International Journal of Management, IT & Engineering
Vol. 9 Issue 5, May 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

"NEW STANDARDS FOR ENCRYPTION AND SECURE DATA TRANSFER"

Mr. Ashok Hajgude*

Mr.NitinTawar**

Abstract

In today's era, the secure transfer of data had been one of the important concerns in the social world. Encryption is a term which is used to transfer data or information securely from one system to another. Here we are proposing to build a secure desktop based application where we can transfer data in the form of text as well as the image which will be encrypted from one system and can be decrypted through another system. Here, we also provide the three lock security while logging into the account. The transfer of data over the internet with the help of encryption secures from unauthorized users.

Keywords: Encryption; Decryption; Cryptography; Steganography; Cipher Text.

* **Head of the Department, Computer Science and Engineering,International Centre of Excellence in Engineering and Management Aurangabad**

** **Ambedkar Marathwada University**

1. INTRODUCTION

Nowadays, the security of data is one of the important aspects of every organization. The concepts such as cryptography and steganography play an important role. The terms such as encryption and decryption are introduced for securely transferring the data. The conversion of plain text messages to cipher text message is called encryption and the reverse method of converting back the cipher text message to the plain text message is called decryption.

Using these techniques data or information is hiding behind image, audio and video. In cryptography terms such as symmetric & asymmetric algorithms are used herein, a key is generated. Symmetric encryption uses the same key for encryption & decryption while asymmetric encryption uses different keys. A Symmetric algorithm is the simplest kind of encryption technique which is old and best known.

The need for this cryptography technique came into existence because of the rise in cybercrime which is built upon the enterprise data. It gives supply chain & market for vulnerabilities, botnets, attack-kits, phishing services, ransomware service and other evolving tools. Due to this

Attack the organization may face a severe loss of data or leakage of private/secret information of their firm. So, data

Security was one of the important concerns among industries or organizations. As the evolution of data security was increasing day by day it was necessary to take preventing measures for the insecurity of data.

The Following figure illustrates the evolution of data security,

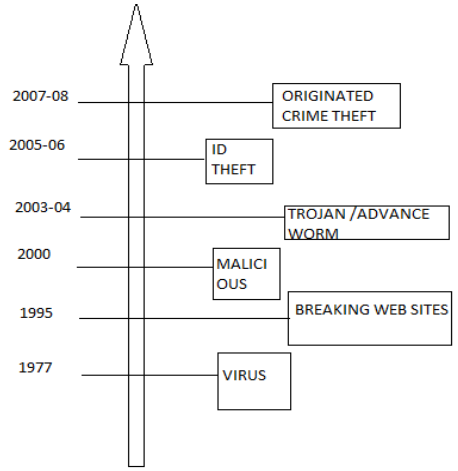

Figure 1.1 Evolutions in Data Security

Two techniques were arising such as cryptography and steganography to give strong security for data or information for the benefit of the particular organization. If we compare old techniques used for data security with the current techniques we will get an excess benefit with new techniques as the loss of data or cybercrimes can be controlled. Different software's are developed for controlling and identifying cyber attacks which are considered as an offense in the judicial system.

2. CRYPTOGRAPHY AND ITS TECHNIQUES

Cryptography or cryptology originated from Greek word "kryptos" means "hidden/secret" & "graphein" means "to write" is a practice for secure transfer of data over the internet or secure communication among networks in the

Presence of an unauthorized user called adversaries.

Cryptography is about analyzing protocols that prevent public, unauthorized users or third parties from reading or illegally using an organization's private data. The terms of cryptography include Encryption, Decryption, Key & Steganography. Using, several algorithms the pain text is encrypted into cipher text i.e. in cryptography cipher text is the result or output generated by the encryption process done on plain text. This cipher text is sent through a network or communication channel and when it reaches the receivers end the cipher text is decrypted using key back into original plain text format.

Symmetric Key Cryptography

Symmetric key cryptography is also known as private key cryptography. A secret key is used to send and receive data from one system to another. Therefore, there should be a copy of secret key with both the sender & receiver. The key is generated at the encryption phase itself where the same key is supposed to be used while decryption also.

The Following figure gives an overview of data is being transferred with the help of symmetric cryptography techniques,

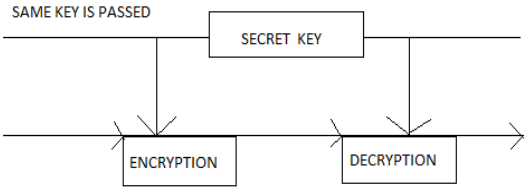

Figure 2.1Symmetric Cryptography Technique

Symmetric key cryptography is considered as valuable as it is relatively inexpensive to produce a strong key. The algorithm used for this technique is also relatively inexpensive to process. Therefore, it is highly effective as there is no time delay in the result of encryption & decryption. The exchanging of a key should only be with the trusted participant. We should also assure that the data exchanged, which are encrypted in a specific key can only be decrypted by another participant that has the key.

The exchanging of a secret key should always be secured. So, there can be a major drawback in the symmetric key as there can be leakage of data while exchanging key if they did not retain the privacy of key. Blowfish, AES, RC4, DES, RC5, RC6 are some examples of symmetric key encryption. The most widely used symmetric key algorithm is AES-128, AES-192 and AES-256. In this project we are implementing the application using the DES algorithm for converting plain text into cipher text and vice versa.

Asymmetric Key Cryptography

Asymmetric key cryptography is also known as public key cryptography. Here, asymmetric key uses two different keys for encryption. These secret keys are exchanged over a large network. It also ensures that the unauthorised person does not misuse the keys. There are two keys, public key & private or secret key, where the public key is made available to anyone who wants to send the message or want to exchange data. But, the second private key is kept secret so that you can only know.

The Following figure illustrates the asymmetric key cryptography,

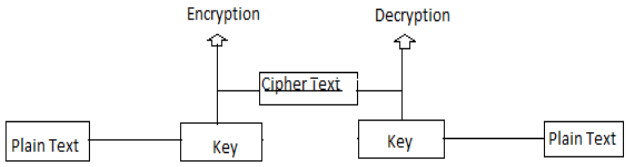

Figure 2.2 Asymmetric Key Cryptography

As shown in the above figure there are two keys used each for encryption and decryption respectively. It is highly secure as compared to symmetric key cryptography. The intruder cannot misuse the data transferring over the network. This is an important requirement for electronic commerce. It enables to use the private key to sign data with the digital signature.

The following are the major asymmetric encryption algorithms encryption or digital signing data,

- Diffie-Hellman key agreement.
- Rivest Shamir Adleman (RSA).
- Elliptic Curve Cryptography (ECC).
- EI Gamal.
- Digital Signature Algorithm (DSA).

I. STEGANOGRAPHY

Steganography originated from Greek word which means covered writing. It hides a secret message within an ordinary message and it is extracted at its destination end. Steganography takes cryptography a step farther by hiding an encrypted message behind some other data and no one suspects that it exists. Even if anyone scans the data they fail to know that it contains any secret message behind it. Some of the techniques used in steganography such as least significant bit insertion and noise manipulation, transform domain and image transformation.

II. APPLICATIONS

Currently, the economy of India is highly depended on various financial issues & their day to day transactions are very high for public, private & government sectors. Financial data transaction in the banking and financial industry is generally reliable. All these credential transaction and data transferring is done through internet. Some of its applications are the security of confidential data of industries or organization, security in social media, digital signature, database security & so on.

- Defence Forces

In the defence system, the transfer of confidential data should always be secure. One of the ways in communication is done via the internet for sharing information. The content sharing might be sensitive which has to be kept secure from unauthorised users. If there occurs any leakage of data, then it can cause harm to the whole defence system as well as to the nation. Here the data is encrypted and a private key is shared among the authorized sender and receiver. Due to which they ensure the secrecy of communication.

- Database Security

Volumetric data from IT industries or various organizations address their security objectives and mandates at the number of system and environments. There will be a need to guard those data from intruders. It is necessary to encrypt the sensitive data in a database, or address the mandates in the cloud. These are some of the reasons for which data security is considered on a large scale among industries.

- E-Commerce (online shopping, net banking)

Nowadays, E-Commerce is considered the vastly used application on the internet among worldwide. Buying and selling of products require the bank details wherein we have to provide all the information of our bank account including the Account number, credit card pin, etc. One of the major cybercrime done is theft of money from your bank account. To avoid this one should ensure the secrecy of confidential information like credit card numbers during the transaction. The encryption of data or information is the best way to avoid such cyber attacks.

III. CONCLUSION

Data security for transferring data over internet plays a very important role in today's era as everything from shopping to banking has become online. Data security helps to keep the records of all the data online and offline away from intruders or unauthorised users. Cryptography is a method where plain text is encrypted into cipher text & the cipher text converted back into plain text using decryption. Using Steganography, we can hide the original message behind any image which is extracted at its destination end. This paper gives an overview of the data security for secure internet transfer. In future we will give some practical based analysis on the applications described in this paper.

References:

[1] Manole VELICANU, Gheorghe MATEI ,"DATABASE VS DATA WAREHOUSE", in Revista Informatica Economică, nr. 3 (43)/2007

[2] Sanu Kumar "ASPECT OF DATA MINING AND DATAWAREHOUSING", The international journal of technology enhancements and emerging engineering research,.

[3] Kalpana Rangra Dr. K. L. Bansal,, " COMPARATIVE STUDY OF DATA MINING TOOLS", International Journal of Advanced Research in Computer Science and Software Engineering.

[4] Drew Cardon, "DATABASE VS DATA WAREHOUSE: A COMPARATIVE REVIEW", HealthCatalyst

[5] Muhammad Bilal Shahid, Umber Sheikh, Basit Raza, Munam Ali Shah, Ahmad Kamran, Adeel Anju, QaisarJavaid ,"APPLICATION OF DATA WAREHOUSE IN REAL LIFE: STATE-OF-THE-ART SURVEY FROM USER PREFERENCES' PERSPECTIVE", in (IJACSA)2016

[6] Milija SUKNOVIĆ, Milutin ČUPIĆ, Milan MARTIĆ, "DATA WAREHOUSING AND DATA MINING - A CASE STUDY", Yugoslav Journal of Operations Research

[7] Mehmed Kantardzic,"DATA - MINING APPLICATIONS", Data Mining: Concepts, Models, Methods, and Algorithms, Second Edition

[8] Kanika Passi, ," REVIEW ON ROLE OF DATA WAREHOUSE IN BUSINESS INTELLIGENCE", IJARCET

[9] KHALID RAZA, "APPLICATION OF DATA MINING IN BIOINFORMATICS", Indian Journal of Computer Science and Engineering

[10] Youssef Bassil "A DATA WAREHOUSE DESIGN FOR A TYPICAL UNIVERSITY INFORMATION SYSTEM", Journal of Computer Science & Research (JCSCR) - ISSN 2227-328X.

[11] Pushpal Desai , Desai Apurva "THE STUDY ON DATA WAREHOUSE AND DATA MINING FOR BIRTH REGISTRATION SYSTEM OF THE SURAT CITY", International Conference on Technology Systems and Management (ICTSM) 2011

[12] Ryan Neary,"BUILDING A DATA WAREHOUSE AND DATA MINING FOR A STRATEGIC ADVANTAGE",JITTA,1999.