ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (540-543), Month: April - June 2015, Available at: www.researchpublish.com

Suspicious Email Detection System via Triple DES Algorithm: Cryptography Approach

[1]Nisha Rani, [2]Mrs. Neetu Sharma

[1]Research Scholar, [2]HOD (CSE Dept.), [1, 2] Department of Computer Science and Engineering,
Ganga Institute of Technology & Management, Kablana, India

Abstract: **The need for Suspicious email detection System is increasing due to the rapid usage of Email communication in the Internet world. The proposed "Suspicious email detection System" provides a way to identify the criminal activities. It detects the suspicious Emails indicating Keywords by applying the Cryptography algorithm called "Triple Data Encryption Standard (3DES)".**

Keywords: **Encryption, Decryption, 3DES, email.**

1. INTRODUCTION

Email is the most popular way of communication of this era. It provides an easy and reliable method of communication. Email messages can be sent to an individual or groups. A single email can spread among millions of people within few moments. Nowadays, most individuals even cannot imagine the life without email. For those reasons, email has become a widely used medium for communication of terrorists as well. A great number of researchers focused in the area of counterterrorism after the disastrous events of 9/11 trying to predict terrorist plans from suspicious communication. This also motivated us to contribute in this area.

In this paper, we have applied Cryptography techniques to detect suspicious emails, i.e., an email that alerts of upcoming terrorist events. We have applied Triple DES (Data Encryption Standard) algorithms, emphasizing initially on Given a plaintext message, the first key is used to DES- encrypt the message. The second key is used to DES-decrypt the encrypted message. (Since the second key is not the right key, this decryption just scrambles the data further.) The twice-scrambled message is then encrypted again with the first key to yield the final cipher text. This three-step procedure is called triple-Triple-DES is just DES done three times with two keys used in a particular order. (Triple-DES can also be done with three separate keys instead of only two. In either case the resultant key space is about 2^112.)

Detecting Suspicious and criminal activities prior to the attacks and providing security to the people is the challenging task for the investigators or administrator Email . is a technology that includes passing and sending information from one place to another, using computer and the Internet. It is beneficial in both our personal and professional life. As Electronic mail is largely used by the terrorists for their communication, there is a need for Suspicious email detection system that classifies emails to detect Suspicious activities and make the administrator alert.

In this paper work, we will detect the suspicious mails sent from the users who are already registered on this System. Firstly new users sign up themselves on the site to send 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 work, suspicious words dictionary is used to detect the suspicious words which are not actually used in the normal messaging or communication.

2. SUSPICIOUS EMAIL DETECTION SYSTEM

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

The proposed work will helps in finding out anti-social elements. This provides the security to system which adapts it. This also helps the intelligence bureau, crime branch etc. Insurance premium calculations, for quarterly, half yearly and annually is completely automated gives us a reliable environment. The system provides claim reporting and status enquiry.

The proposed work will be 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.

3. STUDY OF ENCRYPTION AND DECRYPTION TECHNIQUE

The process of encoding the plaintext into cipher text is called Encryption.

The process of decoding ciphers text to plaintext is called Decryption.

This can be done by two techniques symmetric-key cryptography and asymmetric key cryptography. Symmetric key cryptography involves the usage of the same key for encryption and decryption.

Asymmetric key cryptography involves the usage of one key for encryption and another, different key for decryption.

3.1 Triple DES Algorithm (3DES):

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption Level. Triple DES is DES –three times. It comes in two flavors: One that uses three keys, and other that uses two keys.

The Idea of 3-DES is shown in to the fig.1. The plain text block P is first encrypted with a key K1, then encrypted with second key K2, and finally with third key K3, where K1, K2 and K3 are different from each other.

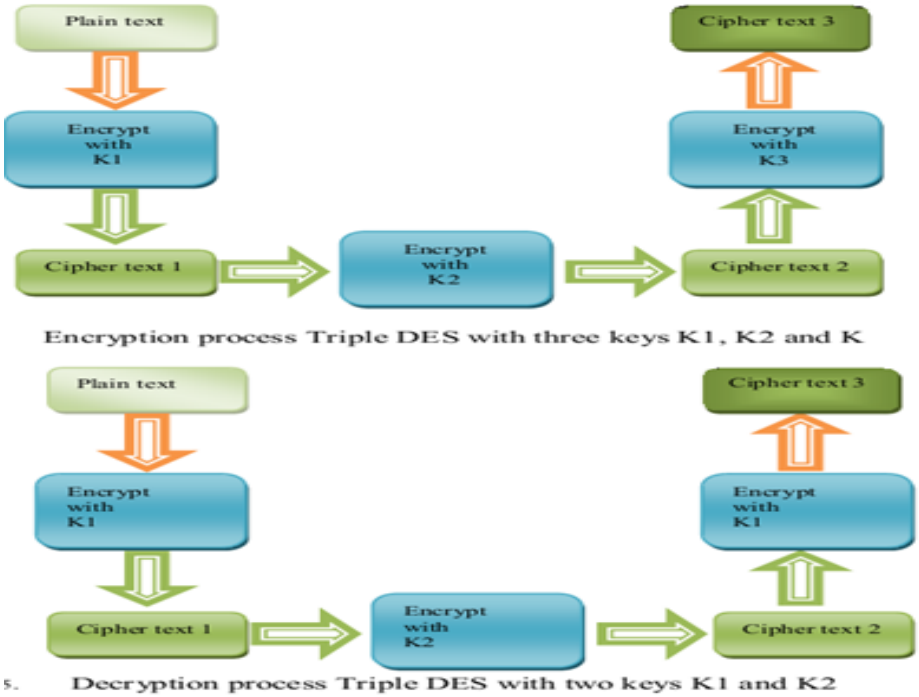
To decrypt the cipher text C and obtain the plain text, we need to perform the operation P= DK3 (DK2 (DK1©)). But in Triple DES with two keys the algorithms works as follows:

[1] Encryption the plain text with key K1. Thus, we have EK1 (p).

[2] Decrypt the output of step1 above with key K2. Thus, we have DK2 (EK1 (P)).

[3] finally, encrypt the output of step 2 again with key K1.Thus, we have EK1 (DK2 (EK1 (P))).

The idea of 3-DES with two keys are shown in fig. 1.



Triple DES

4. LITERATURE REVIEW

The research in the area of email analysis usually focuses on two areas namely: email traffic analysis and email content analysis. A lot of research has been conducted for Email traffic analysis [10], [11].

In the Year 2005 Keila and Skillicorn [11] have investigated on the Enron [13] data set which contains email communications among employees of an organization who were involved in the collapse of the organization. The authors [11] have applied ID3 algorithm to detect suspicious emails by using keyword base approach and by applying rules.

They have not used any information regarding the context of the identified keywords in the emails.

In the Year 2007 S. Appavu & R. Rajaram [2] have applied association rule mining to detect suspicious emails with the additional benefits of classifying the (suspicious in terms of terror plots) emails further into specialized classes such as suspicious alert or suspicious info.

This system decides whether the email can be classified as suspicious alert in the presence of suspicious keyword in the future tense otherwise only it is classified as suspicious info.

In the Year 2008 the authors [13], [14] incorporated feature selection strategies along with classification systems. According to [15], by using feature selection methods one can improve the accuracy, applicability, and understandability of the learning process. Selvakuberan et al. [14] have applied filtered feature selection methods [16] on web page classification; according to their results the evaluator CfsSubset Eval yields better performance with search methods Best First, Ranker search, and Forward selection. Pineda-Bautista et al. [17] proposed a method for selecting the subset of features for each class in multi-class classification task. The classifiers that were used by the authors were Naïve Baye's (NB) [6], k-Nearest Neighbors (k-NN) [17], C4.5 [19], and Multi-Layer Perceptron (MLP). The authors trained the classifier for each class separately by using only the features of that particular class. Durant and In the Year Smith 2007 [15]have emphasized the use of a feature selection method for achieving accuracy of sentiment classification. They proposed to apply Cfs Subset Eval with the Best First search method. Different researcher used different method to implement a System that detects suspicious activities.

The Proposed method used cryptography algorithm i.e. triple DES (3 Data Encryption standard) it is very fast algorithm for encrypt or decrypt the information (email message) in a successful rate.

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 send 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 user's suspicious activity.In this proposed work, suspicious words dictionary is used to detect the suspicious words which are not actually used in the normal messaging or communication.

5. CONCLUSION

The proposed System is solved the problem definition by detecting the suspicious mails. Admin is created the data dictionary of suspicious words and this data dictionary makes help to detect the suspicious activity of the users. Admin further will be added the suspicious words into the existing Suspicious Words data dictionary.

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 Data Mining 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.