Secure Message Transfer using Triple DES

Somya Garg
Computer Science Department
GCET, Greater Noida

Tarun Garg
Computer Science Department
GCET, Greater Noida

Bhawna Mallick, PhD
Professor & Head at GCET,
Greater Noida

ABSTRACT
With the rapid growing of internet and networks applications, data security becomes more important than ever before. Encryption algorithms play a crucial role in information security systems. In this paper, we have a study of a popular encryption algorithm: Triple DES. We overviewed the base functions and analyzed the security for the algorithm. We have succesfully sent mails from one user to other and if a suspicious word is encountered then the mail is being sent to the admin instead of that user.

Keywords
Triple DES, Encryption, Security, Suspicious word, Cipher text, Decryption.

1. INTRODUCTION

Suspicious email detection

Suspicious email detection is a kind of mailing system where suspicious users are identified by determining the keywords used by him/her. The suspicious keywords are found in the mails which are sent by the user. All the blocked mails are checked by the administrator and identify the users who have sent such mails.

Triple DES

The DES algorithm is popular and in wide use today because it is still reasonably secure and fast. There is no feasible way to break DES, however because DES is only a 64-bit (eight characters) block cipher, an exhaustive search of 255 steps on average, can retrieve the key used in the encryption. For this reason, it is a common practice to protect critical data using something more powerful than DES. A much more secure version of DES called Triple-DES (TDES), which is essentially equivalent to using DES three times on plaintext with three different keys. It is considered much safer than the plain DES and like DES, TDES is a block cipher operating on 64-bit data blocks. There are several forms, each of which use the DES cipher three times. Some forms of TDES use two 56-bit keys, while others use three. TDES can however work with one, two or three 56-bit keys. With one key TDES = DES. The TDES can be implemented using three DES blocks in serial with some combination logic or using three DES blocks in parallel. The parallel implementation improves performance and reduces gate count.

Basic Terms Used in Cryptography

Plain Text- The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.

Cipher Text- The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".

Encryption- A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

Decryption- A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

Key- A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

Confidentiality- Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication- The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

Integrity- Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation- Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control- Only the authorized parties are able to access the given information.

Classification of Cryptography

Encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption.

Symmetric Encryption- In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES.

2. EXISTING METHODOLOGY

TRIPLE DES

In cryptography, Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

The earliest standard that defines the algorithm (ANS X9.52, published in 1998) describes it as the "Triple Data Encryption Algorithm (TDEA)" — i.e. three operations of the Data Encryption Algorithm specified in ANSI X3.92 — and does not use the terms "Triple DES" or "DES" at all. FIPS PUB 46-3 (1999) defines the "Triple Data Encryption Algorithm (TDEA)", but also uses the terms "DES" and "Triple DES". It uses the terms "Data Encryption Algorithm" and "DES" interchangeably.

The TDEA is commonly known as Triple DES (Data Encryption Standard).

While none of the standards that define the algorithm use the term "3DES", this term is used by some vendors, users, and cryptographers.

ALGORITHM

Triple DES uses a "key bundle" that 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 encrypt 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.

Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

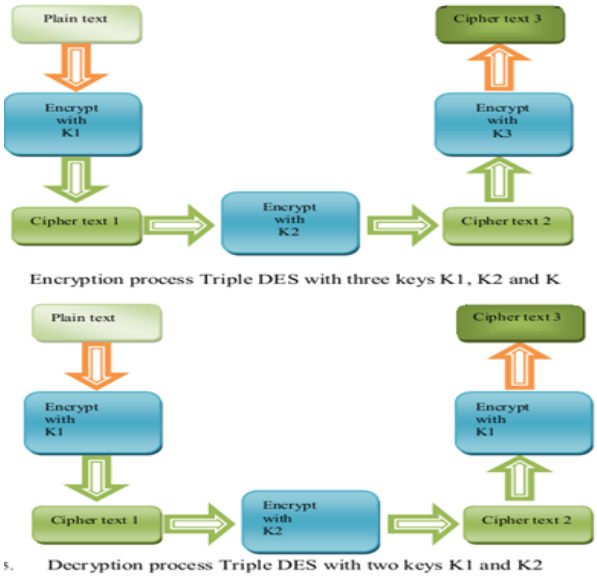

Fig 1 : Encryption and Decryption

3. PROPOSED SYSTEM

In this paper, we will detect the suspicious mails sent from the users who are already registered on this website. Firstly new users sign up themselves on the site to sent the mails to those users who already registered and then view the messages from the registered users. Triple DES Algorithm used by admin to encrypt the messages sent to the users or sent some warnings about the other users suspicious activity.

In this research, suspicious words dictionary is used to detect the suspicious words which are not actually used in the normal messaging or communication.

1. Admin Login

In this project, admin can enter the username and password to authenticate himself to access the account panel modules.

2. User Login

In this module, users can enter their username and password to authenticate themselves to access their account panel modules.

3. User Registration Module

In this module, users can enter their username and password and address, mobile, email id to register themselves to access the account panel modules.

4. Create Message Module for Admin

In this module, admin can select the username and then enter the message along with the subject and also the input encryption key which is used for encrypt the message as well as the subject and then send it to the selected user and message and subject are both stored into the user inbox.

5. Check Suspicious Mails for Admin

In this module, admin can check the suspicious mails which is not actually stored into the user inbox instead of marked as suspicious status and sent it to the admin as suspicious mails with the user details.

6. Data Dictionary for Admin

In this module, admin can add the suspicious words into existing data dictionary to detect more precisely and accurately the suspicious mails sent by the users.

7. View Data Dictionary for Admin
In this module, admin can view the suspicious words exists into the data dictionary and also has access to delete the suspicious words from the existing data dictionary of suspicious words.

8. View Users List for Admin
In this module, admin can view the registered users and their full details and has access to delete the users if any of the registered users are found to do the suspicious activity on the website.

9. Create Message Module for Users
In this module, users can select the other users and then enter the message along with the subject and then send it to the selected user and message and subject are both stored into that inbox of receiving user and at back end of the website Suspicious mail detection module is worked which is detected the sent mails marked as suspicious or normal.

When the message status sets to normal then it will sent to selected user but if sent message status found to be suspicious then it will sent to the admin inbox instead of the selected user inbox.

10. Inbox Module for Users
In this module, users can view the inbox messages which are sent by the users those who are already registered if the user is any registered user then this message will be viewed without any decryption module and also has access to delete that mail.

But if the user is admin, then user has inbox messages as the encrypted messages which are to be decrypted by the user by supplying the decrypting key which is to be decrypted the required message and then turns back into the encrypted message after viewed by the user.

11. Sent Box Module for Users
In this module, users can view the sent mails to the selected users and has access to delete those mails as needed.

4. SYSTEM DESIGN

Platform
To implement a system, we have used Programming Language Advanced Java; NetBeans 7.3.1 as a front end IDE, MySQL Server as a database for storing data and supported Operating System are WINDOWS XP & its above versions.

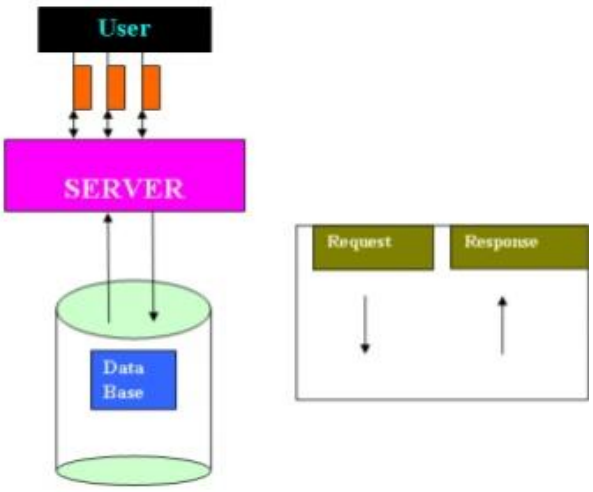

Fig 2 : System Architecture

5. CONCLUSION AND FUTURE WORK

The proposed System solves the problem definition by detecting the suspicious mails. Admin creates the data dictionary of suspicious words and this data dictionary helps in detecting the suspicious activity of the users. Admin further will be adding the suspicious words into the existing Suspicious Words data dictionary.

(i) Email has been an efficient and popular communication mechanism as the number of internet user's increase.
(ii) In many security informatics applications it is important to detect deceptive communication in email.
(iii) The following project has been proved helpful for identifying the suspicious email and also assist the investigators to get the information in time to take effective actions to reduce the criminal activities.

FUTURE WORK
(i) Adaptation to other services like Facebook, LinkedIn etc.
(ii) More scalability and coverage.
(iii) Develop more features which cannot be fabricated.
(iv) Handle multiple redirections.

FUTURE ENHANCEMENTS
(i) According to the emerging changes and new versions, further work can be done to improve the appliaction since project is designed in a flexible software.
(ii) This application is a web based standalone application. This can be implemented on Internet by buying the network space and by creating a website.
(iii) The present application when implemented on internet requires a large database as backend; this can be done by using the MySql database as backend.

AES ENCRYPTION

i. AES is supposed to be the holy grail of Encryption. It is meant to improve on DES and 3DES and last as a standard for the next 20 to 30 years.

ii. The **AES** algorithm is very complex, but basically, it works as follows:

(i) The sender has a stream of data, and the data is separated into blocks of data of n bits.
(ii) The blocks of data are combined with a cipher key.
(iii) Arrays of data (matrices) are created using a series of functions.
(iv) Before transmitting the data, a series of iterations called "rounds" are applied to the arrays. The number of rounds performed depends on the key length. For example, 128 bits uses 10 rounds, 196 bits uses 12 rounds, and 256 bits uses 14 rounds.
(v) The 4 functions performed on the arrays for each round are: SubBytes, ShiftRows, MixColumns, and AddRoundKey.
(vi) When the data is received, decryption is accomplished by a reversed sequence of inverse round functions. Of course, both sender and receiver must know the cipher key.

6. REFERENCES

[1] S.Appavu alias Balamurugan, Aravind,Athiappan, Bharathiraja,Muthu Pandian and Dr.R.Rajaram, "Association Rule Mining for Suspicious Email Detection: A Data Mining Approach", in Proc. Of the IEEE International Conference on Intelligence and Security Informatics, New Jersey,USA, 2007, pp. 316-323.

[2] P.S.Keila and D.B.Skillicorn, "Detecting unusualand Deceptive Communication in Email," Technical reports June, 2005.

[3] S.Appavu and R.Rajaram, "Suspicious Email Detection via Decision Tree: A Data Mining Approach", in Journal of Computing and Information Technology–CIT 15, 2007,2, pp. 161-169.

[4] S.Appavu, R.Rajaram, G.Athiapan, M.Muthupandian, "Data Mining Techniques for Suspicious Email Detection: A Comparative Study". Presented in IADIS European Conference DataMining 2007, pp. 213-217.

[5] R.Agrawal, R.J.Bayardo and R.Srikant. Athena, "Mining-based interactive management of text databases," In Proc. 7thInt. Conf. Extending Database Technology, Konstanz, Germany, 2000, pp.365-379.

[6] R.B.Segal and J.O.Kephart, MailCat: An Intelligent Assistant for Organizing E-Mail, in the Proc. of 3 rd Int. Conf. on Autonomous Agents.

[7] R.Agrawal and R.Srikant, "Fast algorithms for mining association rules,"In Proc. 20th Int. Conf. Very Large Databases, pp. 487-499, Santiago, Chile, 1994.

[8] Liu, W. Hsu, and Y. Ma, "Integrating classification and Data Mining", pages 80-86, New York City, NY, August 1998.

[9] X. Yin, J. Han,"CPAR: Classification based on predictive Association Rules,"SDM'03, pages 331-335.

[10] A.A.Zaidan, B.B.Zaidan, "Novel Approach for High Secure Data Hidden in MPEG Video Using Public Key Infrastructure", International Journal of Computer and Network Security, 2009, Vol.1, No.1, ISSN: 1985-1553, P.P 71- 76.

[11] A.W.Naji, A.A.Zaidan, B.B.Zaidan, Shihab A, Othman O. Khalifa, "Novel Approach of Hidden Data in the (Unused Area 2 within EXE File) Using Computation between Cryptography and Steganography", International Journal of Computer Science and Network Security (IJCSNS), Vol.9, No.5, ISSN: 1738-7906, pp. 294-300.

[12] Anas Majed Hamid, Miss Laiha Mat Kiah, Hayan .T. Madhloom, B.B Zaidan, A.A Zaidan," Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET) , Published by: Engg Journals Publications, ISSN:0975-4042, Vol.1,NO.2,P.P 63- 69.

[13] K.Selvakuberan, M.Indradevi, R.Rajaram, (2008). Combined feature selection and classification – A novel approach for categorization of web pages. Journal of Information and Computing Science. 32pp. 83-89.

[14] A. Arauzo-Azofra, J. M. Benitez, "Empirical Study of Feature Selection Methods in Classification", In proc. of Eighth Internation Conference on Hybrid Intelligent System s, 2008, pp. 584-589.

[15] K. T. Durant , M. D. Smith "Predicting t he political sentiment of web log post s using supervised machine learning techniques coupled with feature selecion".LNCS, 2007, pp. 187-206.

[16] A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", World Academy of Science Engineering and Technology(WASET), Vol.54, ISSN: 2070- 3724, P.P 468-479.

[17] A.A.Zaidan, Fazidah. Othman, B.B.Zaidan, R.Z.Raji, Ahmed.K.Hasan,and A.W.Naji," Securing Cover-File without Limitation of Hidden Data Size Using Computation between Cryptography and Steganography", World Congress on Engineering 2009 (WCE), The2009 International Conference of Computer Science and Engineering, Proceedings of the International Multi Conference of Engineers and Computer Scientists 2009, ISBN: 978-988-17012-5-1, Vol. I, p.p259-265.

[18] M.Abomhara, Omar Zakaria, Othman O. Khalifa, A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198, Vol.2, NO.2, April2010, Singapore.