International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | April 2019 www.irjet.net p-ISSN: 2395-0072

Suspicious Mail Detection

Madhav Gupta[1], Romit Shriwal[2], Divyansh Negi[3], Devarshi Pandey[4], Asst Prof Ms. Shikha Rai[5]

[1,2,3,4]B.Tech Student, Dept. of Information Technology, Dr. Akilesh Das Gupta Institute of Technology and Management Delhi
[5]Mentor: Assistant Professor Ms. Shikha Rai, Dept. of Information Technology, Dr. Akhilesh Das Gupta Institute of Technology and Management, Delhi-110053

Abstract - *Over the past two decades email have become one of the most important and widely used means of communication in various organization and in our personal lives but email has also been used in various organized attacks around the world so there is a need in inspecting the suspicious mail we have utilized some cryptographic strategies for electronic mail detection. Security has great significance in the world of Internet and for communication. Triple Data encryption algorithm is a symmetric-key encryption method that provides reliability and safety in communication. By using a Triple Data Encryption Algorithm, the security has been improved which is very crucial and necessary in the field of email and world wide web.*

Key Words: Decryption, Encryption, TDEA, 3DES, Cipher Text

1. INTRODUCTION

Electronic Mail or E-Mail is amongst the fastest means of communication it is mainly used for formal as well informal communication. E-Mails are often used to communicate to an individual or group of people, people use E-Mail because its quick, free and easy to use for this reasons email has quickly become a source of suspicious activity such as terrorism, frauds and other malicious activity over the internet.

In this research paper we have applied techniques to notice suspicious mails, i.e., associate degree mail that can alert of upcoming unethical events. We have used Triple Data Encryption Algorithm also known as TDEA or Triple-DES (Data Encryption Standard), which focus on a plain text message, when TDEA is used for first time it is used to encrypt the message then the 2nd key is used to decrypt the message which was encrypted. (Because the 2nd key is not a proper key, the data gets scrambled further) then the message which has been scrambled twice is encrypted again with 1st key to give the last ciphered message. This procedure which is done in 3 steps is known as TDES, Triple DES is a type of DES which is done 3 times by using 2 keys in a certain order. (TDEA can also use 3 different keys instead of only using 2. In both the cases the result is 2^112 key space).

A pre-emptive approach to solving bribery, con, terrorism or any other activity harming the society for an organization would be to detect it. Since most of these activities are carried out via an organized approach, hence, they require communication among different members. Electronic mailing systems in organizations is the most common and well-known communication link for the cons or malicious users. Suspicious mail detection helps the admins or the analysts to effectively spot suspicious communication and take the required actions ahead of the hazard and also in-time alert is sent to the admin.

In this research paper, we will identify the unethical mails which users send from the system who are registered. The new users get registered first and then they send mail to other registered users and after that they can view messages from the other users. Triple Data Encryption Algorithm is used by the administrator to encrypt messages which are being sent to the users and administrator can also view and send warnings about the suspicious activities if found.

For this system to work, we use a data dictionary to identify the words which raise the suspicion. Words such as robbery, bribe which are not used in every day to day conversation or messages.

2. Suspicious Mail Detection

Suspicious mail detection is a type of system by which suspected users are detected by identifying the types of words he/she uses. Words can be as hijacking, explosion which can be found in their mails which they send to others. These kinds of mails are then checked by the admin and then the admin can figure out the identity of these users who have sent these mails.

This type of system will work in finding unethical elements. This will also provide better security to the system who decides to adapt it. This can also work in Law Enforcement, and other branch of government offices to monitor of any suspicious activity. This system can provide information and reporting about an incident.

This type of system can work in finding out of suspicious mails and can also provide reliable information on time so that appropriate action can be taken and the crime rate could reduce.

3. TRIPLE DATA ENCRYPTION ALGORITHM

TDEA or TDES is Triple Data Encryption Algorithm is upgraded or enhanced version of DES (Data Encryption Standard) which is a symmetric cryptographic technique in which DES is applied to each block three times which scrambles the plain text to cipher text. TDEA supports key size of 56,112,168 bits and support block size up to 64 bits. TDES can be implemented with the help of 2 keys and from 3 keys as well.

The main process of TDEA is shown in FIG 1. and FIG 2.

The readable text is encrypted with key K1, then again encrypted with key K2 and finally it gets encrypted again with key K3 each time the text is encrypted with the key it gets scrambled further thus protection is increasing at every step.

For decrypting the scrambled or encrypted text we simply perform operation P= DK3 (DK2 (DK1)).

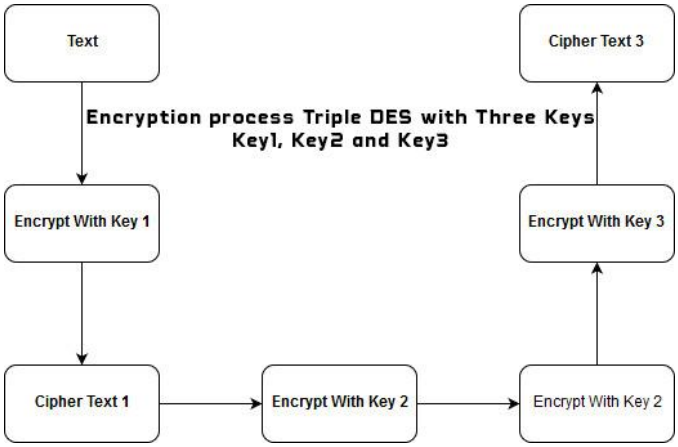

Fig -1: TDEA Encryption

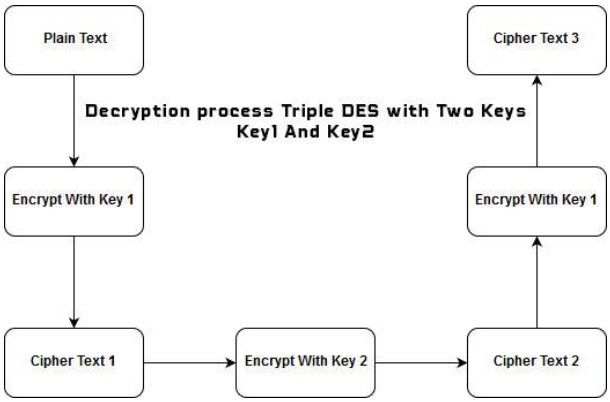

Fig -2: TDEA Encryption

4. PROBLEM STATEMENT

The problem to consider is to detect the mails which are containing evidence to suspicious events the main aim of this software is to make a system that is able to detect activities which are unethical for the social environment as well as the internet.

During this age, communication through mails are a major part of organizations and groups the mail detection software catches the blacklisted words which user have used in their mails and the message is still delivered to other user but the administrator also gets notified of the dubious mail words such as bomb, blast, murder can be blacklisted by the admin.

5. CRYPTOGRAPHY TECHNIQUE

Encryption: Encryption is the procedure of transforming readable text to unreadable form i.e encryption simply changes plain data block to ciphered text.

Decryption: Decryption is the procedure of transforming unreadable or scrambled text to readable form i.e converting ciphered block to plain data block.

Cryptographic Techniques are divided in two categories one is symmetric and other is asymmetric. Symmetric cryptography involves encryption and decryption with the same key popular examples are DES, AES, Blowfish. Asymmetric cryptography involves encryption with public key and decryption with the receiver's private key some popular and widely used examples are SSL and RSA.

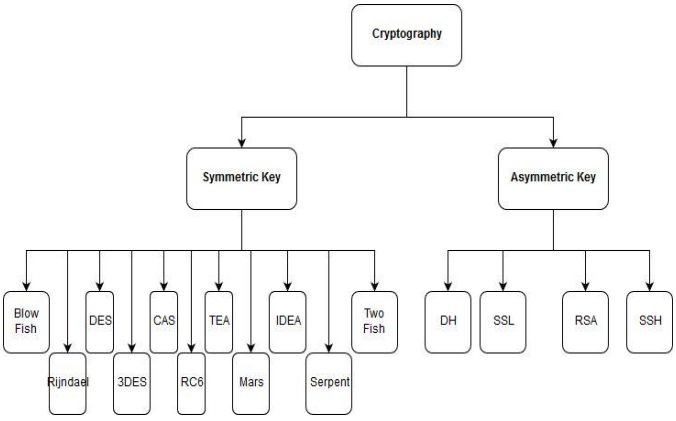

Fig-3 Types of Cryptography

6. IMPLEMENTATION DETAILS

Triple Data Encryption Algorithm is implemented in this system. This system comprises of two components.

1) Employee Component
2) Administrator Component

Above two modules are further branched into different subcategories.

a) Employee Component
   i) Employee Registration
   ii) Employee Login
   iii) Create Mail for Employee
   iv) Inbox
   v) Sent Box
   vi) Discussion Forum/ Employee Forum

b) Administrator Component
   i) Administrator Login
   ii) Check Suspicious Message
   iii) Create Mail
   iv) View Employee List
   v) Data Dictionary
   vi) View Data Dictionary

a) Employee Component: In this module/component the employee of the organization can issue message to other employees. First the user has to login into the system user his/her Employee ID and then the password will be sent to employee's personal email id then the user have to enter code in password box. If anything is found suspicious in sent message the message will be still sent to other user but the administrator will also be notified about the message for further reviewing, the admin can also view all the users registered within the system.

b) Administrator Component: Administrator component is the most important part of this system with this component the administrator can easily view all the suspicious messages/mail between the different employees. Admin can view and edit the data dictionary. The administrator can issue message to the employee and this message is encrypted first with the key and then sent to the employee. Employee has to view the message by entering the same key used at the time of encryption process this key shared by the administrator to the employee, the admin can also view all the users registered within the system.

6. CONCLUSION

The problem is solved by detecting the mail sent from one user to another by the investigator account or the administrator. The Administrator account maintains a data dictionary which stores the distrustful words, if any mail is carrying these words then it is reported to the administrator of the organization and new words can be added to the data dictionary by the Administrator.

REFERENCES

[1] Atul Kahate "Cryptography and Network Security" 3rd edition 2013, ISBN: 9781259029882

[2] Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg. "Network Security: The Complete Reference" 1st edition 2004, ISBN: 9780070586710

[3] Eli Biham, Adi Shamir, "Differential Cryptanalysis of the Data Encryption Standard" 1993, ISBN: 978-1-4613-9314-6

[4] Aggelos Kiayias, Serdar Pehlivanoglu, "Encryption for Digital Content" 52 volume, 2010, ISBN: 978-1-4419-0043-2

[5] Niels Ferguson,Bruce Schneier,"Practical Cryptography", 2nd edition, 2003, ISBN: 0-471-11709-9