IJCSC International Journal of Computer Science and Communication Vol. 3, No. 1, January-June 2012, pp. 55-56

ENCRYPTION TECHNIQUES UTILITY WHILE PROVIDING SECURITY TO THE E-DOCUMENTS

K. Jagan Mohan[1] and T. Venkat Rao[2]

[1]Professor & Dean, Varaha Lakshmi Narasimha Swamy Engineering College, Narava, Visakhapatnam-27,
E-mail: kammili_jaganmohan@rediffmail.com.

[2]Professor and Director, Venkat Educational Academy, Ramavarappadu, Vijayawada,
E-mail: venkateducation@yahoo.com.

ABSTRACT

It is very much necessary to provide security to the multimedia content that is stored in the form of electronic documents that are to be sent from one network to another. The e-documents may be sometimes digitized, compressed, and stored in computerized libraries or multimedia storage warehouses that are linked by transport networks to each other and to the software/hardware clients that allow customers to access them. Generally this can be achieved through messaging software like e-mail, EDI (Electronic Data Interchange), or point-to-point file transfers. The major security components to be considered are – Confidentiality (Access Control, Cryptography and existence of data), integrity (No change in the content sent by the source, prevention mechanisms and detection mechanisms) and Availability (Denial of service attacks).

This technical paper is intended to explain briefly about the importance of encryption, various encryption techniques used to provide security to the electronic documents through internet.

Keywords: EDI, I-way, cryptography, DES.

1. INTRODUCTION

To facilitate any business process, it is necessary to have -Common business servers (for buying & selling process), Messaging & Information distribution (for sending & retrieving information), Multimedia content and network publishing (for creating a product & a means to communicate about it), and the information superhighway (for providing highway system along which all e-documents must travel).

In addition to the development of e-documents that are to be stored in servers, it is also required to see that how servers assure the customers of safe delivery? and how customers pay for using the I-way? (messaging software). Encryption and authentication methods have been developed to ensure security of the contents while travelling the I-way and at their destination. Numerous e-payment schemes are being developed to handle highly complex transactions with high reliability.

2. PRESENT WORK

It is found that the data and message security are very much important as per the transaction security is concerned. The e-data security is of high importance when people make banking and financial transactions by PCs. Due to sniffer attacks with packet sniffing, if one insecure system on a network is exposed to intrusion, then all the other local machines and also any remote systems to which the users connect to may get exposed automatically. This leads to collection of user accounts along with the passwords by the intruders without the knowledge of the users and subsequent intrusions will happen via legitimate accounts on the machines involved. The message security threats are due to lack of– *confidentiality, integrity and authentication.*

The *message confidentiality* is of importance for involving sensitive data such as credit card numbers. The environment must protect all message traffic. Once the successful delivery of data is made to their destination gateways, messages must be removed from the public environment (Because whenever a message enters the public internet for transfer it will be added with some unambiguous identification by the consumer devices/ vendor-software from which it came. On the network this identification takes the form of the IP address. If the identification is lacking, the delivery program will insert it). All that remains is the accounting record of entry, delivery, including message length, authentication data, audit trail of message transfer agents that processed the message and nothing more. To make use of distributed networks and wireless links, security of communication link is needed between computers via *encryption*.

The *message integrity* involves in the business transactions which require that their contents remain unmodified during transport. The mechanism for integrity must prevent active attacks involving the modification of data. Error detection codes, sequence numbers and encryption techniques are the methods to enhance information integrity. Error detection codes operate on the

entire messaged or selected fields within the message. Sequence numbers prevent reordering, loss, or replaying of messages by an attacker. Encryption techniques such as digital signatures can detect modifications of a message.

The *message-authentication* verifies the identity of an entity (a user or service) using certain encrypted information transferred from the sender to the receiver. The cryptographic signed certificates would work better in such cases in which the client and server must compare the origination address of transactions and messages with information associated with each service gateway to ascertain that the origination address is valid with respect to the gateway across which the message enters. It is very important that the clients authenticate themselves to servers, that servers authenticate to clients, that both authenticate each other. Then only it is possible to transfer data from sender to receiver. Sometimes, third-party authentication services exist within a distributed network where a sender can't be trusted to identify itself correctly to a receiver. In short, authentication plays an important role in the implementation of business transaction security.

Encryption: Sensitive information that must travel over internet can be defended by encrypting it from the intruders. Encryption is the mutation of information in any form (text, video, and graphics) into a representation unreadable by anyone without a decryption key. Suppose if A (sender) and B (receiver) uses the same cryptographic key for both encryption and decryption, it is referred to as the single-key-cryptography or *Secret-Key-Cryptography*. This method stands good for one-to-one document interchange and is not feasible in a business environment where a company deals with thousands of online customers as it requires a lot of key-management. The Data Encryption Standard *(DES)* is a widely-adopted implementation of secret-key-cryptography. DES can also be used for single user description, to store files on a hard disk in encrypted form. However, in a multi user environment, *Public-Key-Cryptography* is used which involves a pair of keys – a private key and a public key associated with each other. Information encrypted by the sender by a private key must be decrypted only by the receiver using a public key. The public key verifies the identity of the sender/author by associating with the private key and ensures the message integrity. Each party to a public key pairing receives a pair of keys, the public key and the private key. For example, when A wishes to send a message to B, A looks up B's public key in a directory, A then uses the public key to encrypt the message and send it to B. B uses the private key to decrypt the message and read it. Anyone can send an encrypted message to B but only B can read it. Unless a third party, say C has access to B's private key, it is impossible to decrypt the message sent by A. This ensures confidentiality.

It is also found that the public key cryptography can be used for sender authentication, known as *digital signatures*. Suppose A is intending to digitally sign on a document, puts their private key and the document together and performs a computation on the composite (key + document) to generate a unique number called the digital signature. For example, when an electronic document, such as an order form with a credit card number, is run through the method, the output is a unique fingerprint of the document. This fingerprint is attached with the original message and further encrypted with the signer's (A's) private key. The result of the second encryption is then sent to B. Then B first decrypts the document using A's public key. B checks whether the message has been tampered or not. To verify the signature, B does some further computation involving the original document, the purporated signature, and A's public key. If the results of the computation generate a matching with the fingerprint of the document, the digital signature is verified as genuine. Otherwise, the signature may be fraudulent or the message altered, and they are discarded. This method is the basis for secure e-commerce, variations of which are being explored by several companies.

3. SOME OF THE STANDARD ORGANIZATIONS

We are here by mentioning some of the standard organizations who provides standards for ensuring network-security.

National Institute of Standards and Technology (NIST), Internet Society (ISOC), Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), International Telecommunication Union (ITU), International Organization for Standardization (ISO).

4. CONCLUSION

In this technical paper, we presented the way in which cryptographic techniques can be implemented to provide security to the e-documents for the safe delivery of messages from sender to the receiver. Several implementations of these popular encryption techniques are currently employed in various multimedia applications. This paper is useful for the future technocrats who would like to have a good startup in the field of providing security to e-documents using encryption and decryption techniques.

REFERENCES

[1] E-commerce – C.S.V.Murthy.

[2] Frontiers of Electronic Commerce – Ravi Kalakota, Andrew B.Whinston.

[3] Cryptography and Network Security, Third Edition - by William Stallings

[4] Cryptography and Network Security – Atul Kahate, TMH.