Secured Communication using Data Dictionary through Triple DES

Shubham Kumar
GCET, Greater Noida
Branch: IT
VIII Semester

Saurabh Yadav
GCET, Greater Noida
Branch: IT
VIII Semester

Deepak Kumar
GCET, Greater Noida
Branch: IT
Assistant Professor

ABSTRACT
Secured Communication of data inside an organization is very important issue particularly when the communication is taking place outside the organization. It is very important for the organization to know the kind of data which is being shared by the employee of that organization to outside world. Encryption is an essential tool for protecting the confidentiality of data. Network security protocols such as SSL or IPSec use encryption to protect Internet traffic from eavesdropping. Encryption is also used to protect sensitive data before it is stored on non-secure disks or tapes. Encryption, however, is computationally expensive. A computer server that must encrypt data for thousands of clients before sending it over the network can easily become crypto-bound. The capacity of the server is then determined by the speed at which it can perform encryption. This is especially the case when slow encryption protocols such as the Digital Encryption Standard (DES) or Triple-DES are employed. Since DES and Triple-DES are very widely used, it is important to optimize the performance of these algorithms. Triple-DES (TDES) is basically used in various cryptographic applications and wireless protocol security layers [2]. This paper presents the design and the implementation of the Secured Communication of Data Using Data Dictionary in Triple Data Encryption Standard (DES) algorithm. Data Dictionary is created and used by the admin for the purpose of detection of suspicious communication.

Keywords
Data Dictionary, Data Encryption Standard, Encryption System, Plaintext, Triple DES

1. INTRODUCTION
The secured communication generally depends upon the behavior of users of that organization. In such case, if a particular user will have ill ideas about the organization and that person want to send all the confidential data of the organization to outside world and if there will be no monitoring on the communication then that person can easily send all the confidential document to the outside world and the organization would have to face all the problems afterwards. Here we would monitor the entire communication using a preferred data dictionary. The monitoring of communication is done automatically by matching the suspicious word to the data dictionary. The result of monitoring is redirected to the admin if there will be any suspicious communication detected. The admin can control all users and can remove any user at any time.

Beyond any doubt, the need for secure storage or transfer of information is an inextricable part of human history. Nowadays, the rapid evolution of communication systems offers, to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Therefore, every single transmitted bit of information needs to be processed into an unrecognizable form in order to be secured. This enciphering of the data is necessary to take place in real time and for this procedure cryptography is the main mechanism to secure digital information. Due to the heavy increase in the volume of information data, a variety of encryption algorithms have been developed [1]. Among the different cryptographic algorithms, the most popular example in the field of symmetric ciphers is the Data Encryption Standard (DES) algorithm, which was developed by IBM in the mid-seventies.

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. the rapid advances in the speed of electronic circuitry over the last 20 years, combined with the natural parallelism of Feistel ciphers and DES's relatively small key size, have rendered the algorithm obsolete [5]. 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. Naturally, it is three times slower than the original form of DES but it is way more secure. This paper examines the procedure of securing the communication using data dictionary in triple data encryption standard.

2. PROPOSED SECURED STANDARD FOR COMMUNICATION

2.1 Previous Work
A lot of research & development are going on over DES & Triple DES. DES and Triple-DES are already implemented in Spartan –II devices. DES is also developed using the Handel-C. Triple DES was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys [5].

2.2 Data Encryption Standard
Complete function of DES algorithm can be described briefly as follows [7]. DES is a block cipher. It operates on blocks of 64-bits in size. A 64-bit input block of plaintext will be encrypted into a 64-bit output block of cipher text. It is a symmetric algorithm, which means the same algorithm and key are used for encryption and decryption. The security of DES rests in the 56-bit key. The plaintext block is taken in and put through an initial permutation. The key is also taken in at the same time. The key is presented in a 64-bit block

with every 8th bit being a parity check. The 56-bit key is then extracted ready for use. The 64-bit plaintext block is split into two 32- bit halves, named the right half and left half. The two halves of the plaintext are then combined with data from the key in an operation called Function F. There are 16 rounds of Function f, after which the two halves are recombined into one 64-bit block, which is then put through a final permutation to complete the operation of the algorithm and a 64-bit cipher text block is outputted [4]. The detailed procedure is represented with a flowchart in Figure 1.

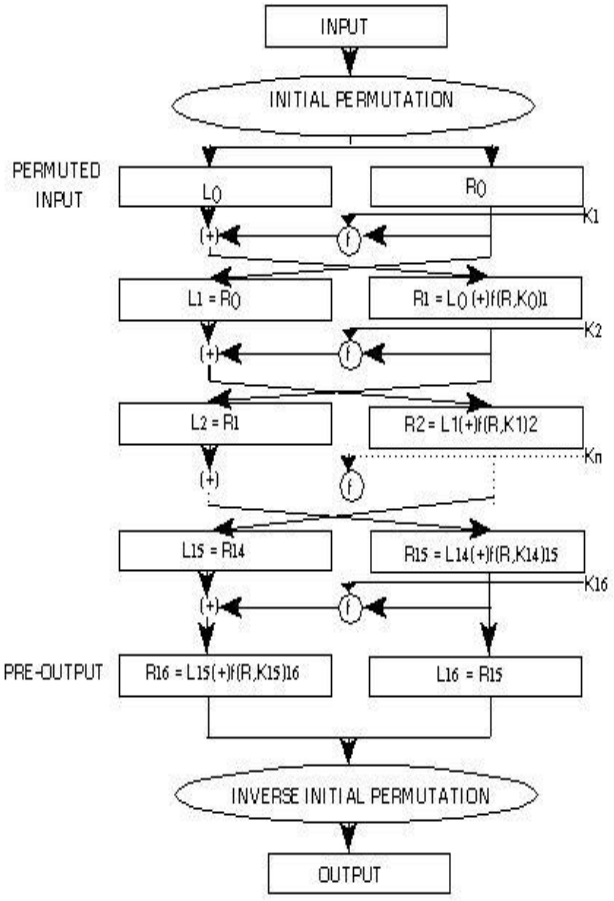

Figure 1: DES Encryption

3. THE F FUNCTION AND KEY SCHEDULE IN DES

As shown in Figure.1 the right half of the plaintext after been expanded from 32 bits to 48 bits is exclusively-ored with a certain round key. The result of this operation is led to the eight following substitution boxes which transforms the 48-bit input to a 32-bit output. Finally a simple permutation (P) is performed before the final output [7].

On each round a certain key is applied. The function f and key is shown in figure 2 and 3 respectively. This key is produced by a specific procedure shown and its characteristic is its two substitution permutations. When the initial 64 -bit key is inserted, a permutation occurs (PC-1) in which every 8th bit of the key is used only for parity check and so its final size is reduced to 56-bits. Then, the key splits in two equal halves of 28-bits and each half is shifted (left, when we have an encryption progress or right, when decryption) zero, one or two bits depending on the number or rounds. After this operation a final permutation occurs [8].

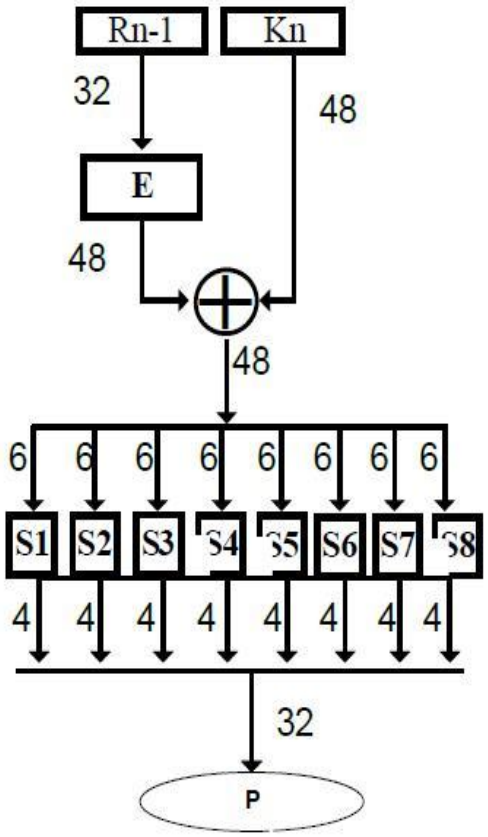

Figure 2: Function f

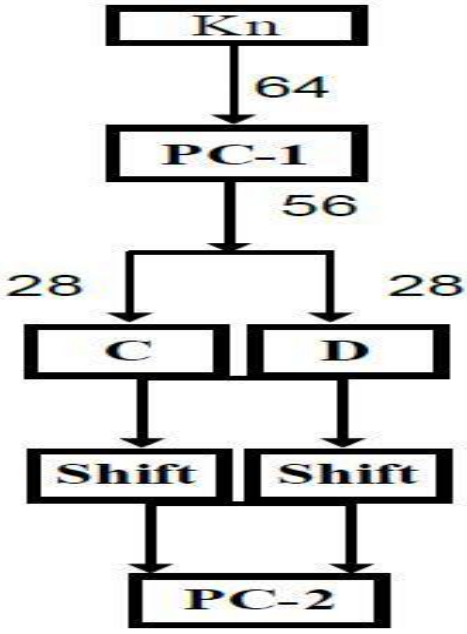

Figure 3: Key Schedule

4. TRIPLE DATA ENCRYPTION STANDARD

A concise representation of Triple Data Encryption Algorithm is described .TDES is a block cipher operating on 64-bit data blocks [2-8]. There are several forms, each of which uses the DES cipher three times. TDES can however work with one, two or three 56-bit keys. This means that the plaintext is encrypted three times [6]. A number of modes of TDES have been proposed:

- DES-EEE3: Three DES encryptions with three different keys.
- DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
- DES-EEE2 and DES-EDE2: Same as the previous formats except that the first and third operations use the same

Let EK(I) and DK(I) represent the DES encryption and decryption of I using DES key K respectively. Each TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations. The following operations are used:

1. TDEA encryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: O = EK3 (DK2 (EK1 (I))).

2. TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: O = DK1(EK2(DK3(I))).

Triple DES using Cipher Block Chaining (CBC) does provide increased security by making it difficult to rearrange cipher text blocks. However, key integrity can still be jeopardized, as described in the 3DES attack, when parts of keys are substituted for other key components and thereby provide knowledge of other keys. By substituting key components, brute force can be used on single-DES keys twice. "This can be done on average in 2 x 2-to-the-55^{th}= 2-to-the-56^{th} steps, which is much smaller than 2 to the 112^{th} (the number of steps needed to try each and every double length 3DES key)". It should be noted that these attacks are effective even when CBC is involved [9].

As can be seen from the above discussion, TDES, in combination with good key management, can provide strong security for the processing of electronic communication. As a consequence, by implementing these technologies where appropriate, our company is able to provide customers with issuer and acquirer services that ensure the integrity, confidentiality, and overall security of their electronic communication.

The implementation of DES and TDES provide high-speed performance with very compact hardware implementation. Implementation of DES and TDES is a flexible solution for any cryptographic system and security layers of wireless protocol. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it to protect user content and system data [10].

The round function of DES is applied sixteen times for TDES as shown in figure 4.

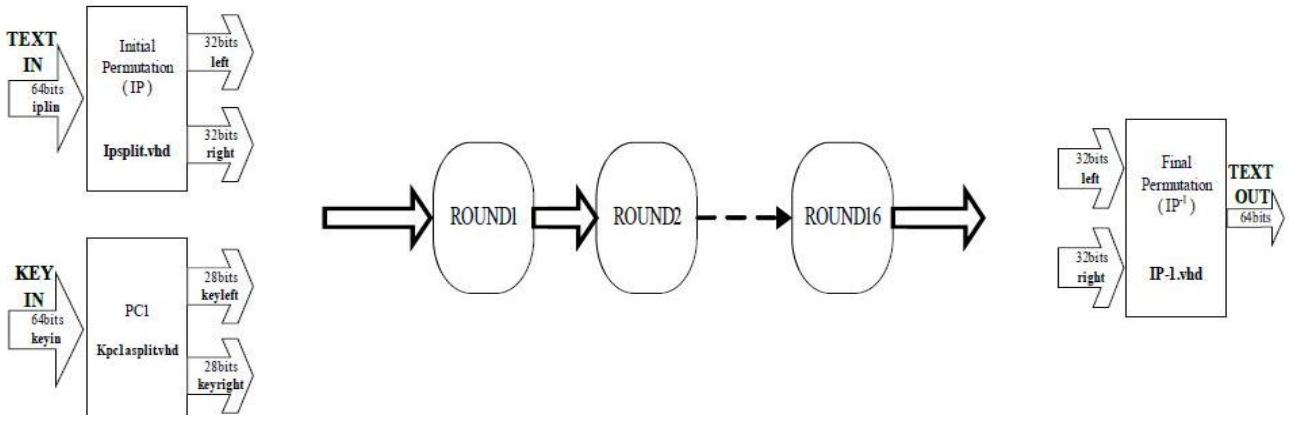

Figure 4: Triple Data Encryption

5. SECURED COMMUNICATION METHODOLOGY

5.1 Modules Description

5.1.1. Admin Login

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

5.1.2. User Login

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

5.1.3. 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.

5.1.4. 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.

5.1.5. Check Harmful Mails for Admin

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

5.1.6. Data Dictionary for Admin

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

5.1.7. View Data Dictionary for Admin

In this module, admin can view the harmful words exists into the data dictionary and also has access to delete the harmful words from the existing data dictionary of harmful words.

5.1.8. 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 harmful activity on the website.

5.1.9. 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 Harmful mail detection module is worked which is detected the sent mails marked as harmful or normal. When the message status sets to normal then it will sent to selected user but if sent message status found to be harmful then it will sent to the admin inbox instead of the selected user inbox.

5.1.10. 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.

5.1.11. 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.

5.1.12. Forum Section for Users

This module is open for all registered users. In this module, users can view the messages which are submitted by other users and then on that message user likes that message or comment on that message and new message is also submitted by that user to open for all registered users. This module is very helpful to share views among other users to take opinion from other users on their submitted message.

Now we will detect the harmful 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. For the security purpose harmful words dictionary is used to detect the harmful words which are not actually used in the normal messaging or communication.

5.2 Method Description

The entire interface of communication will be divided into two kinds of users. First kind of user is admin, who will control the entire communication and will be notified if there will be any malicious mail detected. Second kind is general user, who will be employee in the organization and will communicate among all other users through mails.

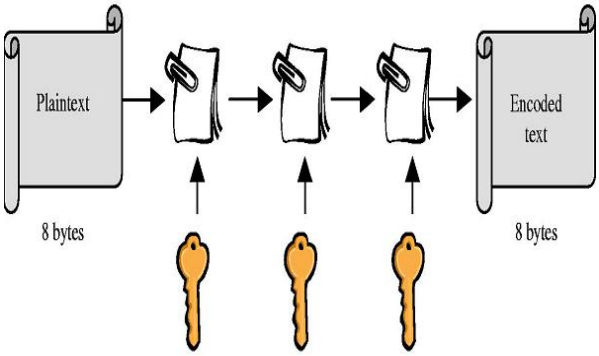

Figure 5: Three Way Verification

Both kinds of users will have login through their user id as registered. An OTP will be sent to the registered email id for login process completion. Admin can send the mail to any of the general users but general users can communicate among themselves only, general user cannot send mails to admin. The message sent by admin will be encrypted using specific key by admin. The security purpose is fulfilled by three way verification as shown above.

In Admin section, the admin will design a data dictionary of words; the dictionary will contain threat words regarding the organization security purpose. As soon as a general user will use the words that were placed in data dictionary the mail will redirect to the admin and will make sure that the mail will not delivered to the desired receiver. Admin will know the entire information such as the source of the mail, destination of the mail and content of the mail and admin will take the appropriate action against the general user if required.

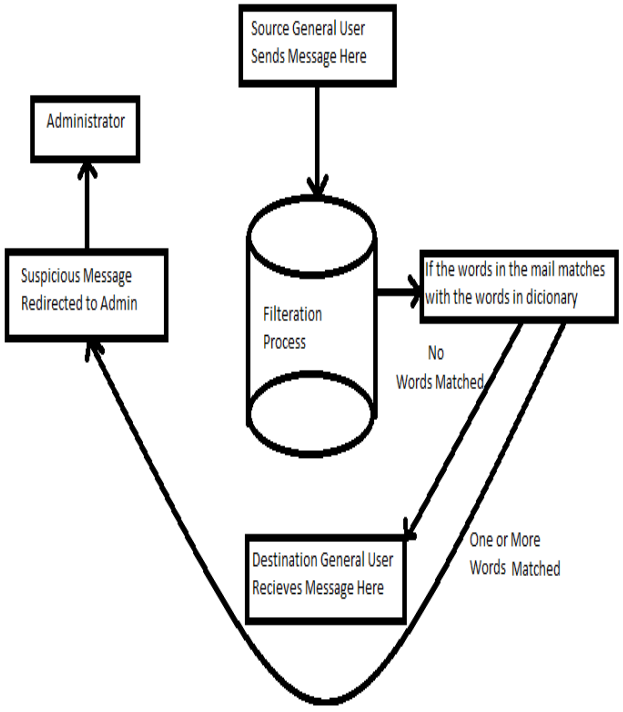

Figure 6: Message Filtration Process

When admin send the mail to any general user, he will encrypt the message using any specific key of his desire. The key will mailed to that specific user who receives the encrypted mail. The general user will use that key for the decryption purpose.

When two general user communicates the message will not be encrypted as the key will mailed to that user only and if the mail consist any malicious word then the redirection of message towards the admin will not be possible as the encrypted word is of no meaning and also the admin cannot decrypt the message because he does not have the key by which the message will be decrypted.

6. CONCLUSION

The proposed implementation of secured communication using data dictionary secures the communication totally on the basis of the word stored in the dictionary. So the words that we will store in the data dictionary must be very threatening word regarding the organization. The implementation provides a method for the communication security and it basically deals with the stealing of information and secured data of an organization. This method solves the problem definition by detecting the harmful mails. Admin creates the data dictionary of harmful words and this data dictionary will help to detect the harmful activity of the users. Admin further will add the harmful words into the existing Harmful Words data dictionary.

7. REFERENCES

[1] "Data Encryption Standard (DES)", Federal Information Processing Standard Publication, FIPS PUB 46-3, National Bureau of Standards, 1977.

[2] P. Kitsos, S. Goudevenos, "VLSI implementations of the triple-DES block cipher", Electronics, Circuits and Systems, ICECS 2003, Proceedings of the 2003 10th IEEE International Conference, pp 76-79, vol. 1, 2003

[3] S. Praveen, M. Nagesh, "Implementaion of the Triple DES Block Cipher using VHDL", International Journal of Advances in Engineering & Technology, pp. 117-128, vol 3, issue 1, 2012.

[4] O. Hamdan, B. Zaidan, "New Comparative Study between DES, 3DES and AES within Nine Factors", Journal of Computing, pp. 152-157, vol 2, issue 3, 2010

[5] R. Shantamurty, "Implementing Triple DES (TCBC) on OpenVMS", OpenVMS Technical Journal, V15, 2010

[6] Aqib Al Azad, "Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA", International Journal of Computer Applications, pp. 6-15, vol 44, No. 16, 2012

[7] V. Kakarla, N.S.Govind, "FPGA Implementation of Hybrid Encryption Algorithm Based on Triple DES and RSA in Bluetooth Communication", International Journal of Applied Research & Studies, vol. 1, 2012

[8] Mandeep Singh Narula, Simarpreet Singh, "Implimentation of Triple Data Encryption Standard" Volume 4, Issue 1, January 2014

[9] Accredited Standards Committee X9, Inc. "American National Standard for Financial Services: ANS X9.24-2002."American National Standards Institute. Approved November 8, 2002.

[10] Koc, Cetin Kaya. "Security & Cryptography Notes."Fall Term 2003 –CRN: 17733. School of Electrical Engineering & Computer Science, Oregon State University.