OPEN ACCESS

Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: http://scholarsmepub.com/sjet/

Original Research Article

Performance Evaluation of Symmetric Data Encryption Algorithms: AES and Blowfish

Bello Alhaji Buhari[1*], Afolayan Ayodele Obiniyi[2], Kissinger Sunday[1], Sirajo Shehu[1]

[1]Department of Mathematics, Computer Science Unit, Usmanu Danfodiyo University, Sokoto – Nigeria
[2]Department of Computer Science Unit, Ahmadu Bello University, Zaria – Nigeria

DOI: 10.36348/SJEAT.2019.v04i10.002 | **Received:** 29.09.2019 | **Accepted:** 07.10.2019 | **Published:** 21.10.2019

***Corresponding author:** Bello Alhaji Buhari

Abstract

People are transferring large amount of data that are critical and consume large amount of time through the Internet such as email, banking transaction and online purchase. But due to high exposure they are susceptible to being heavily attacked or become attractive targets for attackers. This can be solved by using a modern phenomenon called symmetric encryption. Symmetric encryption is used to ensure that information is hidden from anyone for whom it is not intended. This research conducted a performance evaluation of symmetric data encryption algorithms namely Advanced Encryption Standard (AES) and Blowfish. The evaluation is done for four different data types: image data type, audio data types, video data types and textual file data types. The performance evaluation metrics are encryption time and throughput. The prototype is developed using JAVA, compiled using the Netbeans IDE7.1.2 with default settings in jdk 7.1 development kit. Results obtained from this evaluation indicated that blowfish is more efficient than AES. But for Blowfish the encryption time sometime decreases with the increase in data size. This can be attributed to the fact that Blowfish uses 126, 192 or 256 key sizes.

Keywords: AES, Blowfish, Data encryption, Performance evaluation, Symmetric Algorithm.

INTRODUCTION

The Internet plays an important role in day-to-day life. The people can transfer large amount of data that are critical and consume large amount of time through the internet such as Email, banking transaction and online purchase. But due high exposure they are susceptible to being heavily attacked or become attractive targets for attackers. This means that they require special care to make them secure and resilient against security treats. This can be solved by using a modern phenomenon called symmetric cryptography.

Cryptography is the art and science of generating a secret message i.e. code or ciphers of the original message or data for a secure communication between sender and the receiver. The main goals of cryptography are: Authentication, Privacy, Integrity, Non-repudiation [1] and Access Control.

Data encryption is the performance of series of mathematical operations on data to generate an alternate form of that data; the sequence of these operations is called an algorithm. To help distinguish between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as cipher text. Data encryption is used to ensure that information is hidden from anyone for whom it is not intended [2], even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption. The process of encrypting and decrypting can be illustrated in fig-1.

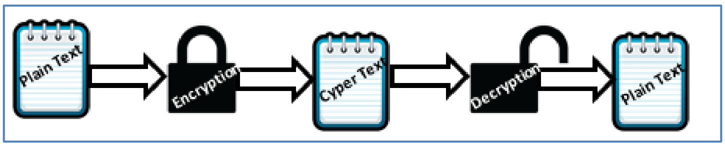


Fig-1: Process of Encryption and decryption

The aim of this research is to conduct performance evaluation of symmetric data encryption algorithms namely AES and Blowfish. The evaluation is done for four different data types: image data type, audio data types, video data types and textual file data types. The performance evaluation metrics are encryption time and throughput. A simulation modeling is used for capturing encryption time for the various data types considered thereby computing their average time and throughput. The prototype is developed using JAVA, compiled using the Netbeans IDE7.1.2 with default settings in jdk 7.1 development kit.

Advanced Encryption Algorithm (AES)

The National Institute of Standards and Technology (NIST) in [3] chose the Rijndael algorithm developed by Joan Daemen and Vincent Rijmen, to replace the data encryption standard (DES) algorithm in [4] as the new advanced encryption standard (AES) algorithm in [5].

AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field.

AES-128 encryption algorithm is as follows [6]:

Input: The 128-bit plaintext blocks P and key K.

Output: The 128-bit ciphertext block C.

```
X ← AddRoundKey(P,K)
for i ← 1 to 10 do
X ← SubBytes(X)
X ← ShiftRows(X)
If i ≠ 10
X ← MixColumns(X)

end
K ← KeySchedule(K)
X ← AddRoundKey(X,K)

end
C ← X
return C
```

The Encryption process consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process. For key length of 128 bits, the number of iteration required are10. (Nr = 10). As shown in fig-2 each of the first Nr-1 rounds consist of 4 operations: SubBytes (), ShiftRows (), MixColumns () & AddRoundKey ().

Blowfish

Blowfish is a symmetric cipher algorithm that can be effectively used for encryption and safeguarding of data. It used the key length, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in [8] as a fast, free alternative to existing encryption algorithms. Though it suffers from weak keys problem, no attack is known to be successful against it [9, 10].

Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totalling 4168 bytes. The data encryption occurs via a 16-round Feistel network. It is only suitable for application where the key does not change often, like communications link or an automatic file encryption.

The basic algorithm for Blowfish is as follows [11]:

```
Divide X into two 32-bit halves XL and XR
For i=1 to 16:
        XL = XL Pi
        XR = F (XL) XR
        Swap XL and XR
End for
Swap XL and XR
XR = XR P17
XL = XL P18
Recombine XL and XR
Output X (64-bit data block: cipher text)
```

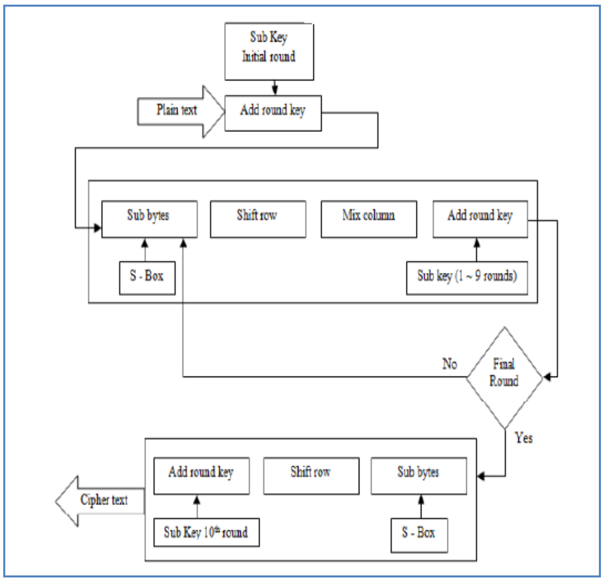


Fig-2: AES Encryption process [7]

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round. This can be shown in fig-3.

In this case images for instance, the original data bit stream is divided into the blocks length of Blowfish algorithm. Data header is excluded to encrypt and the start of the bitmap pixel or array begins right after the header of the file. The byte elements of the array are stored in row order from left to right with each row representing one scan line of the data and the rows of the data are encrypted from top to bottom.

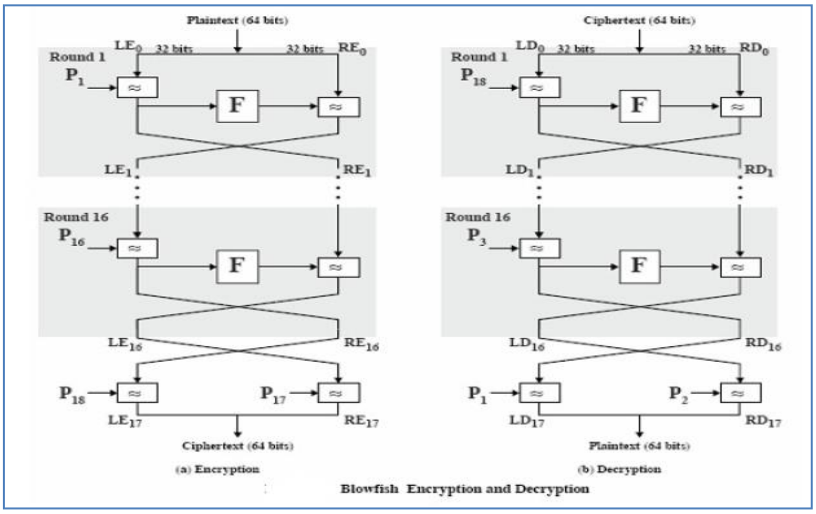


Fig-3: Block diagram of blowfish [12]

RELATED WORKS

With the advancement of computers and interconnectivity, the world governmental institutions and industries are subjective to cyber-attacks, intrusion and industrial espionage. To prevent these threats ATM cards, Computer passwords and transferring data from one place to another are implemented using cryptography. This section reviews previous works related to this research.

Kumar *et al.* in [13] perform a comparative analysis of encryption algorithms for better utilization. The goal of their paper is to compare the different encryption algorithm and to find space complexity of the encrypted and decrypted data by using complexities of encryption algorithm. They perform comparison between five most widely used algorithms. Based on their experiment it has shown that Triple Data Encryption Algorithm (TDES) in general perform better than other algorithms. They did not consider different data types in their experiment.

Also, Bhanot and Hans in [14] conducted a review and comparative analysis of various encryption algorithms. They analysed ten data encryption algorithms Data Encryption Standard (DES), Triple DES, Rivest-Shamir-Adleman (RSA), AES, Elliptical Curve Cryptography (ECC), BLOWFISH, TWOFISH, THREEFISH, Rivest Cipher 5 (RC5) and International Data Encryption Algorithm (IDEA). The parameters used for the comparison are key length, round, block size and attack found. It is observed from the result that the strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key. It was found from their analysis that ECC and Blowfish are leading with the security level that they provide and faster encryption speed.

Lastly, Shaza *et al*. in [15] evaluate the performance of the two encryption algorithms: AES and DES. The performance measure of encryption algorithms are conducted in terms of processing time, CPU usage and encryption throughput on Windows and Mac platform for a different text size. The simulation results conclude that, AES is faster than DES in the execution time for the two platforms. AES has high throughput than DES. DES consumes less CPU usage than AES for two platforms. But their experimental is based on textual data files.

Based on these reviews, this research conducts a performance evaluation of the two commonly used symmetric data encryption algorithms: AES and Blowfish considering different data types such as image data type, audio data types, video data types and textual file data types. Encryption time and throughput are the two performance metrics used for the evaluation.

METHODOLOGY

The performance analysis is done using simulation, analytical, testbeds and operational modelling depending on the system to be model or the designer need. In this research, operational modelling is used. This is because in this research a working system is going to be designed to extract the data to be analyzed for interpretation and finding. Thus, operational analysis deals with the measurement and evaluation of an actual system in operation.

Similarly, Performance metrics are encryption time, decryption time, throughput, CPU process time, and memory Utilization. But this research considers encryption time and throughput as the performance metrics for the evaluation of these data encryption algorithms as shown in fig-4. Encryption time is the total time taken to produce a cipher text from plain text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm which gives the rate of encryption. The throughput of the encryption scheme is calculated as the total encrypted plaintext in kilo bytes divided by the encryption time in seconds.

A prototype system is developed using JAVA programming language to act as experimental environment.

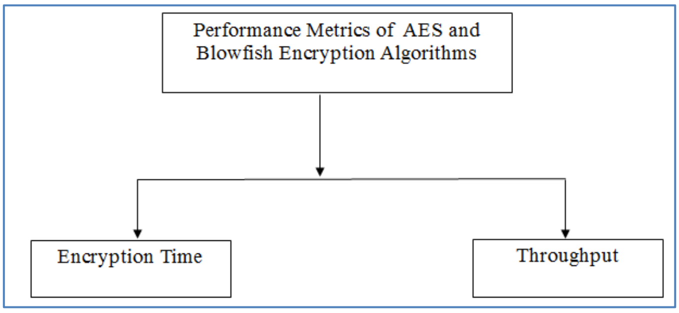

Performance Metrics of AES and Blowfish Encryption Algorithms
Encryption Time
Throughput

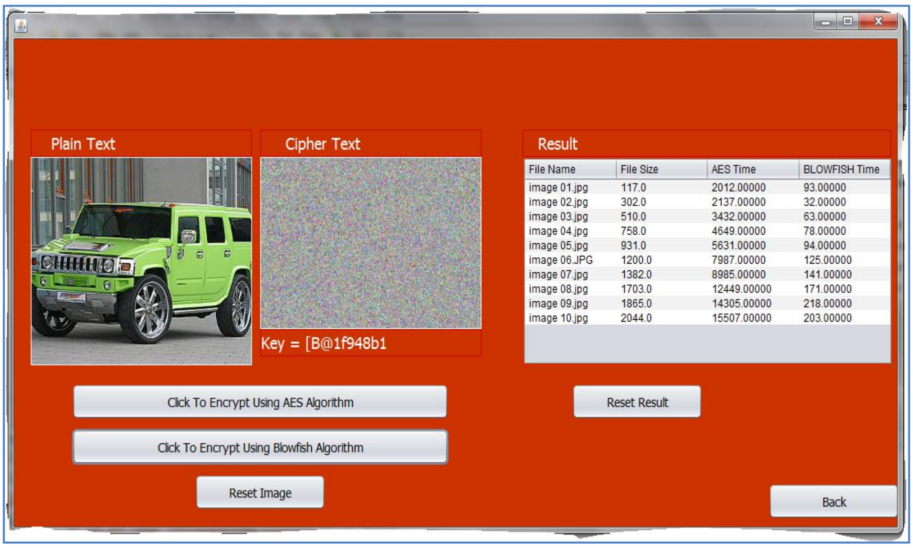
Fig-4: Performance metrics to be considered

EXPERIMENTAL SETUP

In this work, AES and Blowfish symmetric encryption algorithms have been implemented in Java Programming Language and the experiment has been carried out using a Laptop having Intel(R) Core(TM) i3 M370 @ 2.40GHz processor with 4 GB RAM on Windows 7 home premium, 64-bit operating system. The experiment program was compiled using the Netbeans IDE7.1.2 with default settings in jdk 7.1 development kit for JAVA. The experiment was performed couple of times to assure that the results are consistent and are valid to compare the different algorithms.

Image data, audio data, video data and text file data were the specimens for our experiments and the prototype developed consists of two interfaces (start and main interface) which were developed using the Java Interface Development Environment.

The main interface allow the user interacts with the application through a user friendly designed graphical user interface, it functions as part of the physical design of the application software; using the computer keyboard to input the original data (plaintext), the monitor to display output (ciphertext) to the user together with encryption key, the encryption time for both algorithms and the computer processing unit for processing tasks. This can be shown in fig-5.


Plain Text
Cipher Text
Click To Encrypt Using AES Algorithm
Click To Encrypt Using Blowfish Algorithm
Reset Image
Reset Result
Back

Key = [B@1f948b1

Result

File Name	File Size	AES Time	BLOWFISH Time
image 01.jpg	117.0	2012.00000	93.00000
image 02.jpg	302.0	2137.00000	32.00000
image 03.jpg	510.0	3432.00000	63.00000
image 04.jpg	758.0	4649.00000	78.00000
image 05.jpg	931.0	5631.00000	94.00000
image 06.JPG	1200.0	7987.00000	125.00000
image 07.jpg	1382.0	8985.00000	141.00000
image 08.jpg	1703.0	12449.00000	171.00000
image 09.jpg	1865.0	14305.00000	218.00000
image 10.jpg	2044.0	15507.00000	203.00000

Fig-5: The main interface of the prototype

The interface contains two boxes named plaintext and cipher text. The plain text uploads the original data to the box and cipher text hold the encrypted data when any of the algorithm buttons are clicked. The button called click to encrypt using AES algorithm is use to encrypt the original data using AES algorithm and the other one called click to encrypt using Blowfish algorithm is also use to convert the plaintext into cipher text using Blowfish. Below cipher text there is a column that displays the encrypted data key and the reset data button use to refresh the data boxes. Other side has a table called Result table that use to display the result of the experiment.

The file name, file size and encryption time for both the algorithms under study displays automatically by pressing any algorithm mentioned above and throughput of encryption time will be calculated later.

Experimental Settings

The experiment uses the provided classes in java environment to experiment the performance of AES and Blowfish. The implementation uses managed wrappers for AES and Blowfish available in java.cypto and java.perfomance[CryptoSpec] that wraps unmanaged implementations available in JCE (Java Cryptography Extension) & JCA (Java Cryptography Architecture).The Cipher class provides the functionality of a cryptographic cipher used for encryption. It forms the core of the JCE framework. The algorithms settings are shown in table-1.

Table-1: Algorithms Settings

Algorithm	Key size (bits)	Block size (bits)
Blowfish	32-448	64
AES	126, 192, 256	128

The evaluation is meant to evaluate the results by using block ciphers. Hence, the load data (plaintext) is divided into smaller block size as per algorithm settings given in Table-1.

Experimental Procedure

The main purpose here is to calculate the encryption speed of each of the algorithm under study for different data sizes. Their implementation is tried to optimize the maximum performance for the algorithm. The throughput for encryption is calculated for each algorithm. Encryption time is used to calculate the throughput of an encryption scheme .The throughput of the encryption scheme is calculated by dividing the total plaintext in kilobytes by total encryption time in Second for each algorithm. If the throughput value is increased, the power consumption of this encryption technique is decreased.

In this research the different data types: image, audio, video and files were experimented with different data sizes. The performance metrics are analyzed as encryption time and throughput.

Throughput = Plaintext (KB) / Encryption time (Sec.)

RESULTS AND FINDINGS

Encryption algorithms have been experimented using different data sizes. This experiment has been conducted to compare AES and Blowfish which are symmetric key cryptography algorithms. Different sizes of data blocks and standards key size are used to evaluate the algorithm's run time speed. All the implementations were exact to make sure that the results will be relatively fair and accurate. The data block sizes that are used in this research are 128kb for both AES and Blowfish.

Experimental Results for Image Data Type

By considering the result in table-2, the average execution time for image data types of AES is 7709.40000 and Blowfish is 121.800000. Similarly, the throughput is 0.13845 and 8.76547 for AES and Blowfish respectively. This result as shown in fig-6 shows that AES has higher encryption average time and Blowfish has higher throughput, Hence Blowfish is more efficient in image data encryption than AES. Also, in AES increase in size of image increase encryption time. But in the in Blowfish the encryption time some time decreases with the increase in image size. This can be attributed to the fact that Blowfish uses 126, 192 or 256 key sizes.

Table-2: Experimental results for Image data types

File Name	Image Size (kb)	AES (ms)	Blowfish (ms)
Image01.jpg	117.0	2012.0000	93.0000
Image02.jpg	302.0	2137.0000	32.0000
Image03.jpg	510.0	3432.0000	63.0000
Image04.jpg	758.0	4649.0000	78.0000
Image05.jpg	931.0	5631.0000	94.0000
Image06.jpg	1200.0	7987.0000	125.0000
Image07.jpg	1382.0	8985.0000	141.0000
Image08.jpg	1565.0	12449.0000	171.0000
Image09.jpg	1865.0	14305.0000	218.0000
Image10.jpg	2044.0	15507.0000	203.0000
	Average Time	7709.4000	121.80000
	Throughput	0.13845	8.76547

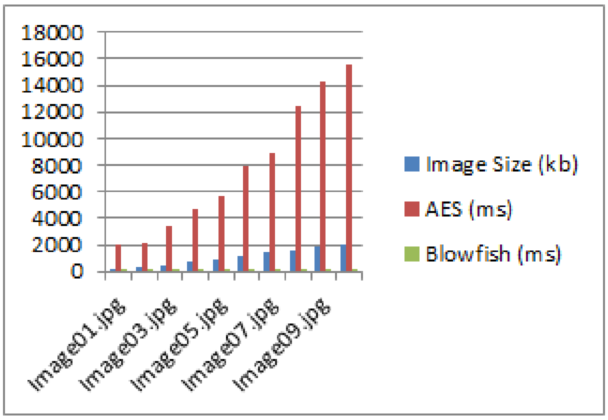


Fig-6: Experimental results for Image data types

Experimental Results for Audio Data Type

Considering the result in table-3, the average execution time for audio data types of AES is 17730.0000 and Blowfish is 120.0000. Similarly, the throughput is 0.06153 and 9.09167 for AES and Blowfish respectively. This result as shown in fig-7 shows that AES has higher encryption average time and Blowfish has higher throughput, Hence, Blowfish is more efficient in video data encryption than AES. Also, the efficiency of Blowfish is increasing with increase in complexity of data types because audios are more complex than images.

Table-3: Experimental results for Audio data types

File Name	Audio Size (kb)	AES (ms)	Blowfish (ms)
Audio 01.aac	100.0	1700.0000	10.0000
Audio 02.m4a	346.0	5150.0000	40.0000
Audio 03.m4a	571.0	9460.0000	60.0000
Audio 04.mp3	768.0	12270.0000	80.0000
Audio 05.aac	901.0	13850.0000	90.0000
Audio 06.amr	1099.0	18350.0000	170.0000
Audio 07.mp3	1300.0	21170.0000	140.0000
Audio 08.mp3	1571.0	25590.0000	170.0000
Audio 09.mp3	1875.0	30910.0000	200.0000
Audio 10.mp3	2379.0	38850.0000	240.0000
	Average Time	17730.0000	120.0000
	Throughput	0.06153	9.09167

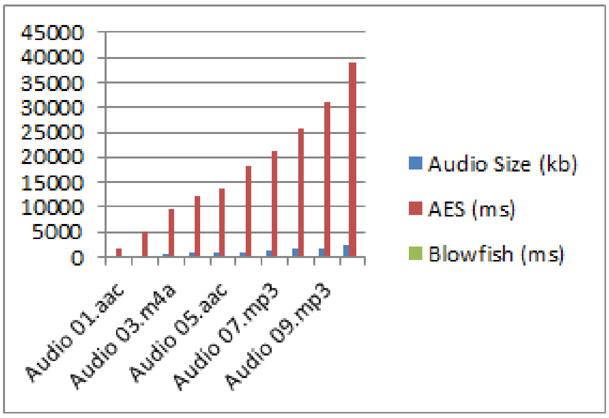


Fig-7: Experimental results for Audio data types

Experimental Results for Video Data Type

Also, from the result in table-4 and fig-8, it shows that the average execution time for video data types of AES is 7506.0000 and Blowfish is 111.0000. Similarly, the throughput of AES and Blowfish is 0.14440 and 9.76486 respectively. Therefore, Blowfish is more efficient than AES maintaining its increase in efficiency as data type becomes heavier. Also, efficiency of AES increases than in audio.

Table-4: Experimental results for Video data types

File Name	Video Size (kb)	AES (ms)	Blowfish (ms)
Video 01.mp4	177.0	1790.0000	40.0000
Video 02.mp4	343.0	2260.0000	40.0000
Video 03.mp4	571.0	3450.0000	60.0000
Video 04.mp4	766.0	5440.0000	90.0000
Video 05.mp4	980.0	6800.0000	90.0000
Video 06.mp4	1036.0	7100.0000	100.0000
Video 07.3gp	1234.0	8300.0000	120.0000
Video 08.mp4	1441.0	9950.0000	140.0000
Video 09.mp4	1761.0	12070.0000	180.0000
Video 10.3gp	2530.0	17900.0000	250.0000
	Average Time	7506.0000	111.0000
	Throughput	0.14440	9.76486

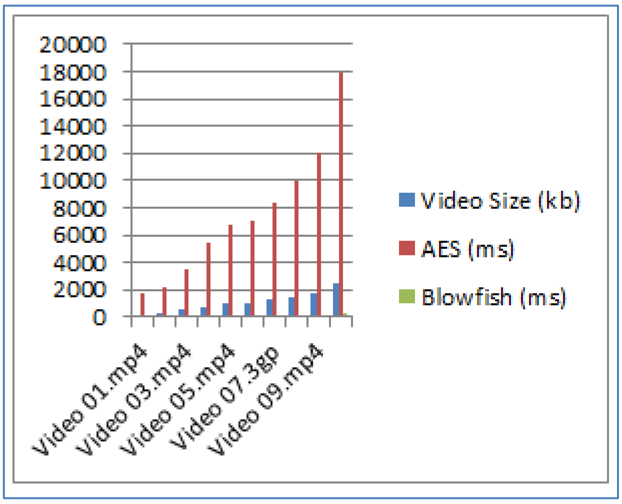


Fig-8: Experimental results for Video data types

Experimental Results for File Data Type

Lastly, the result of table-5 shows that the average execution time for file data type of AES is 7368.1000 and Blowfish is 111.0000. Similarly, the throughput of AES and Blowfish is 0.14836 and 9.84775 respectively. This can be shown in fig-9. Therefore, Blowfish is more efficient than AES. Both the efficiency of AES and Blowfish increases in file data types.

Table-5: Experimental results for file data types

File Name	Text file Size (kb)	AES (ms)	Blowfish (ms)
File 01.pdf	117.0	1330.0000	40.0000
File 02.pdf	347.0	2220.0000	50.0000
File 03.pdf	407.0	3250.0000	50.0000
File 04.docx	573.0	3970.0000	70.0000
File 05.pdf	808.0	4850.0000	80.0000
File 06.pdf	1115.0	7780.0000	110.0000
File 07.pdf	1354.0	9150.0000	140.0000
File 08.pdf	1516.0	10020.0000	150.0000
File 09.pdf	1699.0	11520.0000	140.0000
File 10.pdf	2995.0	19591.0000	280.0000
	Average Time	**7368.1000**	**111.0000**

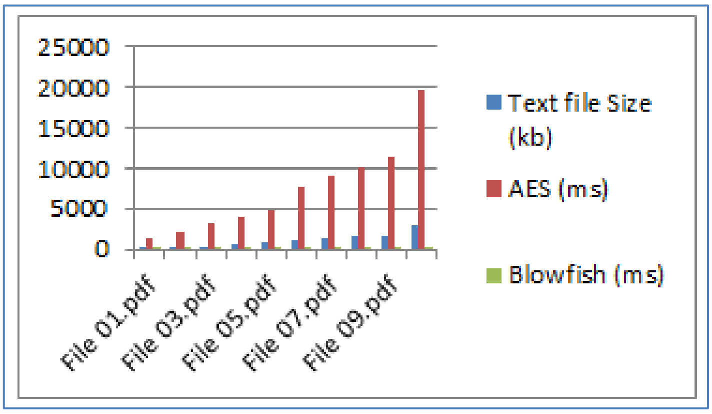


Fig-8: Experimental results for file data types

CONCLUSION AND RECOMMENDATION

In this research, a performance evaluation of symmetric data encryption algorithm was performed. The most commonly used symmetric encryption algorithms are chosen namely: AES and Blowfish.

Since different type of data are transmitted from one place to another or from one network to another there is a need for consideration of these data types in evaluating the performance encryption algorithms. These data types include: image data type, audio data types, video data types and textual file data types.

The performance evaluation metrics are encryption time and throughput. The prototype is developed using JAVA, compiled using the Netbeans IDE7.1.2 with default settings in jdk 7.1 development kit.

Results obtained from this evaluation indicated that blowfish is more efficient than AES. But for Blowfish the encryption time sometime decreases with the increase in data size and its efficiency also increases with complexity of data types. This can be attributed to the fact that Blowfish uses 126, 192 or 256 key sizes.

REFERENCES

1. Kessler, G. C. (1998) "An Overview of Cryptography," published by Auerbach, 1998' (22 Desember 2007). http://www.garykessler.net/
2. Rights, R.F. (2001). SANS Institute InfoSec Reading Room. *Risk*, 1, 27.
3. Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, *1*(2), 6-12.
4. Thambiraja, E., Ramesh, G., & Umarani, D. R. (2012). A survey on various most common encryption techniques. *International journal of advanced research in computer science and software engineering*, *2*(7), 226-233.
5. Pavithra, S., & Ramadevi, E. (2012). Throughput Analysis of Symmetric Algorithms. *International Journal of Advanced Networking and Applications*, *4*(2), 1574.
6. Tunstall, M., Mukhopadhyay, D., & Ali, S. (2011). Differential fault analysis of the advanced encryption standard using a single fault. In *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication* (pp. 224-233). Springer Berlin Heidelberg.
7. Ramesh, A., & Suruliandi, A. (2013). Performance analysis of encryption algorithms for information security. In *circuits, power and Computing Technologies (ICCPCT)*, 2013 *International Conference*, pp. 840-844. IEEE
8. Schneier, B. (1994). The Blowfish encryption algorithm. *Dr Dobb's Journal-Software Tools for the Professional Programmer*, *19*(4), 38-43.
9. Schneier, B. (1996). Applied cryptography: protocols. *Algorithms, and Source Code in C*, *2*, 216-222.
10. Nadeem, A., & Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In *Information and communication technologies, 2005. ICICT 2005. First international conference on* IEEE. 84-89.