ISSN 2250-3153

A block based Encryption Model to improve Avalanche Effect for data Security

[1]Ganesh Patidar, [2]Nitin Agrawal, [3]Sitendra Tarmakar

M.Tech. Scholar, CSE NIIST, Bhopal, patidar_g23@yahoo.co.in
Asst Prof CSE NIIST, Bhopal, seonitin79@gmail.com
Coordinator M.Tech NIIST, Bhopal, sitendra.tamrakar@yahoo.co.in

Abstract- Encryption is widely used to ensure security in public networks like the internet. Any type of data has its own attribute; therefore, various algorithms should be used to protect confidential data from unauthorized access. Mostly the available encryption algorithms are used for text data. However, due to large data size and real time constrains, algorithms that are good for textual data. In this research, a block-based encryption model is proposed for information security using a combination of logical and mathematical operation. This model will be used as a pre-encryption technique to confuse the relationship between the original data and the generated ones. The generated data are then fed to the proposed encryption model. Efficiency, Avalanche Effect, and Execution Time have been used to measure the security level of the data. The experimental results have shown that the existing algorithms resulted in a lower efficiency, a higher execution time, and a more uniform efficiency. This implies a high similarity and a good quality of the retrieved data compared to the original one. Another feature of the proposed model is its generality; it can be applied with any other traditional algorithm to enhance its performance. Experimental results have shown that using the proposed model along with the other algorithms resulted in a better performance compared to using the other algorithms alone.

Index Terms- Encryption, Decryption, Cryptography, Avalanche Effect

I. Introduction

In Usage of Cryptography or the art of hiding messages dates back to 1st century B.C. Ancient ciphers used the process of scrambling of the message to encipher. One serious drawback with this method is that it is prone to brute force attack. Modern methods are less affected by brute force attack because of the usage of keys. The use of the symmetric key encryption is common to ensure data integrity. Symmetric key encryption code can be divided into the block cipher and stream one, and block cipher algorithm has been developed extensively. In symmetric block ciphers, substitution and diffusion operations are performed in multiple rounds using sub-keys generated from a key generation procedure called key schedule. The key schedule plays a very important role in deciding the security of block ciphers. Currently, famous block cipher algorithms were made by the public project such as AES (Advanced Encryption Standard), DES (Data Encryption Standard, Triple Data Encryption Standard (TDES), International Data Encryption Standard (IDEA) Blow-Fish (BF) and RC6. Hardware and software implementation can be done of the existing algorithms, the important thing which type of implementation is more useable in this field. Hardware implementation is too fast but implementation is very difficulty and not easy to understand, so most of the user have preferred software implementation of the exiting algorithm, proposed research has also concentrate on the software implementation. The block cipher can be categorized into Feistel structure and SPN (Substitution Permutation Network) one. Feistel structure has an advantage of the same algorithm between encryption and decryption, and the feature of SPN structure is that it has a different algorithm between encryption and decryption. In particular, the SPN structure has a disadvantage that its area increases twice compared with the Feistel one when SPN structure is implemented via hardware. Commanly all most all existing algorithm require 128-bit and variable-length block cipher encryption algorithm except DES (64) and TDES (192). Proposed encryption model has a modified Feistel structure and a advantage that it has no different algorithm between encryption and decryption. Thus, the proposed encryption model no needs for any extra space compared with the same structure of encryption and decryption at the time of implementation on software. The proposed encryption model has the same structure of encryption and decryption. We devise our model by inserting a symmetric layer using simple rotation and XOR operations. The symmetry layer is put between encryption part and decryption one. The proposed encryption model has the almost high speed compared with the existing algorithms. Nevertheless, the proposed encryption model improves encryption security by inserting the symmetric layer because a differential and linear analysis has a difficulty in ANALYZING AN ENCRYPTED STREAM. FINALLY THIS PAPER IS THE STUDY of key size, security setting and efficiency, speed of an algorithm, and more important thing avalanche effect of an algorithm which is objective of this research. After the detailed study of each algorithm, this research presents some prone and crones of existing algorithm and how it can remove with the help of proposed encryption model. Rest of the paper is dividing in three sections. Section II presents literature survey, section III presents proposed work and section IV present evolution technique and conclusion.

II. Literature Survey

Cryptography is one of the ways to secure electronic documents and encryption is the important in Data and Network Security. The aim of this study is to enhance the strength of already existing technique. The drawback in that technique was inefficiency of Key generation which is essential for any Encryption Algorithm; the prolific growth of network communication system entails high risk of breach in information security. This substantiates the need for higher

security for electronic information. TRIPLE SV (3SV), with 256-bit block size and 112-bit key length method has suggested [1]. Generally, stream ciphers produce higher avalanche effect but Triple SV producing good avalanche effect with a block cipher implementation. The CBC mode has been used to attain higher avalanche effect. Suggested technique has implemented in C language [1]. Another key generation technique "Fauzan-Mustafa Encryption Technique (FMET)" has been suggested in [2]. This is also working in the field of high security. A session based symmetric key cryptographic system has been proposed and it is termed as Bit Orientation Technique (BOT) [3]. BOT consider the plain text (i.e. the input file) as binary string with finite no. of bits. The input binary string is broken down into manageable-sized blocks to fit diagonally upward from left to right into a square matrix of suitable order. Bits are taken row-wise from the square matrix to form the encrypted binary string and from this string cipher text is formed. Combination of values of block length and no. of blocks of a session generates the session key for BOT. For decryption the cipher text is considered as binary string. Using the session key information, this binary string is broken down into manageable-sized blocks to fit row-wise from left to right into a square matrix of suitable order. Bits are taken diagonally upward from left to right from the square matrix to form the decrypted binary string and from this string plain text is formed. Another complex key generation procedure based on matrix manipulations has introduced in [4]. In this describes the matrix based key generation procedure and the enhanced key avalanche and differential key propagation produced in AES. It has been shown that, the key avalanche effect and differential key propagation characteristics of AES have improved by replacing the AES key schedule with the Matrix based key generation procedure [4]. In [5] an encryption technique combines the process of scrambling of bits and substitution boxes resulting in high avalanche effect has suggested. In [6] implements some of the widely used symmetric encryption techniques i.e. data encryption standard (DES), triple data encryption standard (3DES), advanced encryption standard (AES), BLOWFISH and RC4 in MATLAB software. After the implementation, these techniques are compared on some points. These points are avalanche effect due to one bit variation in plaintext keeping the key constant, avalanche effect due to one bit variation in key keeping the plaintext constant, memory required for implementation and simulation time required for different message lengths. In [7] this document reviews some of the classical encryption and modern techniques which are widely used to solve the problem in open networked systems, where information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication. In this suggested building the basics of classical encryption and modern techniques and at least section of paper comparison has been done between each of them.

Problem Identification: Each of the above specified techniques is having their own strong and weak points. In order to apply an appropriate technique in a particular application we are required to know these strong and weak points. Therefore the comparison of these techniques based on several features is necessary. Some of these points under which the cryptosystems can be compared are as follow Avalanche effect a desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts. In the existing technique producing avalanche effect can be raised using more specify operation and structure. Memory is another issue in this filed if any encryption techniques require large memory size for execution then this is the poor implementation. It is desirable that the memory required should be as small as possible. Execution time is also important performance parameter to increase the efficiency of the algorithms. The time required by the algorithm for processing completely a particular length of data is called the execution time. It depends on the processor speed. The smallest value of execution time is desired. Finally study of a previous research its analysed every body is trying to comparing avalanche effect of known cryptography algorithm with his proposed work. Furthermore analysis in the survey that the key size of various algorithms is not fixed which cause of poor efficiency is.

III. PROPOSED WORK

Proposed model will emphasizes on improving avalanche effect as compare existing one. Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text. This change that occurs at the output should be sufficient if we want to create a secure algorithm. Proposed model will extent deals with some of the drawbacks of existing algorithms that includes usage of key as it is without inducing any confusion in the primary key will change by generating keys, similarly the key size 128 bits of proposed concept are fixed. The variation in key introduces the aspect of uncertainty which is a positive aspect when it comes to encryption.

Proposed Evaluation Model:- The proposed model may be useful in several contexts:

- Proposed model will design secure symmetric block cipher algorithms.
- Proposed model can be work as primary model in the filed of cryptography.
- Proposed model can useful in various application like bulk encryption, random bit generation, hashing etc. by choosing proper subset of design decisions and guidelines.
- Proposed model can be implementable on different platforms like microcontrollers, microprocessors, VLSI hardware, MATLAB, .Net, JAVA etc. by choosing proper subset of design decisions and guidelines.

This research presents theory concept of working model. For avalanche effect of the known cryptographic algorithm, it is necessary to describe the detailed evaluation method, as illustrated in Fig.1. We defining one evaluating modes to find whether the key and the plaintext have impact on time consuming of cryptographic algorithms: DPSK (different plaintexts in the same key).

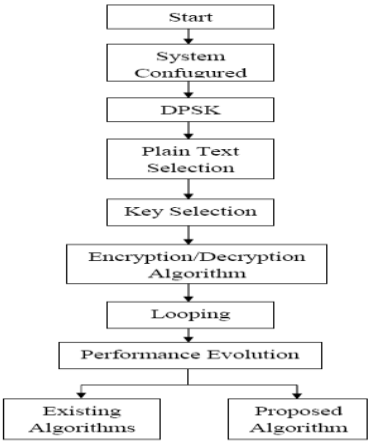

Fig 3: Evolution Model

This evaluation method will compare Avalanche effect of encrypting plaintext with different cryptographic algorithms, Memory Utilization and CPU Utilization. During processing, the content of the plaintext and the key will be both written by the random number. For DPSK evaluation mode, there are two parameters: the number of evaluated plaintexts and the size of evaluated plaintext, where the number of evaluated plaintexts is the number of plaintexts that are generated randomly and the size of evaluated plaintext can be chosen from six kinds that mention above. In this mode, we do n cycles (that is, the number of the evaluated plaintexts).

Why this: - In the private key technique only one key is used for encryption and decryption. In this technique sender and receiver have already know about key before exchange information securely. Important advantages of private key technique are its security and high speed.

Crypto analysis:-. Proposed encryption model is a new block cipher. It has N number of rounds, and 128 bits-length secret key. In Proposed encryption model, the secret key will use to fill an expanded key table which is then used in encryption. Both differential and linear attacks on proposed encryption model will recover every bit of the expanded key table without any exhaustive search. However, the plaintext requirement is strongly dependent on the number of rounds. For 128-bit block size, differential attack on towel-round proposed encryption model uses 2^{45} chosen plaintext pairs (about the same as DES), while 2^{62} pairs are needed for 12-round proposed encryption model. Thus, conclude that 12 rounds are sufficient to make differential and linear cryptanalysis of proposed encryption model impractical.

Advantages: The proposed encryption model offers some advantages are as follow. Proposed model will be fast, suitable and secure for encryption of large files. The proposed encryption model will simple to implement and will have complexity in determining the keys through crypt analysis. Another, the procedure will produces a strong avalanche effect making many bits in the output block of a cipher to undergo changes with one bit change in the secret key.

Some more Advantages are listed below:

- No complex architecture
- Flexibility.
- Reliability
- Highly Efficient
- Good Response Time
- Good Memory Utilization
- Good CPU Utilization
- High Security

I. Results Evolution and Conclusion

Results Analysis: Following parameter will be simulate at the time of results calculation.

- **CPU Utilization:** CPU utilization can be calculated by using equation (1).
  - CPU Utilization (%) = (Used CPU) / (Total CPU capability) * 100 (1)

Existing Technique	Used CUP Capability	%
DES	35	54.68
AES	45	66.23
Blowfish	19	28.71
Caesar Cipher	1	1.56
Vigenere Cipher	2	3.13
Playfair Chiper	4	6.25

- **Memory Utilization:** Memory utilization can be calculated by using equation (2).
  - Memory Utilization (%) = (Used Memory) / (Total Available Memory) * 100 (2)

Existing Technique	Used Memory	%
DES	35	54.68
AES	45	66.23
Blowfish	19	28.71
Caesar Cipher	1	1.56
Vigenere Cipher	2	3.13
Playfair Chiper	4	6.25

- **Throughput:** Throughput can be calculated by using equation (3).
  - Throughput = (Total plaintext in bytes encrypted) / (Total Execution Time) * 100 (3)

Existing Technique	File Size	%
DES	50 KB	60%
AES	50 KB	70%
Blowfish	50 KB	38%
Caesar Cipher	50 KB	2%
Vigenere Cipher	50 KB	4%
Playfair Chiper	50 KB	8%

- **Calculation of Avalanche Effect:** Avalanche effect can be calculated by using equation (4).
  - Avalanche Effect (%) = (Number of Changed Bits in Cipher text) / (Total number of bits in cipher text) * 100..... (4)

Table 1 is showing avalanche effect of existing technique.

Table 1: Avalanche Effect

Existing Technique	%
DES	60%
AES	70%
Blowfish	38%
Caesar Cipher	2%
Vigenere Cipher	4%
Playfair Chiper	8%

IV. Conclusion

From the results calculation its analysed that we can increase performance parameters by using proposed encryption model as compare existing. Also, we can see that the classical ciphers like Playfair cipher, Vigenere Cipher, Caesar Cipher etc. have very less Avalanche Effect and hence cannot be used for encryption of confidential messages. The modern encryption techniques are better than classical ciphers as they have higher Avalanche Effect.

References

[1] Rajdeep Chakraborty, Sonam Agarwal, Sridipta Misra, Vineet Khemka, Sunit Kr Agarwal and J. K. Mandal "Triple SV: A Bit Level Symmetric Block Cipher Having High Avalanche Effect" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011

[2] Fauzan Saeed, Abdul Basit Abdul Qadir, Yar M.Mughal, Mustafa Rashid " A Novel Key Generation for FMET" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011

[3] Manas Paul and Jyotsna Kumar Mandal, "A Novel Generic Session Based Bit Level Cryptographic Technique to Enhance Information Security" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.12, December 2011

[4] Paul A.J., Mythili P. Paulose Jacob K. Matrix based Key Generation to Enhance Key Avalanche in Advanced Encryption Standard International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011 Proceedings published by International Journal of Computer Applications® (IJCA)

[5] Sriram Ramanujam and Marimuthu Karuppiah "Designing an algorithm with high Avalanche Effect" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[6] Himani Agrawal and Monisha Sharma Implementation and analysis of various symmetric cryptosystems" Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010)

[7] Mohit Kumar1*, Reena Mishra2, Rakesh Kumar Pandey3 and Poonam Singh4 "Comparing Classical Encryption With Modern Techniques" S-JPSET, Vol. 1, Issue 1 2010

[8] Bruce Shnier "Applied Cryptography Second Edition Protocols. Algorithms, and Source, and Source Code in C", John Wiley and Sons, Inc., 1996.

[9] Hong S., Deukjo Hong, Youngdai Ko, Donghoon Chang, Wonil Lee, and Sangjin Lee , "Differential cryptanalysis of TEA and XTEA." In Proceedings of ICISC 2003, 2003.

[10] Fauzan Saeed and Mustafa Rashid, "Integrating Classical Encryption with Modern Technique", IJCSNS Vol. 10 No.5.

[11] V. Umakanta Sastry , N. Ravi Shanker and S.Durga Bhavani "A modified Playfair Cipher Involving Interweaving and Iteration" International journal of Computer theory and Engineering Vol.1,No. 5, December,2009 .

[12] V. Umakanta Sastry1, N. Ravi Shankar2, and S. Durga Bhavan "A Modified Hill Cipher Involving Interweaving and Iteration" International Journal of Network Security, Vol.11, No.1, PP.11{16, July 2010