Evaluation of various parameters during Encryption and Decryption of Image, Audio & Video using various Symmetric Cryptographic Algorithms

Nilesh Advani[1], Prof. (Dr.) Atul Gonsai[2]
[1]*(Faculty of Computer Applications, Marwadi University, India)*
[2]*(MCA Department, Saurashtra University, India)*

Abstract: We all very well know that today use of Internet has been increased like anything. [1][4][6]The data on internet is growing like anything day by day. As per the latest survey on data, everyday, every minute around 550+ websites are being uploaded. Along with this every day is important as far as sending secure data is concerned. Our data is very much important and it is very necessary that the data must be sent in a secured way. There are various types of algorithms which are called either Symmetric or Asymmetric work on block of data where as some work as a stream cipher. In our previous paper, we compared symmetric algorithms but only by keeping their encryption and decryption time in mind here we have tried to cover other parameters along with only encryption and decryption time. We tried to compare various types of files i.e. Image, Audio and Video. Total 48 comparisons were made again with AES, DES, 3DES, Blowfish and Twofish. In this, we have used various types of padding techniques. Various parameters which are taken into consideration in this paper are Encryption and Decryption time, Usage of CPU while doing encryption and decryption, Memory usage while doing encryption and decryption, Memory swap size for encryption and decryption. By looking all above parameters the comparison is made.

Keywords: Encryption, Decryption, Cryptography, Symmetric, Asymmetric, Image Encryption, Audio Encryption, Video Decryption, AES, DES, 3DES, Blowfish, Multimedia

1. INTRODUCTION

The use of internet has been increased since last couple of years. Every day the data on internet is increasing like anything. As per the recent survey, it has been found that every minute of each day around 550+ websites are being uploaded. Just imagine how the data is growing. With the increasing use of data, its security is also getting into concern as day by day, new threats are getting introduced by many hackers who are not working in an ethical way. [15][17][18] with the increasing use of Internet and websites, every day lots of digital data is being uploaded on the internet and used by many people. Here the security of data has also got main concern as the data shall be passed through internet in a secured manner.

We know that cryptography is an important integral part of the internet data. It plays an important role when the data is being sent or when the data is being retrieved. Cryptography plays very important role when we are sending or receiving the data through wired medium or wireless medium. Over the [1]years plenty of Asymmetric and Symmetric Algorithms are proposed which work as a block or stream cipher.

Some standard Asymmetric algorithms like DH, DSS, ECDH, DSA, RSA, etc. Apart from this some standard Symmetric algorithms like DES, 3DES, AES, Blowfish an its previous versions have been proposed. As per our previous research paper, we found that from Symmetric algorithms AES as well as Blowfish works faster for many types of files like Image, Audio, Video, etc.

1.1. Symmetric Algorithms

The AES algorithm, founded on the design of Belgian cryptographers Joan Daemen and Vincent Rijmen became the standard for encryption starting 2002. The algorithm has a data block length of 128 bits with variable key sizes of 128-bit (called AES-128), 192-bit (AES-192), and 256-bit (AES-256). The number of rounds to complete the process of encryption depends on the key size: 10 rounds for AES-128; 12 rounds for AES-192; and 14 rounds for AES-256. AES has different advantages such as security, flexibility, and ease of implementation.

Recently Enhanced Blowfish algorithm was developed for security purpose. It was developed for x64FileMessage content.

1.2. Symmetric Algorithms

Nowadays [15][16]ECDSA (Elliptical Curve Digital Signature Algorithm) gaining more popularity than the RSA algorithm because of the better performance of ECDSA over RSA. The main advantage of ECC over RSA is ECC provides the same level of security with less key size and overhead than RSA.

1.3. Types of files used

Now, let us talk about our research work which was done. We took 3 types of files i.e. [1]Image, Audio and Video. Each type of file had 4 different size files i.e. small file, medium file, large file and extra large file. All these names are give just on the basis of their size.

Table I: Files used for Comparison with different sizes

Sr. No.	File Name	Type	File Size (MB)
1	small.jpg	Image	0.30
2	medium.jpeg	Image	1.38
3	large.jpg	Image	3.95
4	xlarge.jpg	Image	7.42
5	small.mp3	Audio	3.34
6	medium.mp3	Audio	8.86
7	large.mp3	Audio	12.10
8	xlarge.mp3	Audio	34.60
9	small.mp4	Video	7.81
10	medium.mp4	Video	14.10
11	large.mp4	Video	31.20
12	xlarge.mp4	Video	45.10

In our previous research also we used exactly the same files and continued further research by additional parameters checking with same files only.

2. EVALUATION OF IMAGE CRYPTOGRAPHY

Various types of images are available today. Most common types of images are JPG, JPEG, BMP, TIFF, PNG, etc. [1] From all types of images generally JPG type of images are used today which support more resolution in comparison to others. Hence we have taken JPG images for comparison purpose.

[2]There are 4 types of images as stated in the table. We have compared there 4 types of images with 4 types of algorithms i.e. AES, Blowfish, DES and 3DES.

Following is the comparison of 4 types of images with all 4 types of algorithms stated above.

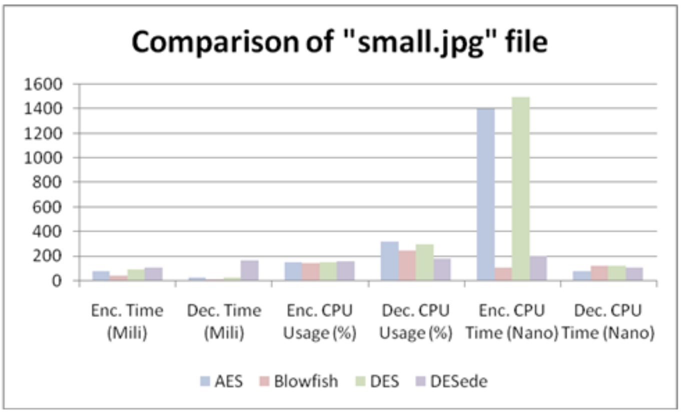

Figure 1 : Comparison of algorithms with “small.jpg” file

In above example, we can figure out that AES as well as Blowfish are taking less time in comparison. In most of the cases, Blowfish is faster than in comparison to AES. In the case of decryption time, Blowfish is taking little more time.

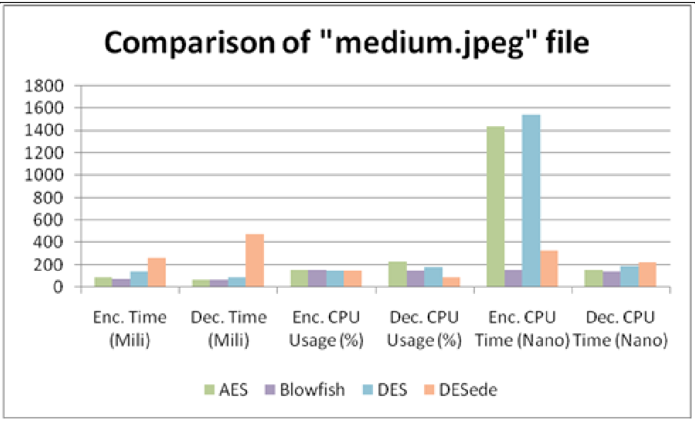

Figure 2 : Comparison of algorithms with “medium.jpeg” file

Here we have compared a little bigger size file which is in the format of JPEG. Here encryption time is much more by AES in comparison.to Blowfish. [2]

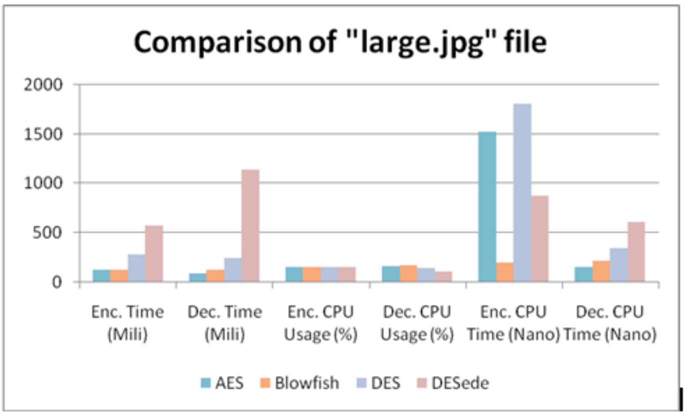

Figure 3 : Comparison of algorithms with “large.jpg” file

While comparison “large.jpg” file, we can figure out that CPU time is taken more for [10][11][12]AES in comparison to blowfish. Where as the same file is taking less CPU time for decrytpion in comparison.

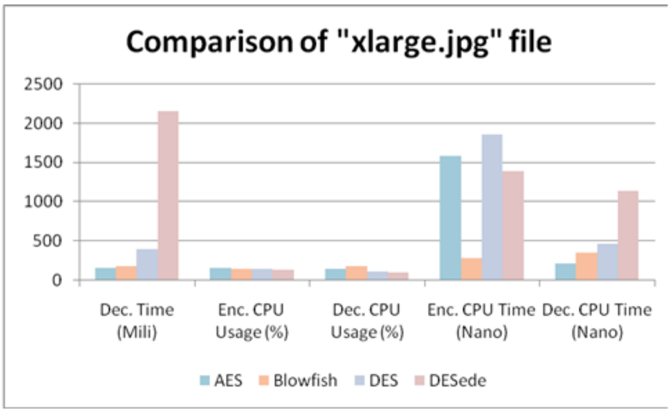

Figure 4 : Comparison of algorithms with “xlarge.jpg” file

Here, we can understand that again Encryption CPU time is more for Blowfish is taking less time in CPU Encryption where as little more for Decryption.

3. EVALUATION OF AUDIO CRYPTOGRAPHY

Just like various types of image files[9][13], there are various types of audio files. Some common types of audio files are WAV, AU, MPEG, MP3, etc. [2][3] Here we have used one of the most common type of audio file for comparison different types of algorithms i.e. MP3 files.

Just similar to image files, we have taken 4 audio files with different sizes of each. Following are 4 types of graphs which are prepared by taking each file to compare with 4 types of algorithms specified earlier.

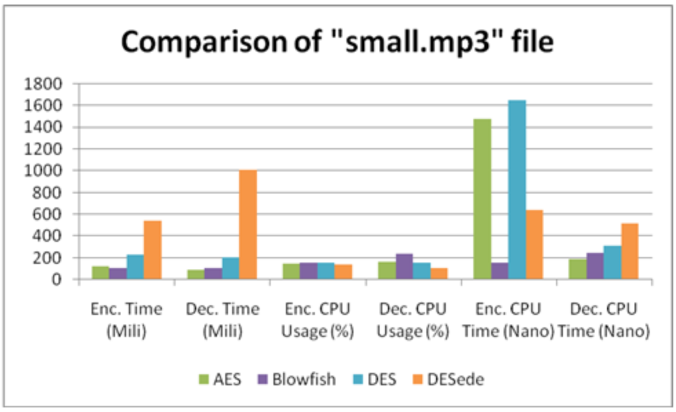

Figure 5 : Comparison of algorithms with “small.mp3” file

You can see above graph and can identify that here AES and Blowfish are taking less time in comparison to others. Here also we can identify that while the time taken by CPU for encryption is more by AES in comparison to Blowfish.

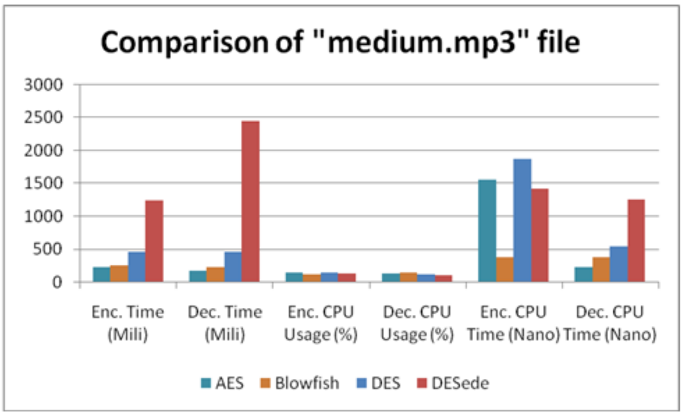

Figure 6 : Comparison of algorithms with “medium.mp3” file

Here as far as Encrytpion and Decryption time is concerned, AES is taking little less time in comparison to Blowfish but CPU Encryption time taken by AES is higher in comparison.

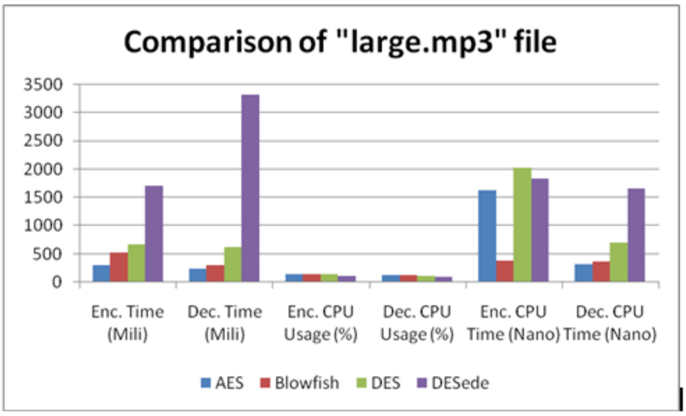

Figure 7 : Comparison of algorithms with “large.mp3” file

Here the results are almost similar to comparing with "medium.mp3" file . In fact, due to large size, [3]AES is taking little more less time for encryption in comparison to time taken by "medium.mp3" file.

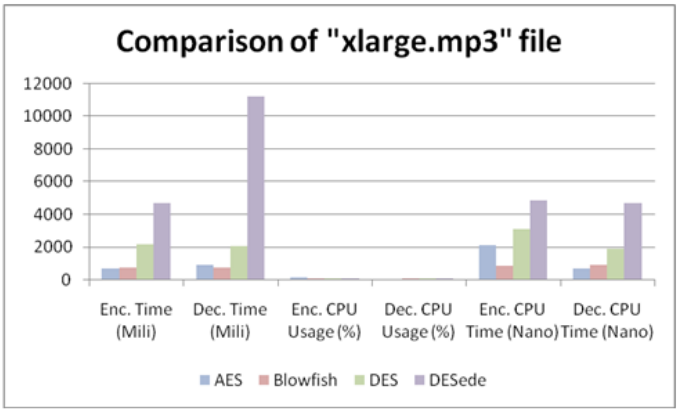

Figure 8 : Comparison of algorithms with "xlarge.mp3" file

Here also the results are almost similar to the comparison of previous files. We can see that just at the time of decryption, CPU time is taken little more by Blowfish in comparison to AES algorithm.

4. EVALUATION OF VIDEO CRYPTOGRAPHY

There are different types of video files. Some of the most common types of video files are MP4, 3GP, WMV, FLV, AVI, etc. Here also we have taken video files with MP4 type with 4 different type of sizes.

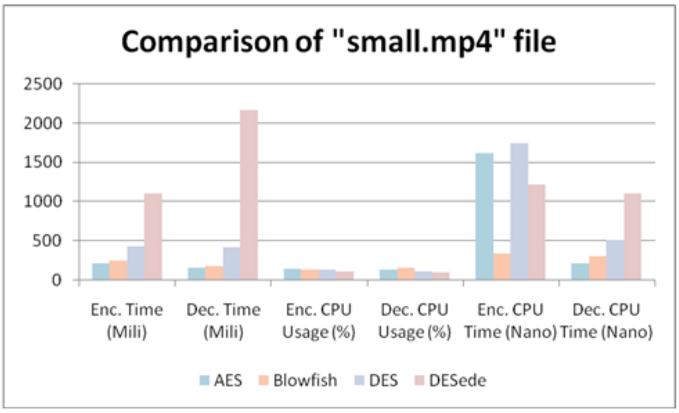

Figure 9 : Comparison of algorithms with "small.mp4" file

In above comparison, you can see that here [3]AES and Blowfish are taking less time. Except encryption time, Blowfish is proved faster than AES. If you compare average encryption and decryption time, AES is taking less time where as for CPU encryption is taking more time with AES and taking less time with Blowfish.

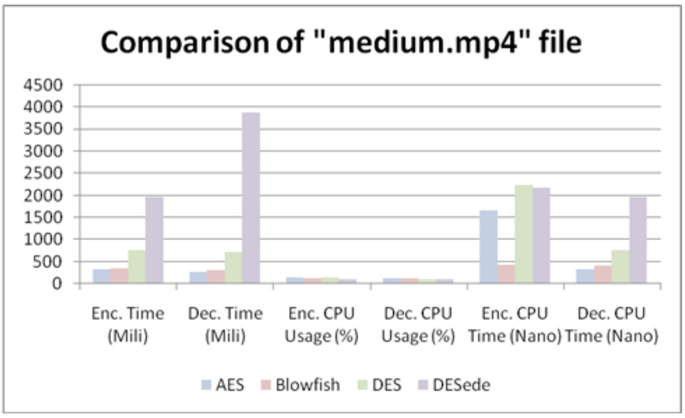

Figure 10 : Comparison of algorithms with "medium.mp4" file

In this cryptography, as far as encryption and decryption time is concerned, [7][8]AES and Blowfish are taking almost same amount of time but as far as Encryption time is concerned AES takes more time in comparison to Blowfish.

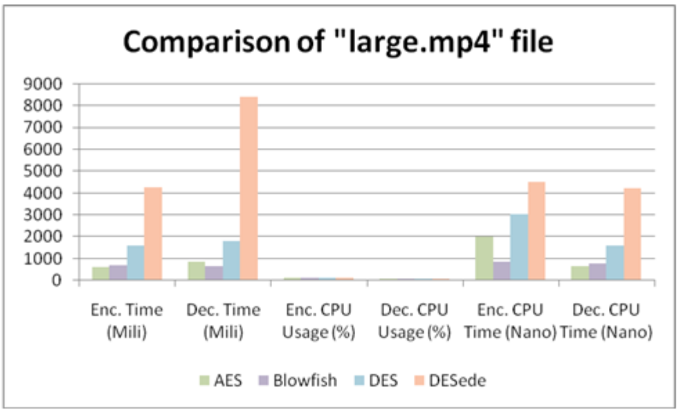

Figure 11 : Comparison of algorithms with “large.mp4” file

While comparing “large.mp4” file, we can easily figure out that the results are almost similar to encryption and decryption of “medium.mp4” file.

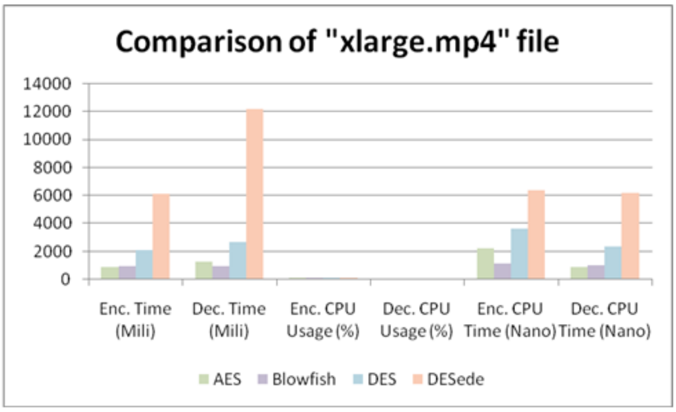

Figure 12 : Comparison of algorithms with “xlargel.mp4” file

Here also the results are same to previous comparison which was done with “medium.mp4” and “large.mp4” file with 4 types of algorithms.

5. ACKNOWLEDGEMENT

In our previous research we used the same files with similar type of symmetric algorithms i.e. AES, Blowfish, DES and 3DES. We used total 12 types of files from Image, Audio and Video. Hence we did total 48 types of different comparisons for different types of files.

So far we came to conclusion that as far as encryption and decryption is concerned, [4][5]“AES” and “Blowfish” are better algorithms. Our next paper we will try to compare “Asymmetric Algorithms” with same types of files or use stream cipher for comparison. [6]

One thing is very much clear that in most of the aspects Blowfish is performing better in comparison to AES algorithm.

6. CONCLUSION

As per the conclusion of our research it says that as far as Symmetric algorithms are concerned, Blowfish seems to be better for all types of files. Yes, in one or two cases AES performed well in comparison to Blowfish. However, we have tested only [3][4][5][7]AES, DES, 3DES and blowfish.

Hence here we conclude that as far as Symmetric algorithms are concerned first preference will be given to Blowfish and after that AES will be preferred. Our future research will be based on Asymmetric algorithm comparison with same types of files so that we can compare which algorithm will be better for doing run time cryptography for image, audio and video.

REFERENCES

[1]. C. Pak and L. Huang, “A new color image encryption using combination of the 1D chaotic map,” *Signal Processing, 2017.*

[2]. L. Mallu and R. Ezhilarasie, “Live migration of virtual machines in cloud environment: A survey,” *Indian J. Sci. Technol., vol. 8,no. May, pp. 326–332, 2015.*

[3]. N. Advani and C. Rathod, “Comparative Study of various Cryptographic Algorithms used for Text, Image and Video,” *Springer, ICETEAS - 2018,* no. ICETEAS-2018 *Special Issue,* pp. 3–7, 2018.

[4]. S. M. Seth and R. Mishra, “Comparative Analysis Of Encryption Algorithms For Data Communication,” *vol. 4333, pp. 292–294, 2011.*

[5]. H. Rahman, N. Islam, M. Hasan, R. Jany, and M. M. Rahmant, “Multimedia Content Security with Random Key Generation Approach in Cloud Computing,” 1902.

[6]. J. Raigoza, “Evaluating Performance of Symmetric Encryption Algorithms,” IEEE, Int. Conf. Comput. Sci. Comput. Intell., pp. *1378–1381, 2016.*

[7]. B. Bhat, A. W. Ali, and A. Gupta, “DES and AES performance evaluation,” *IEEE - Int. Conf. Comput. Commun. Autom. ICCCA 2015, pp. 887–890, 2015.*

[8]. M. Mathur, “Comparison between DES , 3DES , RC2 , RC6 , BLOWFISH and AES,” *Proc. Natl. Conf. New Horizons IT, pp. 143–148, 2013.*

[9]. R. Sivakumar, B. Balakumar, and V. A. Pandeeswaran, “A Study of Encryption Algorithms (DES , 3DES and AES) for Information Security,” *Int. Res. J. Eng. Technol., vol. 5, no. 4, pp. 4133–4137, 2018.*

[10]. M. Bala, P. Kumari, and A. Sharma, “Comparative Analysis of Symmetric Key Algorithms : DES , AES and Blowfish for Audio Encryption and Decryption,” *IEEE, pp. 1048–1054, 2017.*

[11]. A. Devi, A. Sharma, and A. Rangra, “A Review on DES , AES and Blowfish for Image Encryption & Decryption,” *IJCSIT (International J. Comput. Sci. Inf. Technol., vol. 6, no. 3, pp. 3034–3036, 2015.*

[12]. F. Yeganegi, V. Hassanzade, and S. M. Ahadi, “Comparative Performance Evaluation of SVD-based Image Compression,” Electr. Eng. (ICEE), Iran. Conf., pp. 464–469, 2018.

[13]. O. Watanabe, A. Uchida, T. Fukuhara, and H. Kiya, “An Encryption-then-Compression system for JPEG 2000 standard,” *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc., vol. 2015–Augus, pp. 1226–1230, 2015.*

[14]. H. Wang, M. Hempel, D. Peng, W. Wang, H. Sharif, and H. H. Chen, “Index-based selective audio encryption for wireless multimedia sensor networks,” *IEEE Trans. Multimed., vol. 12, no. 3, pp. 215–223, 2010.*

[15]. R. Rigoni, P. G. Freitas, and M. C. Q. Farias, “Detecting tampering in audio-visual content using QIM watermarking,” *Inf. Sci. (Ny)., vol. 328, pp. 127–143, 2016.*

[16]. N. Augustine, S. N. George, and D. P. Pattathil, “An audio encryption technique through compressive sensing and Arnold transform.,” *Ijtmcc, vol. 3, no. 1, pp. 74–92, 2015.*

[17]. M. Paliwal, “Selective Video Encryption using Bit XOR Technique,” *vol. 2, no. 1, pp. 177–183, 2015.*

[18]. A. Alfalou, C. Brosseau, and N. Abdallah, “Simultaneous compression and encryption of color video images,” *Opt. Commun., vol. 338, pp. 371–379, 2015.*