Comparative Analysis - Performance, Efficiency and Security Measures of Block Cipher Algorithms

[1]Sumit Sharma, [2]Mrs. Shobha bhatt
[1]Student (M.tech(IS)), [2]Assistant professor
CSE Department, AIACTR

***Abstract*- The security of data is an important aspect and encryption algorithms play an important role to provide the security to data. The main aim of the cryptography is to enhance the data confidentiality and privacy by making data un-readable. Hence the data cannot be interrupted by the attackers. The Encryption techniques and various algorithms are used to provide the security to the applications. This paper provides a performance comparison between the various symmetric key algorithms such as the AES, DES, BLOWFISH and Binary tree approach. We have compared various parameters for the symmetric key encryption. The parameters such as the tunability, key length, computational speed, and the type of attacks on the security issues are provided. As a result, the better solution to the symmetric key encryption is provided.**

Index Terms- Cryptography, Encryption, AES, Symmetric key encryption

I. INTRODUCTION

The demand for the ubiquitous personal communications is driving the development of new networking techniques. In the communication the security of the data plays the vital role. To improve the security of the data being transmitted various techniques are employed. The important method used to provide the confidentiality is the data encryption and decryption technique. Network security becomes more crucial when the volume of the data becomes larger and complex. Cryptography is the art of transforming the information's on the applications into scrambled or in unintelligible format. It relates to the study of mathematical techniques related to the aspects of information security such as the confidentiality, data integrity, and authentication of the data. The technology used for this is called as the cryptology. When the user defined input may in any of the format such as the text, or an image is which is plain, is converted into a scrambled form called as the cipher text or cipher image. This process is referred to us as encryption. To convert the data the user should provide the specific algorithm. The reversible process in which the original data is recovered is called as the decryption process. In cryptography majorly three types of encryption techniques are taken place such as The substitution technique, the transposition technique and the transposition-substitution technique.

The most important type of the encryption type is the symmetric key encryption. In the symmetric key encryption both for the encryption and decryption process the same key is used. Hence the secrecy of the key is maintained and it is kept private. It works with high speed. The symmetric key encryption takes place in two methodologies either as the block ciphers or as the stream ciphers. One of the main advantages of using the symmetric key encryption is that the computational power to this encryption technique is small. The keys for this are unique or there exists a simple transformation between the two keys. The strength of the encryption algorithms is based on how it is vulnerable to the attacks made on it. The major attacks on the encryption techniques are such as the chosen-plain text attacks, known – plaintext attacks, brute force attacks, linear cryptanalysis etc. To avoid these attacks needed security measures should be enhanced with the encryption.

II. RELATED WORK

In this section the various methodologies and techniques for the encryption techniques used by various papers are provided. In the paper proposed by Jolly Shah and Dr. Vikas Saxena, the various performance factors such as the computational speed, tunability, format compliance, the visual degradation after the encryption and the security issues are proposed.

Vidyasagar Potdar, Elizabeth Chang in their paper proposed the technique to encrypt the text and made it hidden and evaluated the various security issues that are araised.In the paper proposed by M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki a Modified AES Based Algorithm for the encryption on text and the images is given.In the paper proposed by Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry the efficiency and the performance parameters of the algorithms when applied for the image encryption is taken place.

In the paper Cryptographic Algorithms for Secure Data Communication, by Zirra Peter Buba and Gregory Maksha Wajiga the asymmetric keys and its performance efficiency, key scheduling are discussed. In the paper, proposed by Gurjeevan Singh, Ashwani Kumar Singla, and K.S. Sandha the performance metrics for the symmetric key algorithms and their results are discussed.

III. PROPOSED WORK

In this section we give the overview of the symmetric key encryption techniques and the parameters that are verified for the algorithms and the security issues are briefly placed in the following sub sections:

Symmetric Key Encryption

The most important type of the encryption type is the symmetric key encryption. In the symmetric key encryption both for the encryption and decryption process the same key is used. Hence the secrecy of the key is maintained and it is kept private. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption. A block cipher is taken as the input, a key and input, and then the output block will be same in size in most of the symmetric key encryption.

The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. In the block cipher mode the whole data is divided into number of blocks and based on the block the key is provided for encryption. In the case of the stream ciphers the data is divided as small as single bits and randomized and then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems. The performance evaluation is taken place for the following symmetric key encryption techniques such as AES Algorithm, the DES algorithm, Blowfish algorithm and the binary tree approach.

1) The AES Algorithm

The encryption algorithm is an integral work of encryption and decryption process. They should preserve high security to the data being transmitted. Basically, encryption algorithms are divided into three major categories – transposition, substitution, and transposition – substitution technique. Internally the AES algorithm's operations are performed on a two dimensional array of bytes called the state. The state consists of four rows of each bytes, each contains Nb number of bytes, where Nb is the block length divided by 32.

2) The DES Algorithm

Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses using a 56-bit. DES encrypts and decrypts data in 64-bit blocks, using a 56-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks.

3) Blowfish Algorithm

Blowfish algorithm is the important type of the symmetric key encryption that has a 64 bit block size and a variable key length from 32 bits to 448 bits in general. It is a 16 round fiestel cipher that uses the large key size. Since the key size is larger it is complex to break the code in the blowfish algorithm. Moreover it is vulnerable to all the attacks except the weak key class attack.

4) Binary Tree Approach

It uses an approach in which, first we need to break the message into block of the 8 character each. After that, we assign these 8 characters to the leaf nodes of the binary tree of level 3. Other nodes of the binary tree filled using the functions which generates the characters corresponding to the internal nodes of the binary tree. Then we apply another function for transpose the positions of the characters in binary tree. After that we can apply any tree traversal method for generating the ciphertext.

IV. PERFORMANCE FACTORS

In this paper, the following factors are used as the performance criteria, such as the tunability, computational speed, the key length management, the encryption ratio and the security of data against attacks. Now we will discuss these factors one by one:

1. **Tunability -** It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications.
2. **Computational Speed -** In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.
3. **Key Length Value -** In the encryption methodologies the key management is the important aspect that shows how the data is encrypted. The image loss the encryption ratio is based on this key length. The symmetric algorithm uses a variable key length which is of the longer. Hence, the key management is a considerable aspect in encryption processing.
4. **Encryption Ratio -** The encryption ratio is the measure of the amount of data that is to be encrypted. Encryption ratio should be minimized to reduce the complexity on computation.
5. **Security Issues -** Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic security in three levels: low, medium and high.

V. RESULTS AND DISCUSSIONS

This section presents performance and comparison between various algorithms which are discussed above with respect to various parameters such as tunability, encryption ratio, security issues, computational speed and key value. The encryption ratio is measured in terms of either moderate, high or very high. The speed is defined by the following term such as fast, slow, moderate. We specify tunability as either yes or no. The key value is measured in terms of bit value used. The experimental results are implemented using the visual studio .Net packages. After that, we prepare a table which represents the performance of the various algorithms discussed above.

Analysis factors	AES	DES	Blowfish	Binary Tree Approach
Encryption Ratio	High	High	High	Very high
Key Length	128,192 or 256 bits	56 bits	32 to 448 bits	Can be of any length depend on the requirement
Computational Speed	Fast	Fast	Fast	Moderate
Tunability	No	No	Yes	Yes
Security Issues	Chosen plaintext, Known plaintext	Brute force attack	Dictionary attack	Brute force attack

From the above evaluated table we can conclude that the encryption ratio is very high in binary tree approach. The Tunability is presented when we used either blowfish or binary tree approach. The key is chosen of any length in the binary tree approach which is a great advantage of this algorithm. In the aspect of speed the binary tree approach disappointed us but key encryption is viewed as good. Finally, the binary tree approach is specified as the better solution then follows the AES, DES and blowfish algorithm.

REFERENCES

[1] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha , "Performance Evaluation of Symmetric Cryptography Algorithms", IJECT Vol. 2, Issue 3, Sept. 2011 ,ISSN : 2230-9543.

[2] Jolly Shah and Dr. Vikas Saxena," Performance Study on Image Encryption Schemes", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4,2012.

[3] MarwaAbd El-Wahed and Mesbah and Amin shoukry, "Efficiency and Security of some Image Encryption Algorithms", Proceedings of the world Congress on Engineering 2008 Vol I.

[4] Nachiketh Potlapally Srivaths Ravi Anand Raghunathan and Ganesh Lakshminarayana,"Algorithm Exploration for Efficient Public-Key Security Processing on Wireless Handsets", U. S. Department of Commerce, The Emerging Digital Economy II, 2011.

[5] W. Stallings. Cryptography and Network Security, Prentice Hall, 2005.

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based Algorithm for Image Encryption" ,in World Academy of Science, Engineering and Technology, 2010.

[7] Zirra Peter Buba & Gregory Maksha Wajiga,"Cryptographic Algorithms for Secure Data Communication International "in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2, 2011.

[8] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram," comparative analysis of performance efficiency and security measures of some encryption algorithms", International Journal of Engineering Research and Applications,Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.