International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Study and Performance Evaluation of Different Symmetric Key Cryptography Technique for Encryption

Preethi Hebbar[1], Pratheeksha Hegde[2], Shailesh Nayak[3], Sambhav Kerni[4], Rajgopal K T[5]

[1,2,3,4]*Student, Dept. of computer science and engineering, CEC, Karnataka, India*
[5]*Professor, Dept. of computer science and engineering, CEC, Karnataka, India*

Abstract - *Technology is growing day-to-day. In order to have a better and faster technology, information security is a must. This requires data authentication at the execution levels. Cryptography is a useful tool through which secure data independency can be established. Cryptography technique uses two basic operations namely encryption and decryption. A large number of cryptographic techniques have been proposed and implemented so far. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. Proposed project provides a performance comparison between four of the most common encryption algorithms: DES, 3DES, Blowfish and AES. The comparative analysis is done by considering different criteria. Symmetric key cryptography is a cryptographic technique in which the same key is used by both sender and receiver. The advantage of symmetric key cryptographic technique is its less computational cost compared to public key cryptography technique.*

***Key Words*: Symmetric key cryptography, AES, DES, Blowfish, One-time pad**

1. INTRODUCTION

The process of concealing the messages to introduce secrecy in information is considered as cryptography. The process of hiding a message is encryption. The output obtained after encryption is ciphertext. The process of obtaining plaintext from ciphertext is decryption. Cryptography is the technique of using mathematics to encrypt and decrypt data. Cryptography helps us to store sensitive information and allows only intended receiver to access it. Symmetric-key algorithm use the same keys for both encryption and decryption.

AES stands for Advanced Encryption Standard. It is known as block cipher with a block length of 128 bits. AES supports three key sizes, they are 128, 192, and 256 bits. The AES is also known as Rijndael. The design principle used in AES is known as a substitution permutation network.

DES stands for Data Encryption Standard which is a symmetric-key algorithm for the encryption of electronic data. The key size used in DES is 56 bits and is small therefore DES is insecure.

Another symmetric key cryptographic algorithm is which is a symmetric key block cipher. Blowfish takes input as a variable length key, varying from 32 bits to 448 bits, which can be used for domestic purpose. Blowfish algorithm is considered to be a general-purpose algorithm and was designed by Schneier.

One-time pad is an encryption method that cannot be cracked and it requires the use of one-time pre-shared key which is of size same or longer than the original message. Since it can be computed by hand with only pencil and paper it is used in hypothetical espionage situations.

This paper presents performance analysis for different cryptography technique so that unauthorized users cannot access the data. The criteria considered for performance analysis are file size, file type, time required for encryption and decryption and block size.

2. LITERATURE SURVEY

Diaa Salama Abd Eliminaam, Hatem Mohamed Abdual Kader and Mohiy Mohamed Hadhoud "Evaluating the performance of Symmetric Encryption Algorithms": This paper provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparative analysis has been conducted based on different sizes of data blocks, different key sizes and finally encryption/decryption speed. Key understanding is in the case of changing packet size, Blowfish has better performance than any other algorithm.3DES has low performance compared to algorithm DES.RC2 has disadvantage over all other algorithms in terms of time consumption. AES has best performance than RC2, DES and 3DES.[1]

Aamer Nadeem, Dr. M Younus Javed "A performance comparison of data encryption algorithms": This paper revolves around the four of the popular secret key encryption algorithms, that is, DES, 3DES, AES and the Blowfish. Input to the processing algorithm is data files of varying size and format. The algorithms were implemented, and were tested on two different hardware platforms, to compare their performance. The four symmetric key algorithms are in the following order, as

regards their performance: Blowfish(fastest), DES, AES, 3DES (slowest). This approach failed to analyse the performance/security trade-off in greater depth.[2]

Pria Bharti, Roopali Soni "A new approach of data hiding in images using cryptography and steganography": In this paper propose a new method to embed data in colour images. 4 bits data can be embedded in a 4*4 block and some blue part of pixels need to be changed on average. Experimental results show that the method is very efficient especially when applied to those binary images whose colour pixels are distributed nearly uniformly.[3]

Piyush Marwaha, Paresh Marwaha "Visual Cryptographic steganography in images": This method can be used to increase the security on web-based applications. The user should provide the secret key and the password can be compared from image files using the key. It can be used as advancement over the existing option to input the security phrase in various web-based applications.[4]

Saleh Saraireh "A secure data communication system using cryptography and steganography": In this paper a high security model uses both cryptography and Steganography has been developed. The encryption of the data is done by filter bank cipher. Discrete wavelet transform is used to embed encrypted data in a cover image. PSNR and histogram are used to evaluate the performance. The results showed that, the PSNR of the proposed system are high, which ensure the invisibility of the hidden message through the cover image. Also, the histograms of the stage and cover images are very close to each other, which ensure the resistivity of the proposed system against the attacks.[5]

Jawahar Thakur, Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis": This paper provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. The results showed that Blowfish has a better performance than other common encryption algorithms used. AES showed poor performance when compared to other algorithms. Using CBC mode has added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data block. When compared to ECB and CBC, OFB showed better performance but require more processing time than CFB. Overall time differences between all modes are negligible.[6]

Priti Sehgal, Sarvesh Rawat, 3Saurabh Kaushik, Shafaq Ali, Rohit Yadav "Hiding encrypted text using text and image steganography: A dual steganographic technique": Due to the exponential growth of internet users, unauthorized access of information has become one of the most significant problems. There is always a constant fear of hackers and other unwanted users for they might attack and gain access to important data, passwords or any other covert information. Therefore, to provide more security to the information at the time of communication over unsecured channel, dual steganography, an advance technique for data security is needed. In this paper, we propose a highly secure dual steganography technique which takes the secret message and hides it in three phases. First it encrypts the secret message using vigenere cipher then it applies whitespace text steganography technique and lastly it hides the cover text in cover image using LSB image steganography technique. The Final Stego image is looking perfectly intact and has high PSNR value and low MSE value. Hence, an unintended observer will not be aware of existence of the secret message inside the cover image.[7]

Septimiu Fabian Mare, Mircea Vladutiu and Lucian Prodan "Secret data communication system using Steganography, AES and RSA": This paper introduces steganography as an additional security layer that covers the entire communication process by using harmless images (as seen from a third party). The data travels through finely modified and enhanced pixel colours, indistinguishable for both human and computerized analysis. Breaching such a system would imply intercepting, identifying, extracting, reverse engineering and decoding.[8]

Ajit Singh, Swati Malik "Securing Data by Using Cryptography with Steganography": In this paper two layers of security i.e. cryptography and steganography are used which makes it difficult to detect the presence of hidden message. But in some cases, if the eavesdropper has attacked the carrier of message then he will not be able to get the original message as all the relevant data here is in encrypted form. For cryptography Blowfish algorithm is used which is much better than AES and DES. In order to break blowfish algorithm, he has to spend a lot of time and effort for trying several attacks and getting the original message. Although both of these techniques are easy to implement but their combination will provide much efficient and reliable security.[9]

Ako Muhamad Abdullah "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data": Using internet and network are increasing rapidly. Various kind of algorithms are available to encrypt data. Advanced encryption standard (AES) algorithm is widely supported and adopted on hardware and software. This paper describes a number of important features of AES algorithm and presents some previous researches that have done on it to evaluate the performance of AES to encrypt data under different parameters. According to the results obtained from researches shows that AES has the ability to provide much more security compared to other algorithms like DES, 3DES etc. [10]

3. PROPOSED WORK

In this project, four main algorithms are considered like AES, DES, Blowfish and one-time pad. Different steps involved in AES are: deriving set of round keys from cipher keys, adding the initial round key to the starting address, performing exact nine rounds of state manipulation, doing tenth and final round and giving final array output as encrypted data. Steps involved inn DES are: dividing data into 64-bit blocks, performing initial permutation, dividing blocks into left and right (each of 32 bits), performing permutation and combination for 16 times, joining of left and right parts again and inversing permutation. Main steps involved in Blowfish algorithms are key expansion and encryption. In one-time pad, the key length should be same as the message length. For the key and plaintext, modulo 26 is applied. Again modulo 26 is used for values obtained after subtracting key value from the cipher text. Since the key size of DES is too small, combination of DES and Blowfish.

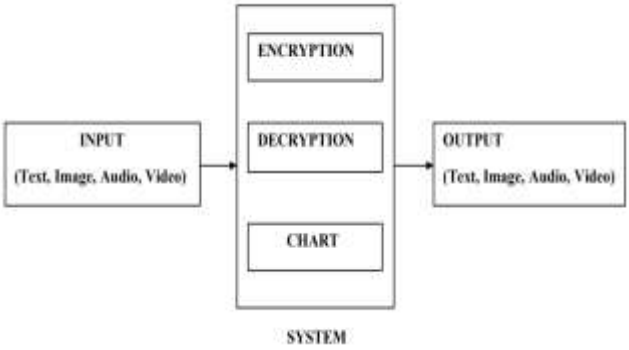

Fig -1: Architecture Diagram for performance evaluation

Input can be text files, image, audio or video. After encryption, encrypted file is given to decryption procedure which decrypts and provides original file as the output. graph is generated by taking time and file size as x-axis and y-axis respectively.

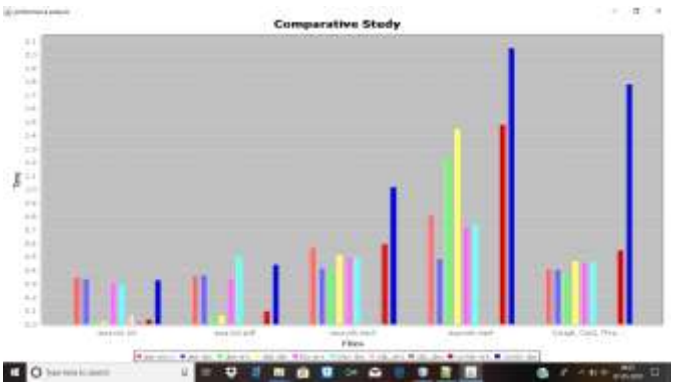

Fig-2: Bar chart showing time taken by all algorithms

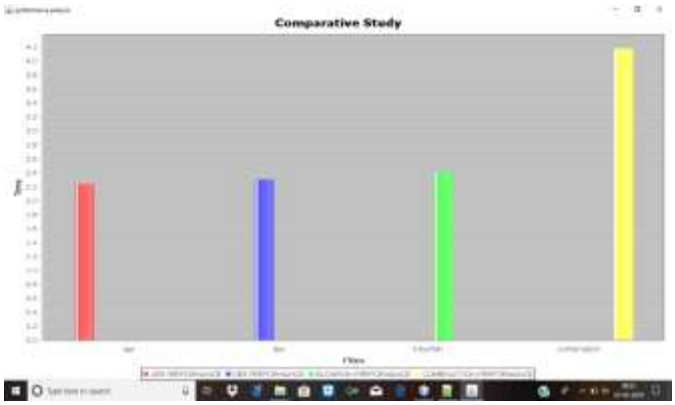

Fig-3 Bar chart of overall performance

4. CONCLUSION

Data should be sent from one user to another user in a secure way. Information security plays a major role in this. In this paper, various symmetric key cryptographic algorithms are considered. Performance evaluation of these algorithms are done by measuring several parameters like type of file, size of file and time needed to encrypt and decrypt. DES needs more time to encrypt and decrypt. DES is insecure because of smaller key size. AES is better when compared to DES because of its key size and time required for encryption and decryption. Key size of DES is too small. So, combination of DES and Blowfish is implemented. Time required for combination is more than the time required for individual algorithm, but provides robust security. In AES time required for encryption is more than decryption because in AES encryption, CBC technique is used. Key size should same as plaintext's size in one-time pad and it is really difficult to break.

REFERENCES

[1] Diaa Salama Abd Eliminaam, Hatem Mohamed Abdual Kader and Mohiy Mohamed Hadhoud- "Evaluating the performance of Symmetric Encryption Algorithms". International Journal of Network Security, Vol.10, No.3, PP.213{219, May 2010.} 213-219.

[2] Aamer Nadeem, Dr M.Younus Javed-"A Performance Comparison of Data Encryption Algorithms". Department of Computer Engineering, College of Electrical and Mechanical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan. 07803-9421-6/05/$20.00 ©2005 IEEE.84-89.

[3] Pria Bharti, Roopali Soni- "A New Approach of Data Hiding in Images using Cryptography and Steganography". International Journal of Computer Applications (0975 – 8887) Volume 58– No.18, November 2012. 1-5

[4] Piyush Marwaha1, Paresh Marwaha2- "Visual Cryptographic Steganography in images". 2010 Second International conference on Computing, Communication and Networking Technologies. 978-1-4244-6589-7/10/$26.00 ©2010 IEEE

[5] Saleh Saraireh- "A secure data communication system using cryptography and steganography". International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013. 125-137.

[6] Jawahar Thakur, Nagesh Kumar- "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation-based performance analysis". International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 2, December 2011). 6-12.

[7] Priti Sehgal, Sarvesh Rawat, Saurabh Kaushik, Shafaq Ali, Rohit Yadav- "Hiding encrypted text using text and image steganography:A dual steganographic technique". International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084 Volume-5, Issue-7, Jul.-2017. Hiding Encrypted text using text and Image Steganography: A Dual Steganographic Technique. 54-57.

[8] Septimiu Fabian Mare, Mircea Vladutiu and Lucian Prodan- "Secret data communication system using Steganography, AES and RSA". 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME). 978-1-4577-1277-7/11/$26.00 ©2011 IEEE. 20-23 Oct 2011, Timisoara, Romania. 339-344.

[9] Ajit Singh, Swati Malik- "Securing Data by Using Cryptography with Steganography". International Journal of Advanced Research in Computer Science and Software Engineering. © 2013, IJARCSSE All Rights Reserved. 404-409.

[10] Ako Muhamad Abdullah- "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data". Cryptography and Network Security. Publication Date: June 16, 2017.