Implementation of Secure Cryptographic Key Techniques for DES Algorithm using Verilog HDL

[1]Vangmai Sheshatwam, [2]B Sreekanth Reddy
[1]M.Tech, [2]Asst. Prof, M.S, ECE dept.
[1]Electronics and Communication Department
[1]G. Narayanamma Institute of Technology and Sciences, Hyderabad, India

Abstract : Now a day, Cryptography plays a major role to achieve the goal of secure communication and avoid an unauthorized access of data. Secured key assumes a vital part in cryptography. In this proposed concept Data encryption standard (DES) Algorithm is used as it is well-suited for the VLSI implementation of low-cost lightweight cryptography applications. Any cryptographic algorithm security mostly relies on the privacy of the key. To increase the level of security, "Dynamic Key Theory" is presented and analyzed in this paper. Dynamic key method enhances the DES algorithm securities using multiple key generation techniques to achieve the goal of secure communication. For implementation, this project is done in two parts, one is DES algorithm part other is key generation part using multiple keys. To control the rounds of DES encryption/decryption mode, control unit starts to operate. The proposed architecture is modeled using Verilog HDL in Xilinx ISE. Simulation results can be verified using either Mentor Graphics Tools or Xilinx ISE. Figures of merit are implemented to understand the performance of different keys.

Keywords: Cryptography, DES, GRAY-X, Dynamic Key, Security.

I. INTRODUCTION

In modern security models, cryptography has major importance in protecting data and security in any communication. It is the way of protecting the data from any illegal access through unauthorized persons or hacking of information [1]. Cryptography includes two parts encryption and decryption, encryption is the process of converting direct input plain text to scrambled output cipher text and similarly decryption is the process of converting back cipher text to the plaintext [3]. For conversion, cryptography consists of two main techniques based on the usage of key in the encrypted algorithm; they are Symmetric and Asymmetric cryptography. In symmetric cryptography, same key is used to encrypt and decrypt the data but in asymmetric cryptography different keys are used to encrypt and decrypt the data [10]. Both has pros and cons. Due to its characteristics, asymmetric cryptography is more secure compared to symmetric in key functions but the key size in asymmetric cryptography must be ten times or more of a symmetric cryptography key in order to have a similar level of security. Security of the data or system depends on both cryptographic algorithm and key used for encryption/decryption. Many applications, including telecommunication electronic passwords, ATM cards, health-monitoring and biometric data based recognition system, need short-term data security.

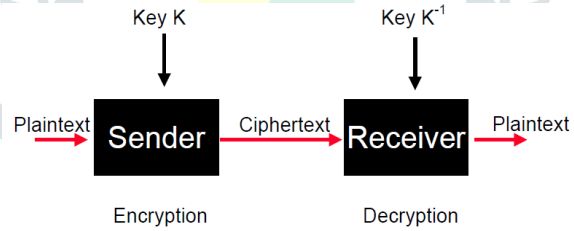

Fig 1: Basic Cryptography Model

To design short-term security based applications, there is an essential need of high-performance, low cost and area-efficient VLSI implementation of lightweight ciphers [1]. Data encryption standard (DES) is best for the implementation of low-cost lightweight cryptography applications. Hence we are using DES Algorithm in the proposed concept. The DES algorithm is a block cipher which operates on the 64-bit plaintext and same 64-bit key for both encryption and decryption. 64-bit plaintext and 64-bit key combinely produces the 64-bit encrypted cipher text for decryption same process is done in reverse i.e., with cipher text and key produces plaintext. To maintain the confidentiality of any cryptographic algorithm which is based on the privacy of the key, dynamic key theory is described and mathematically analyzed in this paper to achieve the goal of secure communication. This proposed work is divided in two parts, first one implementation of DES algorithm and second is dynamic key generation using different key techniques such as direct key by used, LFSR & 2's Complement of direct key.

II. LITERATURE SURVEY

This section involves the work done by the researchers for exploring the cryptographic algorithm in the area of data security of any communication.

T. Rajani Devi explains the importance of cryptography and provides a broad review of network security. A general overview of data security and cryptography and various cryptographic algorithms are discussed in "Importance of Cryptography in Network Security",2013.[6]

M. E. Smid and D. K. Branstad, elaborate the changes in Data encryption standard: past and future and analyses the change of algorithm computation, which is the scrutiny of data encryption, an improvement that obliges a safe, secure and private information sector.[7]

J. G. Pandey, Aanchal Gurawa, Heena Nehra, A.Karmakar shows the FPGA Implementation of an Efficient VLSI Architecture for Data Encryption Standard algorithm related to encryption and decryption technique.[1]

Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar established the DES count the rearrangement framework is added before the DES computation to show out its procedure[4].

prashanti.g, deepthi.s, sandhya rani.k says in "A Novel approach for data encryption standard algorithm" that to enhance the DES algorithm by substituting the 8/32 S-Box by 6/4 S-Box and then a New operation of modulo-2 is permorfomed during the 16 rounds of des instead of regular XOR operation. They explained about modified s-box operation for improving the privacy. This develops the performance of the DES algorithm and security level also gets enhanced.[8]

Hitesh Mittal and Ajay Kakkar explained in "Performance analysis of multiple keys used for data security" that the importance of dynamic key theory for secure data communication and performance analysis of different keys used in various cryptographic algorithms as it is an essential factor of an organization in order to keep the data safe from the unauthorized persons, it helps in securing the data.[9]

III. SYSTEM DEVELOPMENT

3.1 DES Algorithm

Data Encryption Standard (DES) Algorithm is a symmetric key block cipher which uses same key to encrypt and decrypt the given input data. DES algorithm takes 64bit input plain text and produces 64bit output cipher text with the help of 64bit input key.

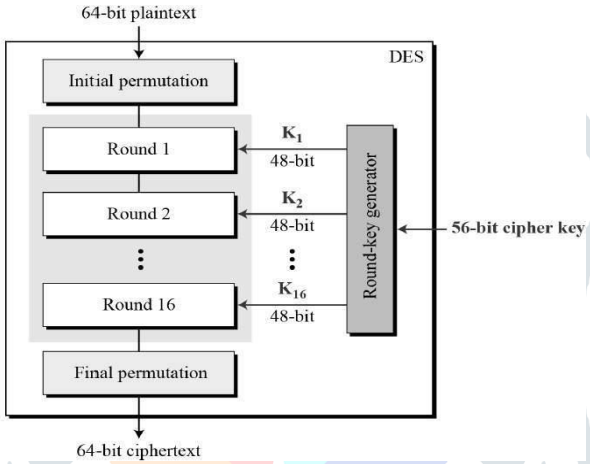

Fig.2 DES Algorithm

First, Input plain text is sent to initial permutation(IP) and is divided into two registers i.e., left half and right half 32bit each and are permuted and right 32bits are expanded to 48bit by using expansion function. DES algorithm has 16 rounds of operations to produce the output. 64 bit input key is performed internal permutations and gives sixteen 48bit subkeys such that each subkey is given to a single round of operation and is Ex-or'ed with the expanded 48bits and sent as input to the S-box. S-box is a LUT(Look up table) which consists of 6bit -input and 4bit output. As 48bit input to S-box divides them into 8 S-boxes which converts into 32bit output each box consisting of 4bit data and finally these 32bit is permuted and XOR'ed with left half 32bit and complete 64bit data is sent to Inverse initial permutation(IP-1). DES Algorithm and its function is shown in fig2 and fig3 below.

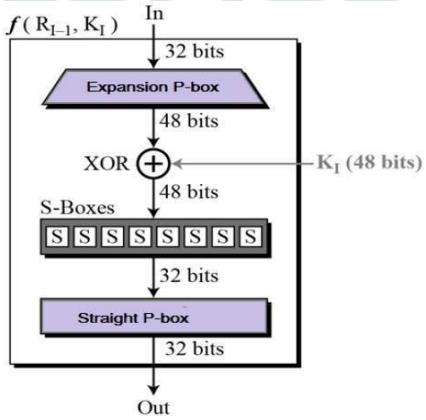

Fig.3.DES function details (F)

3.2 Existing Key Techniques

Key generation techniques are implemented individually to encrypt and decrypt the data. Some of the existing keys that are used as input for key generation block are

3.2.1 Direct key

Direct key is a simple 64bit key given by the user and is passed to the DES algorithm directly.

3.2.2 2's Complement

This is another key technique used to make more generations of keys. Here 2's complement is performed using direct key. It's equation is as follows:

2's complement = 1's complement + 1

1's complement = (2^n) – N

3.2.3 Linear Feedback Shift Register (LFSR)

LFSR is a simple shift register which contains sequence of bits which functions with a linear feedback. Taps are the inputs given to the XOR and applied to the feedback as shown in fig.4. Here LFSR is used to create different combinations of bits in the arrangement of keys. Similarly LFSR is also performed here using direct key.

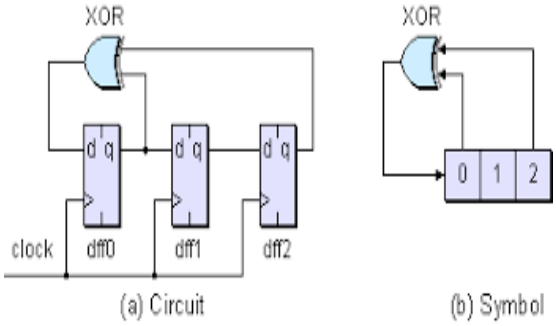

Fig. 4 LFSR

3.3 Proposed Key Technique

To increase the level of security compared to the existing techniques which are mentioned above, a new technique is proposed i.e., "GRAY-X" based on gray code conversion and additional XOR logic applied to it.

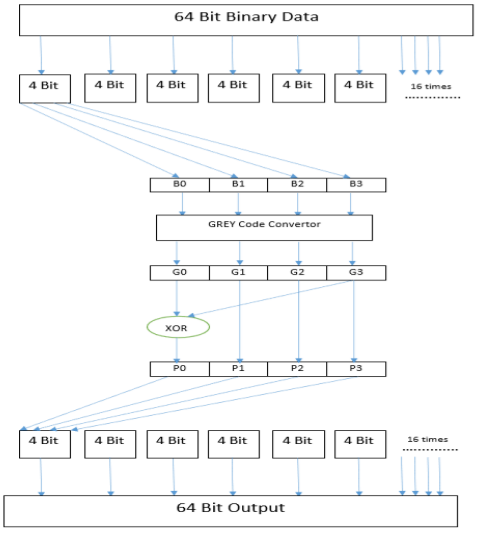

Fig. 5 GRAY-X key Technique

To get abnormal state of security and create more confusion, a special key algorithm technique called GRAY-X is designed. The operation is based on gray code conversion with an external XOR logic. Addition of external logic helps us in protecting the privacy of key structure. Unauthorized person cannot estimate the key used simply by comparing the input and output values. First, 64bit binary key is divided into 16 registers 4bit each and then each register undergoes gray code conversion. After converting the data 1st and 4th bit of each 4bit register is XOR'ed and placed in 1st position, remaining bits would remain the same. Thus, 16 4bit registers are combined together to get 64bit encoded output. The operation is shown in Fig.5. The design is implemented in Xilinx software and the simulation results are shown in section 5.

IV. DYNAMIC KEY THEORY

As per the research done, DES Algorithm is weak due to its weak key generation. As the key plays a vital part in DES algorithm, guessing the key must be more problematic to decrypt the algorithm. Therefore to make the key generation more effective and strong and overcome the limitations in maintaining the secrecy of data and dynamic key theory is introduced. Dynamic key theory mainly helps in eliminating "brute force attack" as DES has 56 bit key which is very weak. So to improve the performance of algorithm and to enhance the secrecy of the data dynamic key theory uses multiple keys with the help of multiplexer and sends the particular key to the algorithm at particular instants of time with the help of selection lines. Here direct key is the original key and the other keys generated are dependent on the direct key input and then sent to multiplexer. The different combinations of output keys are given to the DES algorithm by increasing the level of performance and security. Block diagram of dynamic key theory is shown in Fig. 6 below.

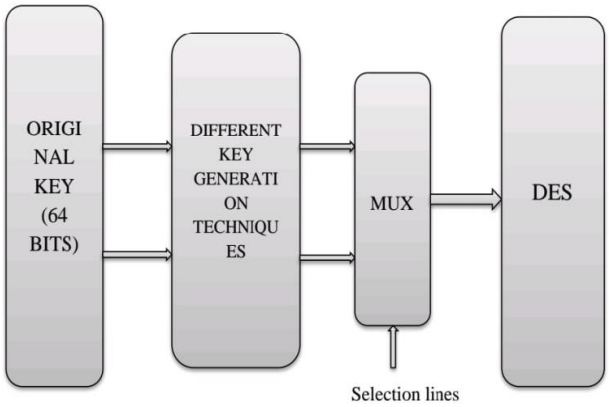

Fig. 6 Block diagram of Dynamic key theory.

V. RESULTS AND DISCUSSION

DES Algorithm is implemented with Verilog and RTL level is simulated with Xilinx ISE 13.3 simulator. Simulation results of proposed key GRAY-X algorithm with encrypted and decrypted outputs are shown in Fig.7. Simulation results of different keys using dynamic key theory is shown in Fig 8. By using direct key input[sel:00] and the selection lines, the output keys of 2's complement for [sel:01], LFSR for [sel:10] and proposed key for [sel:11] are generated.

In Fig 9, simulation results contains the DES Algorithm encrypted output ie., 64bit cipher text with the original 64bit key directly. The input plain text given to the DES Algorithm is 0123456789ABCDEF and the 64bit input key taken as 133457799BBCDFF1. Finally, entire encrypted algorithm simulation results are shown in Fig 10. which contains the encrypted 64 bit output cipher text of different key techniques generated through a single key using dynamic key theory with slight increase in delay.

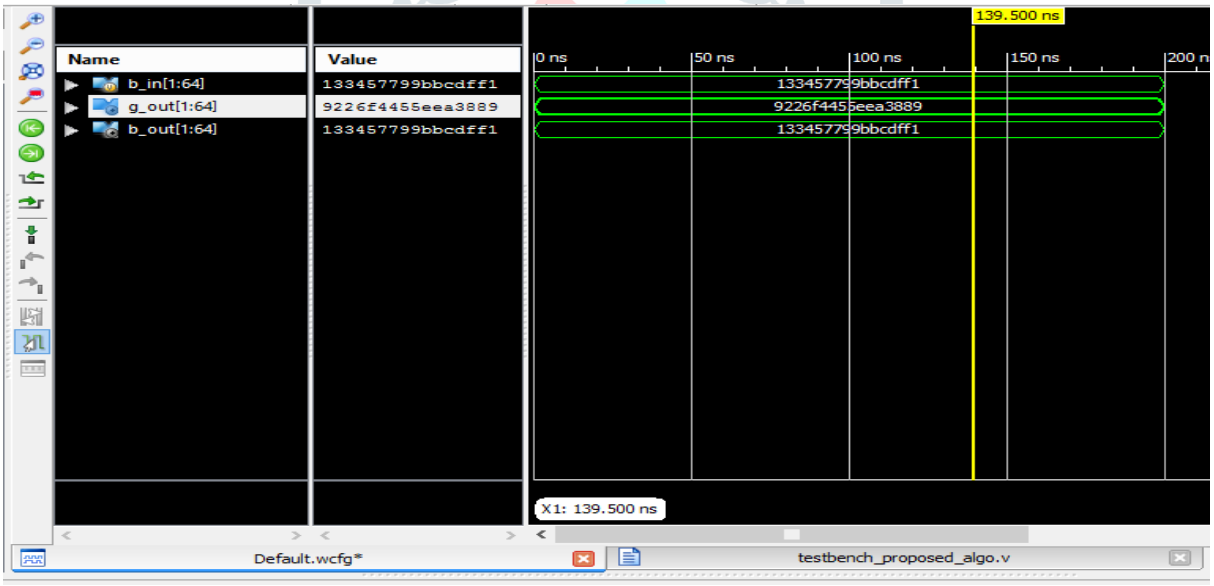

Fig.7 Proposed key "GRAY-X"

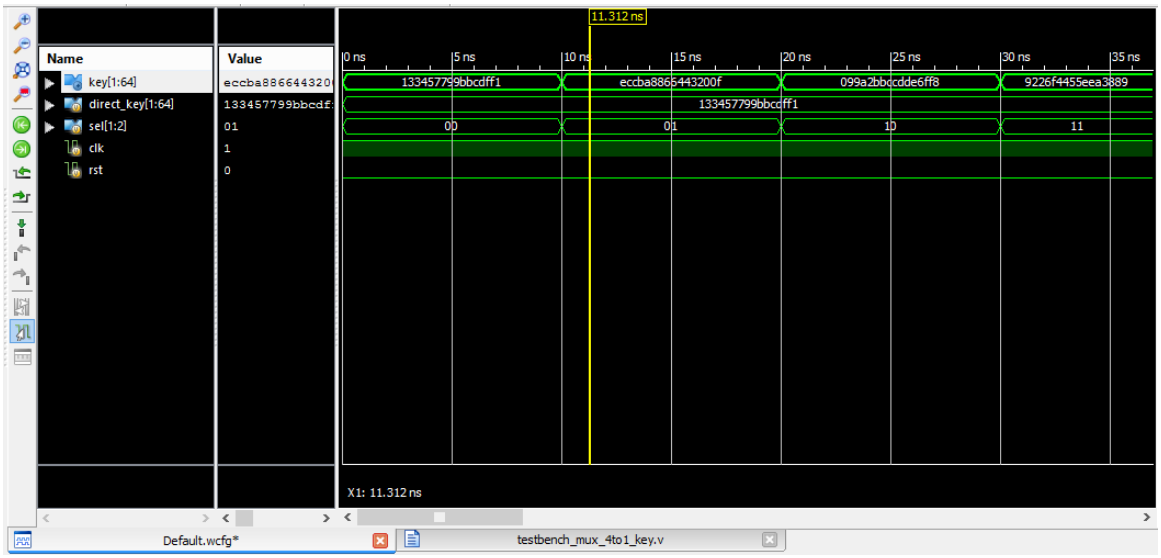

Fig.8 Results of Dynamic key Theory using original key

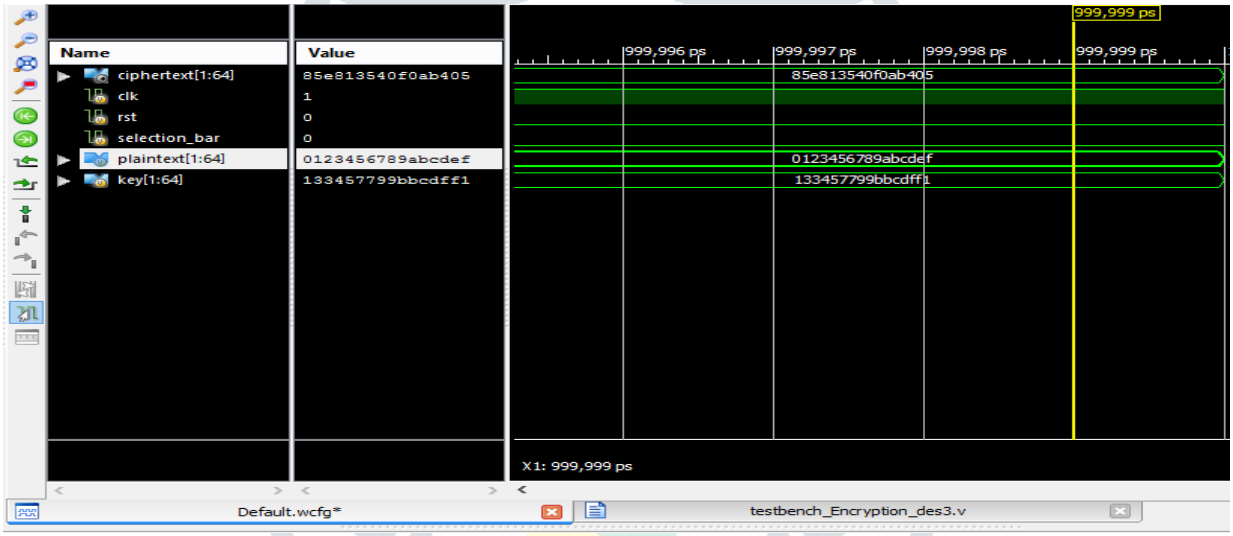

Fig.9 DES Encryption with a simple key

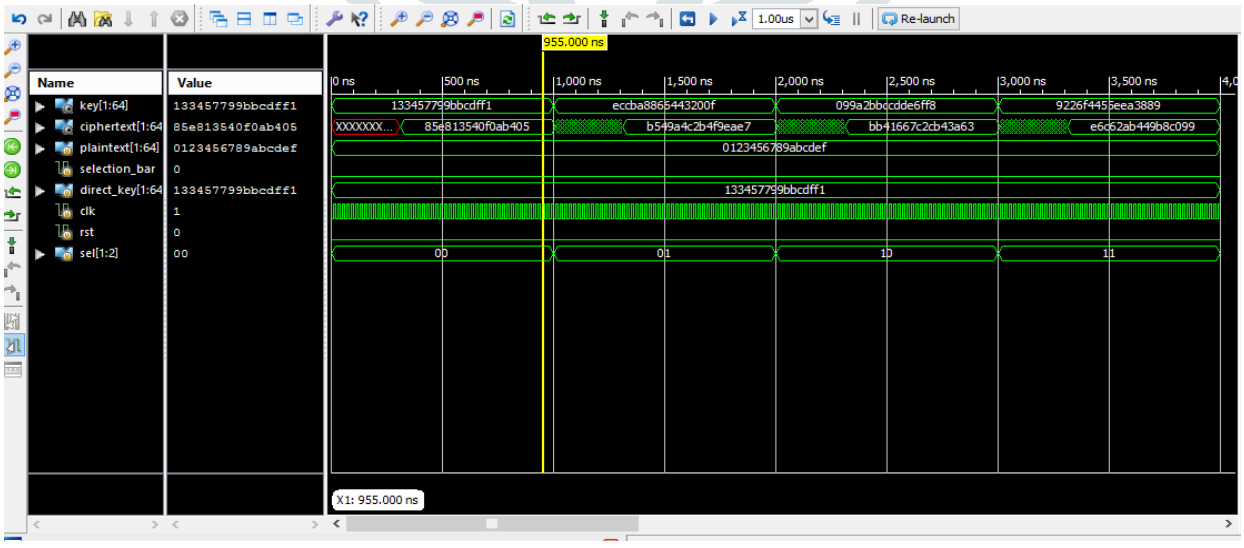

Fig.10 Encrypted results of DES Algorithm with different key techniques

VI. ACKNOWLEDGMENT

This research was supported by G. Narayanamma Institute of Technology and sciences. We are thankful to all the faculty of the department who provided immense support for this research.

REFERENCES

[1] Punam Milind Chabukswar, Manoj Kumar, P. Balaramudu, "An Efficient Implementation of Enhanced Key Generation Technique in Data Encryption Standard (DES) Algorithm using VHDL", International Conference on Computing Methodologies and Communication (ICCMC), 2017

[2] J. G. Pandey, Aanchal Gurawa, Heena Nehra, A. Karmakar, An Efficient VLSI Architecture for Data Encryption Standard and its FPGA Implementation, International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA), 2016 .

[**3]** William Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall publication, page no.51-56, 2011.

[4] Sombir Singh, Sunil K. Maakar, Dr. Sudesh, Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques, International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Volume 3, Issue 6, June 2013.

[5] O. P. Verma, R. Agarwal, D. Dafouti, and S. Tyagi, "Peformance Analysis of Data Encryption Algorithms," in 3rd Int'l Conf. on Electronics Computer Technology (ICECT), vol. 5, Kanyakumari, 8-10 Apr. 2011, pp. 399-403

[6] T. Rajani Devi "Importance of Cryptography in Network Security", International Conference on Communication Systems and Network Technologies, 2013.

[7] M.E. Smid, D.K. Branstad "Data Encryption Standard: Past and Future", Journals & Magazines proceedings of the IEEE, Volume:76 Issue:5.

[8] Prashanti.G, Deepthi.S, Sandhya Rani.k "A Novel Approach for Data Encryption Standard Algorithm", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249-8958, Volume-2, Issue-5, June 2013.

[9] Hitesh Mittal, Ajay Kakkar, "Performance Analysis of Multiple Keys used for Data Security", International Journal of Computer Applications, Volume:95, Issue:14,2014.

[10] C. Radha, P. Sakthi Priyanka, Dr.S.Prabha, "Enhanced Hybrid Cryptography Technique To Secure The Network", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 19 Issue 2 – JANUARY 2016.

[11] S. Kelly. Security implications of using the Data Encryption Standard (DES). (2006, Dec.) [Online] https://tools.ietf.org/html/rfc4772.

[12] https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

[13] https://www.cybrary.it/0p3n/des-data-encryption-standard/