Mandal & Kumarjit Banerjee, Biswajit Maiti and J. Palchaudhury et.al [3] to provide the security and privacy to digital data, a most important schematic RSA cryptosystem is used. RSA algorithm is based on two large prime numbers. Due to disreputable on two large prime number it has a problem to handling quantity because to handle large prime number is a

very time taken procedure. This paper, a new technology named as "modify trial division technique" is used to implement RSA algorithm for large number due answer the problem of arrange of compiler. Al-Slamy, N.M.A. [4] E-commerce is a new creation generated from economy it makes the life informal for bidders and buyers. Both can sign in massive projects or transactions without making any kind of effort (you control everything from your home); However, there is another adjacent making the best of efforts to disturb, handle or hack the e-commerce transaction. So how can we protect it? If we succeed in the security, what are ways that could help the organization to gain the consumer's trust.

Z. Durif [5] to impose some challenges to executives. People are always distrusted to the internet and banking businesses are theencountering challenge of security and information privacy assurance to overcome this distrust. They should also provide confirmation of transactions to prevent unauthorized transactions when complex authentication information is thieved. In this paper, an integrated service providing amodel for e-banking is proposed that combining centralized management, simplicity, and reduced faults, and deliver more security using transaction support process.

Vibhor Mehrotra & Prakash Singh Rana et.al [6] this paper represents a new algorithm program which contacts the RSA scheme. The main of suggested this algorithm is to theinvention the private key of RSA scheme and factoring the segments which are based on public RSA scheme. This algorithm plays an important part in reducing running time and delivers more effectiveness in theassociation of that algorithm which are already subsisting.

Proposed work:

In proposed work describes using with military applications mostly used in bordered areas equipments through e-commerce and the way of generating a public/private RSA key pair from a passphrase to overcome these problems. Although the paper's focus is on the generation of RSA keys, the process can be applied to any cryptosystem (symmetric or asymmetric) which relies on random data for generating the 100 keys and providing secure.

User Interface Design:

- In this module,user has to produce an account for only allowing right persons to contact the resources. All the information will be stored in a database which is placed in server. If he entered accurate username and password then he will be able to contact the public cloud.
- Logging in is usually used to enter a specific page, which trespassers cannot see. Once the consumer is logged in, the login token could be used to track what actions the manager has taken although connected to the site. Logging

out may be performed unambiguously by the user taking some achievement, such as entering the suitable command, or clicking a website link labeled as such. It can also be through implicitly, such as by the user powering off his or her terminal, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period.

- In the case of websites that use cookies to pathway sessions, when the user logs out, session-only cookies from that establish will generally be deleted from the user's computer. In addition, the server invalidates any associations with the session, making any sessionhandle in the user's cookie store useless.

Shared Security Services:

In order to reserve privacy, one would like to do things when nobody else could see or disturb him or her. In thecase of an application which can be used in overall life, an attacker can infringe the privacy of users easily by tracking usage antiquity. Suppose that user purchases items such as clothes, food, and medicine several times at a supermarket. The supermarket can get information approximately her tastes, preferences, and health conditions. The collected information could help her to efficiently purchase products; however, it may comprise facts which she does not want others to know such as her health conditions or security questions.

Eavesdropping and Data modulation

The module data can be arbitrary information or regular data depending on the purpose of attackers. Fortunately, the records that is being transmitted can be effortlessly protected from eavesdropping by using confident code. In application, key agreement is performed through public and private key is generated by obtained from results. The user's data is encrypted when it is transmitted through the securecode when an attacker only obtains the encrypted data or public key, and he is unsuccessful to get meaningful data from supermarket.

Security Requirement

- **Data Confidentiality:**

Service provides the message between application with confidentiality and integrity using a key generated done SSE (security element) service. The key generated through SSE and delivers confidentiality and integrity to the communications using generated keys. The three keys created in SCH are used to deliver the confidentiality and integrity of the message.

❖ **Data Integrity:** The transmitted data should be indistinguishable to the source data. It is guaranteed that data is not modulated in the process of transferring user's purchase information PA (public key of user's).

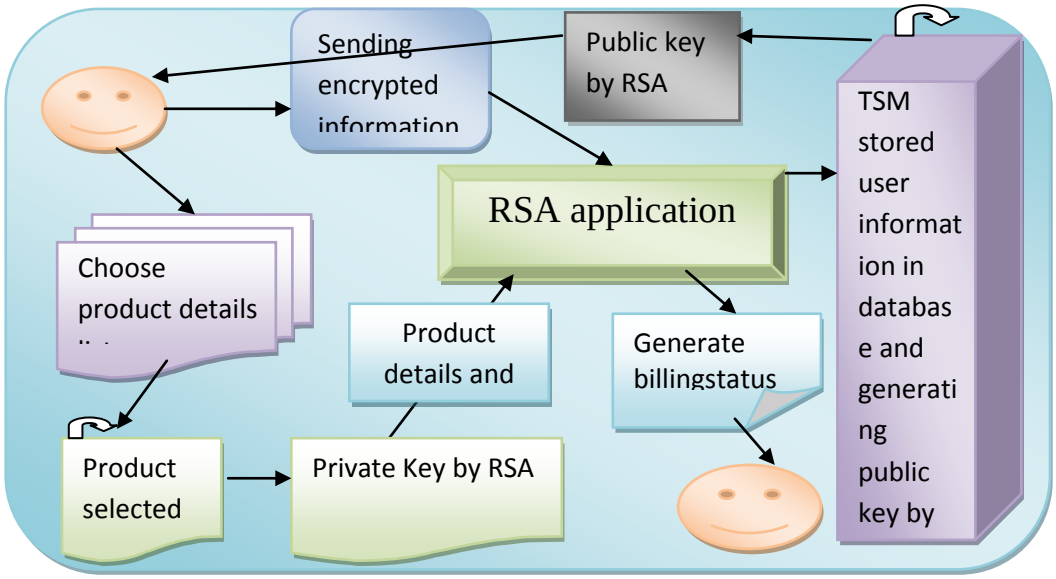

Figure 2: Architecture.

Result and analysis

The term of the software developed is RSA E-commerce Security System (RSA-ESS). The software releases thesending/transfer of encrypted credit card payment information online by a military customer in aninaccessible system and in order to make data more secure. The decryption/use of such payment facts by the bank staff to withdraw from customer account and credit themerchant account during an e-commerce contract is performed through RSA public key and private key. It generated a random key for public and private up to 100 keys. Because of this data is become more protected and confidential. It is organized into numerous subsystems/modules as reflected in the table.

Table:public and private key generations

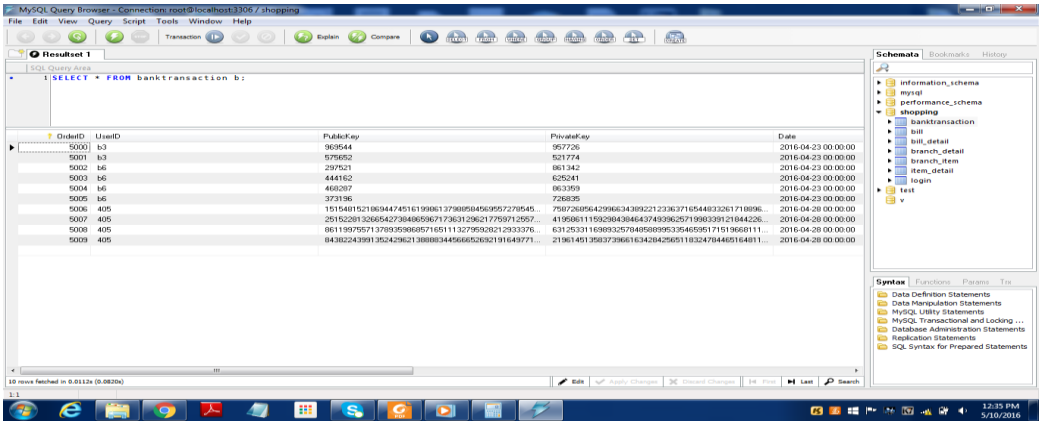

Fig: Results obtained.

Here we have encrypted consumer message "PRODUCT" into figures using private and RSA public key and hence decrypted the keys to finding the final character and the final communication. Here we analyzed with existing DES, 3DES, and AES algorithm to invention out our modified RSA performance.

Performance Metrics

ALGORITHM	SIZE OF KEY	ENCRYPTION AND DECRYPTION (TIMING (100 BITS))
Modified RSA (PUB+PRIV)	2048	10SEC
AES	256 BITS	15SEC
DES	64 BITS	10SEC
3-DES	2^112	20SEC

DES is the old "data encryption standard" from the seventies. Its key size is too short for appropriate security. 3DES is believed to be protected up to at least "2112" security. But it is slow, especially in software. AES is the replacement of DES, and it receives keys of 128, 192 or 256 bits. Our proposed Modified RSA combination of analgorithm based , which has remained using in many application. The key size of RSA algorithm is standard and compatible with all application also encryption/decryption timeof the Modified RSA than comparing to the other algorithms. It is more protected than others using the arrangement of two different algorithms. Table and Figureshow the the performance of DES, 3-DES, AES and our proposed Modified RSA algorithm.

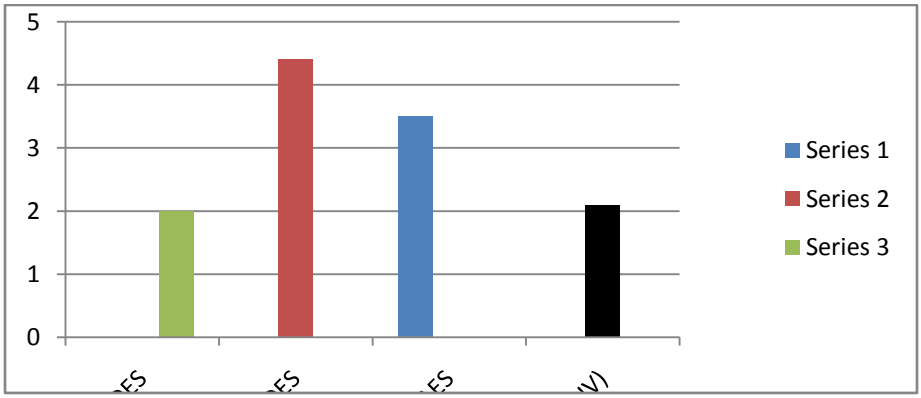

Fig: Comparison chart.

Conclusion and future work

In this paper, we have presented the comprehensive implementation of 1024-bit RSA encryption/decryption algorithm is presented for use in securing e-commerce payment information. This algorithm is implemented using J2EE (JSP, SERVLET). The entire design was tested using J2EE (JSP, SERVLET), MYSQL and IDE (NetBeans) virtual environment tool. On implementation, the encryption and decryption of any information have a secret or private key, which is used for data encryption. For this purpose asymmetric key or public key system is used. Also as keys are randomly generated, it is not conceivable for aphishing site to get aunique share.

For future work, we plan to develop additional high-performance public key crypto blocks. Also, to improve the security of our crypto, we will develop side channel attack resistant techniques in the private and public key cryptoblocks.

References

1. Wiener, M.J., 1990. Cryptanalysis of short RSA secret exponents.*Information Theory, IEEE Transactions on*, *36*(3), pp.553-558.
2. Jhaveri, R.H., Patel, A.D., Parmar, J.D. and Shah, B.I., 2010. MANET routing protocols and wormhole attack against AODV. *International Journal of Computer Science and Network Security*, *10*(4), pp.12-18.
3. Mehrotra, V. and Rana, P.S., 2012. An effective Method for Attack RSA Strategy. *Int. J. Advanced Networking and Applications*, *1363*, pp.1362-1366.
4. Vincent P.M.D.R, Sathiyamoorthy E," A Secured and Time Efficient Electronic Business Framework based on Public Key Cryptography" in International Review on Computers and Software, Vol 9 No 10, pp. 1791-1798, 2014.
5. Wong, J.Y. and Anderson, R.L., Jaesent Inc., 1999. *System for secured credit card transactions on the internet*. U.S. Patent 5,956,699.
6. Sun, H.M., Wu, M.E., Ting, W.C. and Hinek, M.J., 2007. Dual RSA and its security analysis. *Information Theory, IEEE Transactions on*, *53*(8), pp.2922-2933.
7. P.E., Irani, Z., Li, H., Cheng, E.W. and Tse, R.Y., 2001. An empirical analysis of the barriers to implementing e-commerce in small-medium sized construction contractors in the state of Victoria, Australia. *Construction Innovation*, *1*(1), pp.31-41.

8. P.M.Durai Raj Vincent, Sathiyamoorthy E, " A Novel and efficient public key encryption algorithm" International Journal of Information and communication technology, Vol. 9, No. 2, pp 199-211, 2016.
9. Ling, Y., Xiang, Y. and Wang, X., 2007, December. RSA-based secure electronic cash payment system. In *Industrial Engineering and Engineering Management, 2007 IEEE International Conference on* (pp. 1898-1902). IEEE.
10. Vincent P.M.D.R, Sathiyamoorthy E, "A novel and efficient key sharing technique for web applications" in IEEE Fourth International Conference on Computing, Communications and Networking Technologies. 2013.
11. Agnew, G.B., Mullin, R.C., Onyszchuk, I.M. and Vanstone, S.A., 1991. An implementation for a fast public-key cryptosystem. *Journal of CRYPTOLOGY*, *3*(2), pp.63-79.
12. Ambedkar, B.R., Gupta, A., Gautam, P. and Bedi, S.S., 2011, June. An Efficient Method to Factorize the RSA Public Key Encryption. In*Communication Systems and Network Technologies (CSNT), 2011 International Conference on* (pp. 108-111). IEEE.
13. P.M.Durai Raj Vincent "RSA Encryption Algorithm- A survey on its various forms and its security level" International Journal of Pharmacy and Technology, Vol 8 No 2 12230-12240, 2016.