A Model to Secure E-Commerce Transaction using Hybrid Encryption

Devendra Singh Solanki
Research Scholar
Suresh Gyan Vihar University
Jaipur,Rajasthan, India.
Devs.s19@gmail.com

Dr. Savita Shiwani
HOD(Information Technology)
Suresh Gyan Vihar University
Jaipur,Rajasthan, India.
Savitashiwani@gmail.com

***Abstract*— The essential part of e-commerce is its data in the database. The issues associated with the security in the database of traditional e-commerce on the basis of analysis on the process of users registration and retrieving password are explained. Security of e-commerce system by single encryption technique is difficult to ensure. The technologies like asymmetrical encryption and symmetrical encryption were introduced to forward the combining thought to produce a hybrid encryption. The method so developed is used to modify the e-commerce process by which the e-commerce database security is enhanced.**

Index terms:- e- commerce , database security, hybrid encryption ,symmetric encryption, asymmetric encryption

I. INTRODUCTION

E-commerce is an important topic in dealing with the security issues. Its core research area is its way of protecting the security of e-commerce system and data[1]. Transaction records, commercial transactions, user account, market scheme and others are the sensitive financial data and assets in the e-commerce database. The parties involved in e-commerce are needed to be assured of security of their data transactions completely. As in the transactions there are always a threat of third party hack. So we need a secure transaction with maintaining speed and efficiency.

However a simple encryption technology, such as symmetrical encryption or asymmetrical encryption, is very difficult to guarantee the security of network transactions. We must combine both of these and through hybrid encryption we can create a safe, efficient e-commerce transaction mechanism.

II. ENHANCEMENT WITH OLD ONE

HTTP hyper text transfer protocol basically it is an application layer protocol implemented for the transaction. It is a sort of request-response protocol implied over client-server model. While dealing with conventional http protocol it does not deal with any flow or error control mechanism so no such security aspects are there but due to lack of these mechanisms implied it is really fast and efficient.

Now in this research paper we tried to evolve a technique or a methodology which is applies over the HTTP layer to make it secure but side by maintaining the speed of transaction.

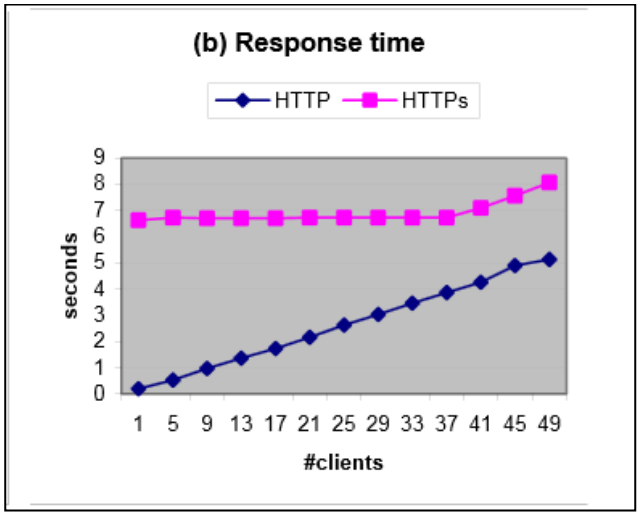


Figure 1: Comparison Between Http&Https

Hence Figuere1[7] this was the conventional comparison chart of the http and https present with their response times. Effectively it is observable that http has less response time as comparison to the https response time.

III. EXISTING ALGORITHM

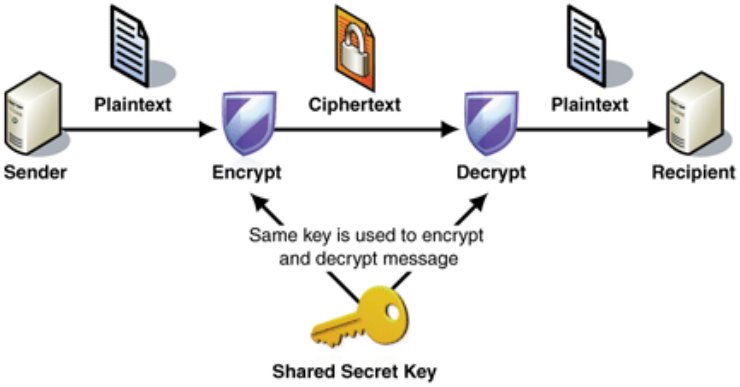


Figure 2 Symmetric Encryption

Figure 2[6] is a schematic diagram of symmetric encryption. The original information will be changed into cipher text since the sending information is encrypted with certain algorithms and keys. While receiving information, cipher text will be restored by decryption of it with same algorithms and keys.

The algorithm proposed by the IBM company is DES (Data Encryption Standard)which is the most extensively used symmetric encryption algorithm [2,3]. DES is a binary data encryption algorithms. Data packet length is

978-1-4799-4190-2/14/$31.00 ©2014 IEEE
Authorized licensed use limited to: Universita di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.

64 bits. Key length is also 64 bits. Eight bits in them are used for parity and effective key length is 56 bits. The basic process is as follows.

Initial permutation: Replace the location of cipher text of 64 bits and get an out-of-order explicit group of 64 bits. It is divided into two paragraphs of 32 bits. L0 and R0 are respectively used to express.

Execute the following iterative transformation to L0 and R0:

$Li = Ri-1$
$Ri := Li-1 \oplus f(Ri-1, Ki)$ $i=1,2,\ldots,16$

Two parts output after the 16th transform exchange order, do inverse initial permutation and then cipher text will result.

Symmetric encryption is fast and highly efficient thus having advantages over other types of encryption. Large amount of data can easily be encrypted using this encryption. The disadvantages are that keys are easily intercepted which will result in the threat to the information as it is transmitted on the network. In symmetric key encryption the main problem is key sharing and it needs to be guaranteed.

B. Asymmetric Encryption Technology

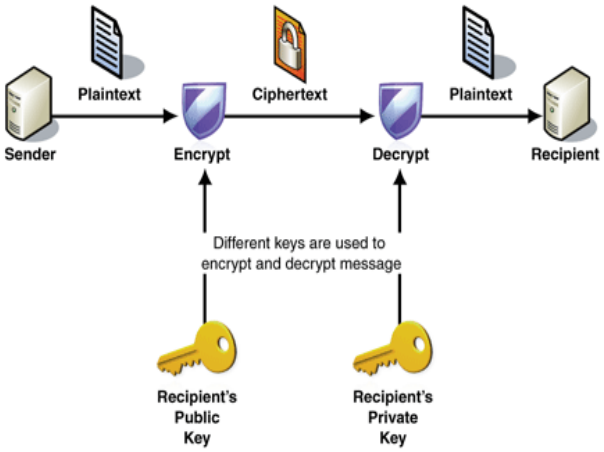


Figure 3 Asymmetric Encryption

Figure: 3 is showing scheme of asymmetric encryption technique. In the asymmetric encryption key pair (private key and public key) is used for encryption and decryption. Here private key is owners key and other is public key Public key is available for everyone. The plain text encrypted by public key can only be decrypted by corresponding private key and vice versa.

Figure 3. The schematic diagram of asymmetric encryption

The best known asymmetric encryption algorithm is the RSA algorithm [4]. The R. Rivest, A. Shamir and L. Adleman proposed the following algorithm from the Massachusetts Institute of Technology. It builds on the basis of the theories of the decomposition of large numbers and detection of prime numbers is the basis for the developed algorithm. The following is the description of the algorithm.

Select confidential large numbers p and q.
Calculate $n = p * q$, $\varphi(n) = (p-1) * (q-1)$.
Here $\varphi(n)$ is Euler function value of n.
Select an integer e, satisfy $1 < e < \varphi(n)$ and e and $\varphi(n)$ are coprime.
Solve equation $d * e = 1 \bmod \varphi(n)$ and calculate d.

Based on the above steps, obtain public key {e,n} and private key {d,n}.here e is encryption index and d is decryption index.

Divide text into packets, the packet value is m and m should be less than n.

Encryption and decryption operations are as follows.

Encryption: $c = m^e \bmod n$
Decryption: $m = c^d \bmod n$

Ease of key management is the major advantage of asymmetric encryption technology. Complexity of encryption algorithm and slow encryption are some of the disadvantages of this algorithm

Asymmetric encryption technique is not good for large amount of data. Therefore in e-commerce based transactions symmetric encryption is good rather than asymmetric encryption. Encrypt data can be considered first and using asymmetric encryption technology to transmit symmetric encryption as key second. So both the techniques with their desired results or undesired results could be merged up together to a more effective technique for encryption technology.

C. Hybrid Encryption Technology

After considering the strengths and weaknesses of symmetric encryption and asymmetric encryption techniques. We can grab advantages of both encryption technique by combining both as Hybrid cryptography.

A: Encrypt plain text using symmetric encryption. As discussed in symmetric encryption Key sharing was the big problem. So here in hybrid encryption we are encrypting key by using public key of B (receiver). By this we can ensure about key sharing because only B knows its asymmetric private key. Even any hacker have get key cipher text he/she cannot decrypt it.

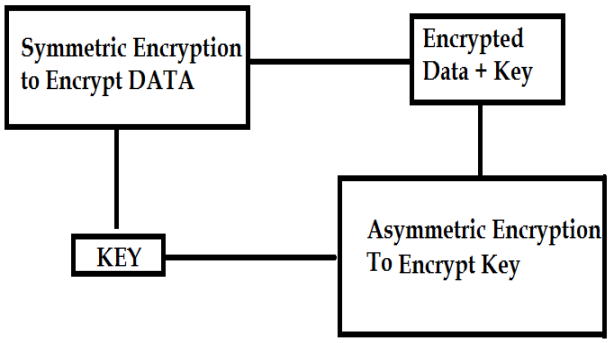
B: At the receiver end, first B will decrypt this cipher text by using its own asymmetric private key and receive the symmetric key, by using symmetric key he/she may untie the cipher text to receive the plain text and receiver finally gets the original information.

We can see that hybrid encryption technique overcomes the key exchange problem and also the large packet encryption problem of asymmetric encryption. So by using hybrid cryptography we can take advantages of both encryption techniques.

IV. Proposed changes in the Algorithm

The Modfied RSA algorithm

978-1-4799-4190-2/14/$31.00 ©2014 IEEE
Authorized licensed use limited to: Universita di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.



In this algorithm we have extremely large number that has two prime factors (similar to RSA) .In addition of this we have used two short range natural numbers in pair of keys. So its name is short range natural number public key algorithm

B. MODRSA Key Generation, Encryption, Decryption Process

1) Key Generation process

- Generate two large random primes, p and q, of approximately equal size such that their product n = p x q is of the required bit length, e.g. 1024 bits.

- Compute n= p x q.

- Compute phi = (p-1) (q-1).

- Choose an integer e, 1 < e < phi, such that gcd (e, phi) = 1. Compute the secret exponent d, 1<d<phi, such that (e x d) mod phi = 1.

- Pick short range natural number u randomly such that u < phi-1. Pick another short range natural number a randomly such that phi > a > u. And compute ua .

- Find d such that- e * d mod ((p-1)*(q-1)) = 1

- The public key is (n,e,ua) and the private key is (d,a,u). The values of p, q, and phi should also be kept secret.

Encrypt Data using DES symmetric algorithm and the key would be input for modified RSA algorithm

2) Encryption process

Sender does the following:-

- Obtains the recipient's public key (n,e,ua)

- Represents the plaintext message as a positive integer m.

- Computes the cipher text c = (m ua)e mod n.

- Sends the cipher text c to recipient.

3) Decryption process Recipient does the following:-

- Uses his private key (d, a, u) to compute m = (v e c) d mod n Where v= u phi-a mod n.

- Extracts the plaintext from the integer representative m.

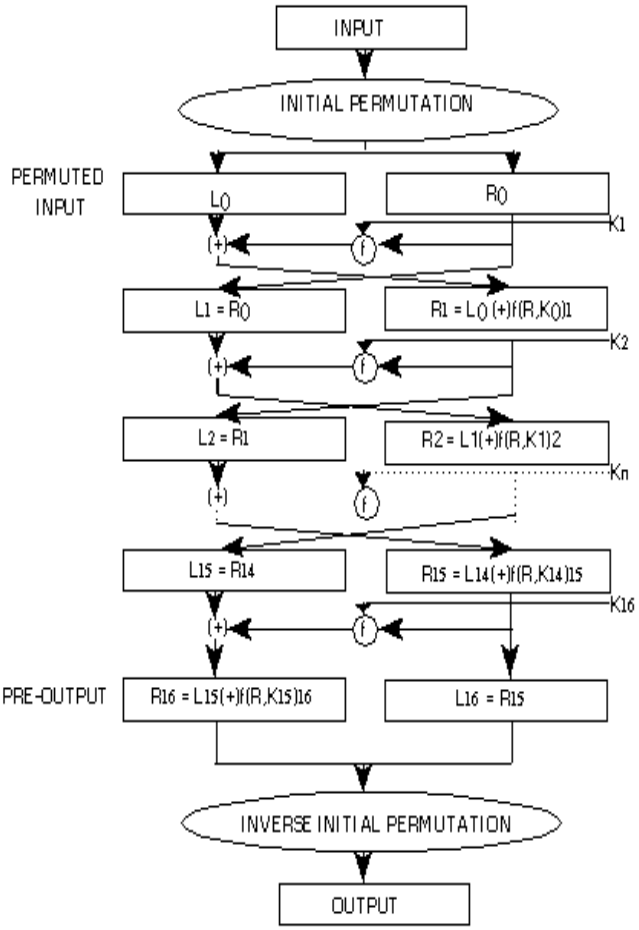


Figure 4: Process of DES algorithm

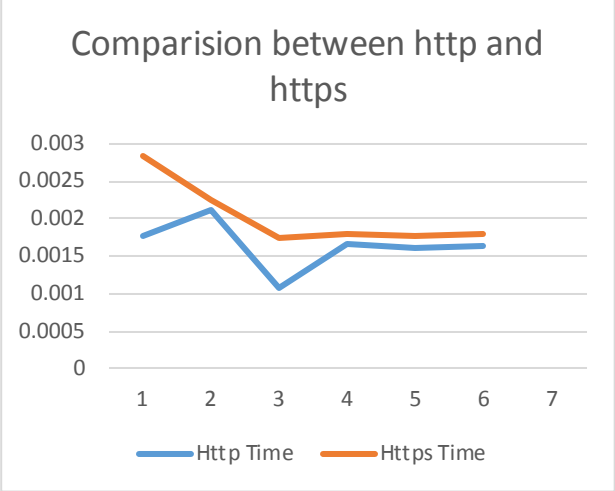
V. IMPLEMENTATION

We implemented our algorithm by using .net frame work. We developed modified RSA algorithm using C# and used DES algorithm library (System.Security.Cryptography.Des). The concept of the algorithm emphasizes on encryption, therefore make sure the computer system compatibility.

VI. RESULT OF IMPLEMENTATION

Now based on above research and applying the modified RAS and DES Encryption following comparison is made practically. Using the HTTPS transaction and HTTP transaction with our methodology to make a secure transaction it is clearaly observable from the graph that our convention still has a greater speed of transaction then conventional HTTPS .

978-1-4799-4190-2/14/$31.00 ©2014 IEEE
Authorized licensed use limited to: Universita di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.



Here for this comparison graph data mining is done by taking the varied number of strings over Our HTTP methodology and conventional HTTPS Transaction.

Table1: Result on Simulated implementation

Strings length	Http Time	Https Time
5	0.00176	0.002835
10	0.002124	0.00224
15	0.00108	0.001741
20	0.001654	0.001798
25	0.001603	0.001768
30	0.001634	0.001786

VII. CONCLUSION

We worked to improve transaction security. The primary objective of the research paper was to ensure a faster and more secure means to transfer most sensitive part of data in an e-commerce transaction, i.e., the credit card number, its CVV and user PIN.

By restricting our encryption algorithm to list amount of data we were able to achieve the following

1. Faster Data rates for up to 4 units [1 unit = 4 Bytes] of data then the existing encryption technique,
2. Comparable Data rates for data more than 4 units then the existing encryption technique,
3. Enhanced Security because DES and RSA were interleaved to achieve the benefits of both symmetric and asymmetric encryption.

In future the data unit size can be increased to accommodate complete transaction information which can extend up to 100 units or 400 Bytes of data by embedding a compression technique to reduce the data size.

REFERENCES

[1]Ziff Davis, "E-Commerce." Software World, 2003, vol. 30, pp. 207-212.

[2] S. H. Qing, Cryptography and Computer Network Security. Beijing: Tsinghua University Press, 2001.

[3] Y. P. Hu, Y. Q. Zhang, Symmetric Cryptography. Beijing: Machinery Industry Press, 2002.

[4]S. Z. Guan. Public Key Infrastructure PKI and Certification Authority. Beijing: Publishing House of Electronics Industry, 2002.

[5] X. J. Tong, W. Jiang, "Research of Secure System of Electronic Commerce Based on Mix Encryption," Microprocessors, 2006, vol. 4, pp. 44-47.

[6]Microsoft MSDN A Performance Analysis of Secure HTTP ProtocolXubin http://citeseerx.ist.psu.edu/viewdoc/download

978-1-4799-4190-2/14/$31.00 ©2014 IEEE
Authorized licensed use limited to: Universita di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.