Kavitha S Nair / International Journal of Engineering Research and Applications (IJERA)

ISSN: 2248-9622 www.ijera.com

Vol. 2, Issue 2, Mar-Apr 2012, pp.462-465

Providing Security and Safety in Electronic Commerce And Internet Transactions

Kavitha S Nair

Computer Engineering Dept., Maharashtra Academy of Engineering, Pune, India

Abstract— Most ecommerce merchants leave the mechanics to their hosting company or IT staff, but it helps to understand the basic principles. Any system has to meet five requirements. Firstly, Confidentiality i.e. the communication between two parties has not been seen by a third party and the material of the communication has remained secret. Secondly, Integrity i.e. the communication has not been tampered with nor has the message been edited (or the amount of money had been changed). Then, Authentication i.e. the identity of the author/ sender can be verified so that the receiver knows the message / information did indeed come from the proper source. Plus, Non-repudiation i.e. the sender cannot deny having sent the message nor can they have means to change any of the content (including currency amounts) within the message and finally Access Control - only the authorized recipient can open the message.

Keyword: **confidentiality, integrity, authentication, non-repudiation and access control.**

I. INTRODUCTION

Electronic commerce, commonly known as e-commerce or e-business consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. There is a widely perceived risk attached to payments made via the Internet, and this perception is in some circumstances justified. This is not like making a phone call or sending a fax. The information sent from the customer to the Web server may pass through many different stages before being delivered. The information is in digital form, and at any stage an unauthorized individual may scan every message looking for credit card numbers (which are easily identified).

So, in this paper , we are basically dealing with the security in e commerce which is a very important issue to think on in today's world. We are using an encryption algorithm named Triple DES explained in section (III), cryptography technique is used explained in section (I), with implementation of shopping cart explained in section (IV) and payment gateway integration is used for payment and we are using PayPal which is elaborate in section (V).

Main motive for doing this project is the awareness and requirement of e commerce site in India and specially necessarily security in any kind of transactions over internet.

II. CRYPTOGRPHY

Cryptography is a method of mathematically encoding used to transform messages into an unreadable format in an effort to maintain confidentiality of data. Cryptography comprises a family of technologies that firstly include Encryption transforms data into some unreadable form to ensure privacy. Internet communication is like sending postcards in that anyone who is interested can read a particular message; encryption offers the digital equivalent of a sealed envelope and then Decryption is the reverse of encryption; it transforms encrypted data back into the original, intelligible form. Then Authentication identifies an entity such as an individual, a machine on the network or an organization. Lastly, Digital signatures bind a document to the possessor of a particular key and are the digital equivalent of paper signatures. Signature verification is the inverse of a digital signature; it verifies that a particular signature is valid.

III. ENCRYPTION ALGORITHM: TDEA

Triple DES i.e. Triple Data Encryption Algorithm (TDEA). Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. Triple DES is based on the DES (Data Encryption Standard) algorithm; therefore it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Triple DES runs three times slower than

ISSN: 2248-9622 www.ijera.com

Vol. 2, Issue 2, Mar-Apr 2012, pp.462-465

DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse.

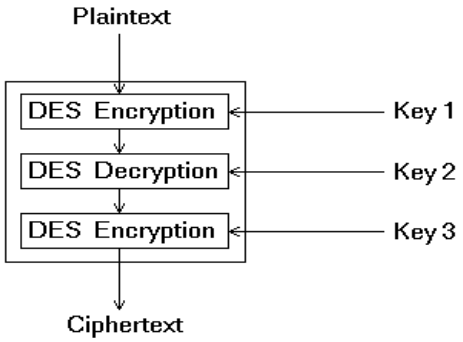

Figure 1: Triple DES

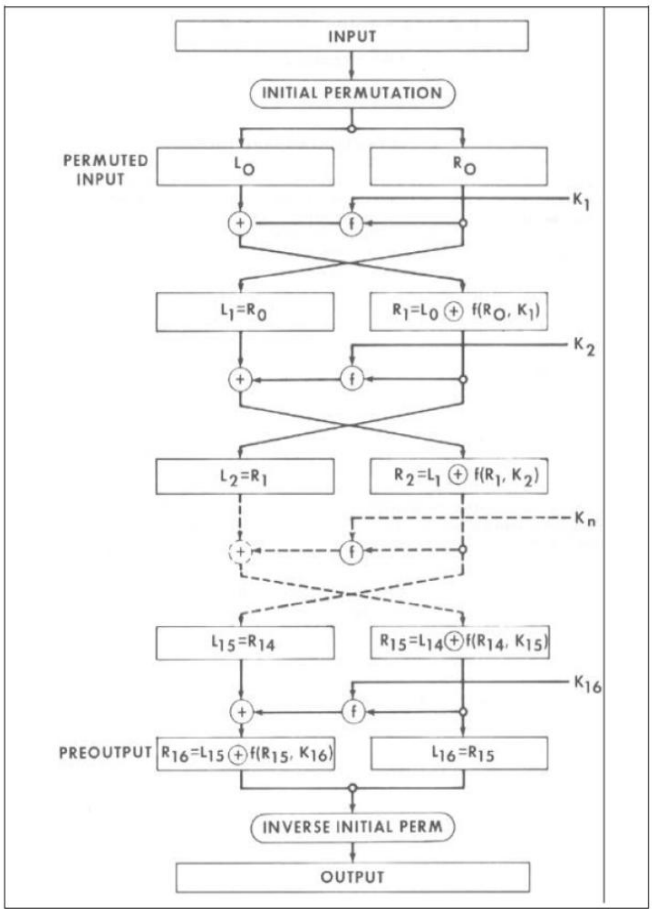

Figure 2: DES

Algorithm:

Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The **encryption algorithm** is:

ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

I.e., DES encrypts with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.

Decryption is the reverse:

plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$

I.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.ach triple encryption encrypts one block of 64 bits of data.

ISSN: 2248-9622 www.ijera.com

Vol. 2, Issue 2, Mar-Apr 2012, pp.462-465

SECURE SOCKET LAYER

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.SSL encrypts data, like credit cards numbers (as well other personally identifiable information) which prevents the "bad guys" from stealing your information for malicious intent.

IV. SHOPPING CARTS

Ecommerce software packages enable you to build sites where customers can

1. view your goods
2. add or delete items from their selection, and
3. Review their final selection prior to purchase.

The payment process is made intuitive, fast and secure. It keeps records — for accounting and tax purposes, but also for more effective marketing and planning. Shopping cart software can be generally categorized into two main categories:

1. Licensed software(downloaded and installed),
2. Hosted service (application service provider software).

V. PAYMENT GATEWAY: PayPal

An e-commerce application service provider that authorizes payments for e-businesses. It is equivalent to physical point of sale terminal. A payment gateway facilitates the transfer of information between a payment portal (such as a website, mobile phone or IVR service) and the Front End Processor or acquiring bank. In our project payment gateway which we are using is:

PAYPAL

"PayPal is an e-commerce business allowing payments and money transfers to be made through the Internet. PayPal serves as an electronic alternative to traditional paper methods such as checks and money orders."

VI. ADVANTAGES

1. Anonymity and intractability can be maintained: User Id's are kept highly confidential.
2. Credit card over internet: Credit cards are convenient because you pay immediately instead of having to mail a check or money order to the online company. The merchant then can send your merchandise promptly rather than waiting for the money to arrive. You have an automatic record of the transaction on your credit card statement if the company claims it did not receive the money. You may able to store your card number and other billing information at websites from which you make purchases frequently.
3. Creates Transaction Database: Stores transaction information in your database for as long as you want. You'll never have to search for lost transaction information.
4. Increases Accountability: It is easy to confirm whether you have received the proper amount of credit for each transaction. Minimizes Fraud: Performs address verification (AVS) and eliminates the chance of shipping to someone using a stolen credit card, saving you from a charge back.
5. Quicker Transactions: Allows you to send multiple transactions as a batch, thus reducing authorization time to as low as three seconds per transaction.

VII. DISADVANTAGES

1. Communication Overheads: Security and anonymity cost become a bottleneck of the system. This can happen at times during real-time verifications.
2. Massive Databases: The bank will have to maintain a detailed and confidential database.
3. Synchronization: The bank needs to synchronize its server every time transaction is made. It would be insanely impractical to maintain.
4. Main disadvantage is time it takes for the website to load and for the customer to navigate through the website. Some of the other disadvantages would include the cost required in order to maintain a secure website.

VIII. FUTURE SCOPE & ENHANCEMENT

1. Email notification,
2. Cheques deposit using online from anywhere,
3. Spreading security to increase the power of our country,
4. Increase the use of e commerce,
5. Adapting higher security in intelligence of the country.

IX. CONCLUSION

With the implementation of Triple DES as encryption algorithm, the security has been accomplished and a secure website is ready to use over internet.

X. REFRENCES

[1] Chakrabarti, Rajesh and Kardile, Vikas (2002), *E-Commerce:The Asian Manager's Handbook*, New Delhi: Tata McGraw Hill.

ISSN: 2248-9622 www.ijera.com

Vol. 2, Issue 2, Mar-Apr 2012, pp.462-465

[2] Chaum, D. (1992), *"Achieving Electronic Privacy",* Scientific American, August,pp 96-101 accessed on http://www.digicash.support.nl/publish/sciam.html.

[3] Erikson, J. (2003), *Dictionary of E-Commerce*, New Delhi: Anmol Publications Pvt. Ltd., p.151.

[4] Sumanjeet (2008), *"Factors Affecting the Online Shoppers' Satisfaction: A Study of Indian Online Customers",* The South East Asian Journal of Management, Vol. 11, No. 1, pp 3-11.

[5] Sumanjeet (2008), *"Securing Payment Systems in the Age of Electronic Commerce",* International Journal of Management Research and Technology, vol. 2, No. 1, pp 19-32.