Indonesian Journal of Electrical Engineering and Computer Science
Vol. 16, No. 2, November 2019, pp. 988~994
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v16.i2.pp988-944

Time performance analysis of advanced encryption standard and data encryption standard in data security transaction

Zolidah Kasiran, Hikma Farah Ali, Noorhayati Mohamed Noor
Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA, Selangor, Malaysia

Article Info

Article history:

Received Jan 22, 2019
Revised Apr 21, 2019
Accepted May 11, 2019

Keywords:

Advanced encryption standard (AES)
Cryptography
Decryption
Encryption
Encryption standard (DES)
Security transaction

ABSTRACT

The advancement of the data communication technologies has increased the traffic of data exchange over the internet and at the same time created the opportunity of data attack by various party. This paper present Time Performance Analysis Of Advanced Encryption Standard And Data Encryption Standard in Data Security Transaction. In this study we proposed an AES algorithm with different key size, and different file format. Our aim is to safely to transfer the file for using the AES algorithm. Proposed algorithm has done by analyzing the different time taken for both AES and DES, experiments were done by three different file format which were text, image, and voice. Each file format type was tested with five different file sizes. The result of each experiments were analysed and it was confirmed that the AES algorithm have better performance in term of time taken as compared to DES.

Corresponding Author:

Zolidah Kasiran,
Faculty of Computer & Mathematical Sciences,
Universiti Teknologi MARA,
Shah Alam, Selangor, Malaysia.
Email: zolidah@tmsk.uitm.edu.my

1. INTRODUCTION

With the advancement of technology, the traffic of data exchange over the internet are increasing day be day and so does the attack. Compromised data during the data exchange may cause havoc to both sender and recipient. Now every connected devices has the potential be hacked to get the confidential data. To protect data from various attacks, many encryption methods are evolving and before transmission, we must logically encrypt the data to ensure integrity. In the current technology, data leakage is considered a huge test for various basic industries. Therefore, the demand for data security are also in the rise. For this reason, many ways have been proposed to protect the information that is broadcast and received on unsafe channels. To work around this problem, a set of information security templates was created using many cryptographic algorithms [1].

Availability of the Internet and emerging technologies such as social networks and smartphones to ensure the privacy of data in the case despite the exchange of data between partners who are not reliable for the purposes of analysis, general data must be restructured to avoid data users from allocating shared data to others without the consent of the data provider. Protecting sensitive information for individuals is critical. Also, data is increasingly important. If information is leaked, it may affect individuals based on information sensitivity. In order to maintain the privacy of data sharing data, the shared data cannot be stored directly in the data lake [2]. Otherwise, the Administrator may cause the data to leak to unauthorized data users without the consent of the corresponding data provider.

Cryptography is one of the security approaches [3]. It has a set of security objectives to ensure the confidentiality of data. This changes the content of the data being sent to a readable form once received by the recipient and is converted back to its original form. Must be in different areas like banking, military,

rail and media broadcasting. Security at the Electronic Reserve Exchange is also necessary, such as ATM cards, PC passwords and electronic passwords. It has wide ranges as it has the ability to handle different attacks [4]. Encrypt data in unreadable format called privacy data. It's a ruthless process that can interfere with information that is difficult to understand. This privacy is restored to the original data called data decryption process. The security of the information or framework depends on the key used for encryption calculation and encryption or decryption. Changing the reflex back to plain text is called operation decryption process. This is used to protect information during the transmission of users.

This research paper is addressing the performance issue of two popular symmetric cryptography used in securing data transmission over the data communication channel. Common symmetric cryptography techniques are Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

The Data Encryption Standard (DES) is a cryptographic model that presented something about security and interesting things in the 1970s and 1973 in US National Standards. Binary data with many operations is suitable for multiple repetition. DES is very well-known algorithm because it is the first standard symmetric block algorithm and fully describes the set of algorithms. However, the DES algorithm is still used in some applications. However, DES has the smallest length key of sixty-four bit and it is considered unsafe, and the Brute force attack shows that the DES could be attacked [5].

DES provides the influence in security world to protect the information. Fifty-six-bit key is used in DES, and it transforms sixty-four-bit input block into a 64-bit output block. The key looks like a sixty-four-bit quantity, but one bit in each of the 8 octets is used for odd parity on each octet. There are many attacks and methods recorded those revealed the weaknesses of DES, which made it an insecure block cipher. DES is a symmetric key algorithm for encryption of the data, to secure from attacker or unauthorized party. The data encryption standard DES, uses block cipher. DES does not applied one by one bit, it uses the both cryptographic key and algorithm puts to the block of data at same time. DES group used 64 bit block while encryption any message. DES has encryption primitives both permutation and substitution, the secret key uses for it is 64 bit ciphertext by the secret key. Decryption used inverse of the same decrypting process but is uses in orderly the way the keys are used for the input [6].

DES has 16 bit round key to generate the applied of encryption and decryption. The user sends the file to the smart card generator is to encrypted for authentication purpose. Using the DES algorithm, the key size is large. If the user wants the file, having the key to decrypt the file. The block cipher encrypts input block data simulations for whole data, after that process it continue goes for the next flowing blocks. It is a most famous encryption algorithm that has been use all along time. The plain text of block encryption algorithm classified into many blocks that has set the length of block the secret key used by enciphered. Furthermore, DES block cipher, the plain text and key manages the cipher text on dependently for each bit of it. In addition to outcome of cipher may act in combining operation that used to mix plaintext and keys in multifaceted nonlinear style. Currently, it has enhancing to consider secretly to make sure the improvement of requirement addition. It has been upgraded to three times DES that named Triple DES [7]. Cryptographic private key approaches the sender and receiver should aware the private key that needed to use. It uses have many numbers of keys and every key is selected at randomly. The first five rounds are most important to make sure the dependencies.

Although both the AES and DES are commonly used technique, it is claimed that AES to have better performance compared to DES. The advantage of AES over other encryption technologies is that it supports the encryption of large amounts of data and requires less execution time. The 16 bytes are organized in four by four matrix [8]. It designed to prevent all known attacks. It has platform speed and capability based on platform. Leakage of possible information in the channel includes attacks, correlation power analysis attacks, differential power analysis and power analysis attacks associated with energy consumption. The weak attack, scheduled attack, the attacker will decrypt the encryption system by analyzing time it takes to run the algorithm.

The execution time of algorithm depends on input and logical process. It can attack the encryption system by returning to input. The time required to answer the questionnaire may reveal important communication about the system. Side channel attacks are any type of attack based on data derived from the use of encryption algorithms. Many standards, including the design of the cryptographic system, CPU time, and the amount of work that distribute leaked data channel channels in different AES. Variants AES have specific applications that provide security for certain attacks [9-10]. Some people criticize the AES mathematical arrangement which leads to a time-based computation of attacks [11].

The area of AES application researches in AES time taken in encrypting and decrypting process can be found in [12-17]. The AES also had been used to test the efficiency of data security with optimal data throughput [18-19]. Meanwhile [20] proposes a framework that utilized Advanced Encryption Standard (AES) encryption prepare utilizing USB gadget. This paper additionally gives the spine structure to storage frameworks where the security and individual protection is profoundly expanded. If in case the USB gadget

is unavailable, then the person cannot upload the data and similarly cannot download the data. More research was done by implementing AES in Field Programmable Gate Array (FPGA) hardware to secure the data [21].

2. RESEARCH METHOD

The objective of this project is to do comparison study between Encryption Standard (AES) and Data Encryption Standard (DES) performance. Nowadays the development of a technology is increasing accordingly and it is much more important to secure the data for using different methods to hide the data from the individual who needed to obtain the information without to use and modification for other people's information. To avoid that the technology brought the encryption to protect the information from stealing it. AES become the most important algorithm that has applied old symmetric security algorithms after analyzing AES become completely secure according the most symmetric security algorithm.

The AES uses byte that allows easy to implement and understand the system. AES has been designed because of needed security enhancement. AES keys increased into one by one subkeys. For that the subkeys operates on a same function by inverse when encrypting and decrypting. The encryption of AES algorithm is flexible. The method is named as key expansion. AES has different length of keys used 128,192 and 256 bit the block size is fixed concededly by 128bit. The number of rounds of AES algorithm used as 10, 12, 14bit, for the round key depends of a key size while performing the encryption [22].

A. Proposed algorithm (AES)

Cryptography is an actual way to keep sensitive information because sensitive information is stored on the media or circulating on the internet communication path [23]. Advanced encryption standard has four different transformations, (Sub Bytes, Shift Rows, Mix Columns and Add Round Key). That are applied genetically to a specific input data result, and decrypt and encrypted data streams are not the same. AES 256, first 128 bits in the first round and the remaining bits for the next round. Extended key modules are used to key that assigns keys to multiple revisions of the AES algorithm. The frequency revision of the standard advanced encryption algorithm varies depending on the length of the input key [24]. The AES-128 decryption process involves similar number of rounds as the AES-128 Encryption process with corresponding inverse transformations. The initial round includes only the addroundkey step which is the same as in AES-128 Encryption.

In this paper, we compare the performance time of our process with existing DES algorithm [25]. The flow of the research is as below;

a) First, we have checked and reviewed [25] privacy-aware authentication scheme for the mobile cloud services. To overcome the time delay, we show that their scheme is it takes more time to process the authentication. We make sure that their privacy-aware authentications scheme has key weaknesses that can be decrypted easily.
b) Second, our proposed for data privacy using AES provides strong keys to avoid the key weaknesses for existing in [25].
c) Lastly, the proposed method will provide the information of performance time of our process with existing DES algorithm to prove the proposed AES is much stronger than DES.

Figure 1, shows the diagram for the proposed system that is the process of implementing of AES algorithm and start with user, registration, smart card, authentication AES key generation then file security to encrypt and decrypt the files.

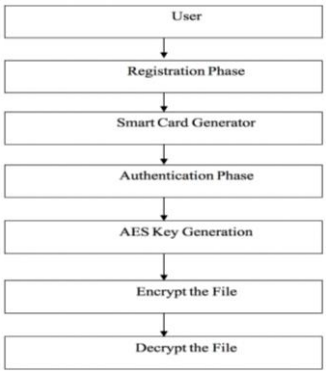

Figure 1. Flow diagram for proposed system

3. RESULTS AND DISCUSSION

The experiments made 3 different file format such as experiments using text file format, image file format, and voice file format. For these three experiments each file format has different file size to check the time taken on encryption and decryption by comparing proposed system AES and existing system DES. The execution time of this experiments are using in milliseconds (ms). The tables and figures in the following section show graphical representation time of encryption and decryption execution time process. In these graph red line shows the decryption time for existing algorithm (DES) and the blue line shows the decryption time for proposed algorithm (AES). AES and DES comparison time based on different file size using two parameters as encryption and decryption time taken. The time taken by AES and DES security on encryption using various files is shown below in the graph. The comparison was done using three different file formats which are text, image and audio/voice. Each file format was experimented with five different file sizes.

3.1. Experiment 1: Encryption and Decryption of Text File Format

In this experiment, five different files in text format were used. The size of these files were 10kb, 50kb, 100, 200kb and 500kb. These file sizes were from the files that is in the computer, and it can test any different file in the user's system. All files were tested for encryption and decryption process. The result of the experiments explained in the next section.

The Figure 2 shows the time taken by AES algorithm for encryption process is shorter than its counterpart DES algorithm for all the file sizes. The trendline in the graph indicated that time taken for DES to encrypt the files is almost exponential with the increase of the file sizes. Whereas the time taken by AES algorithm did not differ as the file size are increasing.

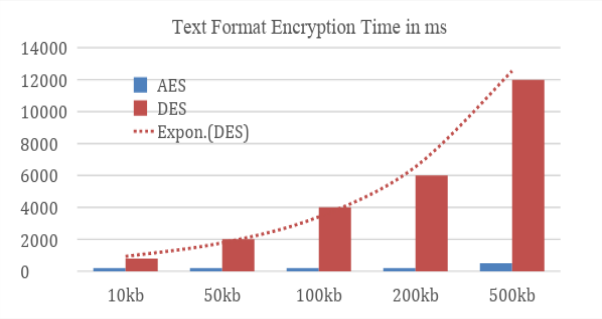

Figure 2. Time based analysis on text file encryption process

Referring to Figure 3, the graph shows the time taken by AES and DES algorithm on decryption using text files is shown above in the graph. Processing time of AES and DES algorithm shows that AES algorithm decryption time are considerably taken shorter time for all file sizes. The DES algorithm shows big leap of time taken as the files size were increased. The time taken for 500kb file size is almost double to file size of 200kb. Meanwhile, the AES algorithm did not shows much different changes as the size of the file were increased. The AES algorithm only took 6ms more to decrypt the 500kb file size compared to 200kb.

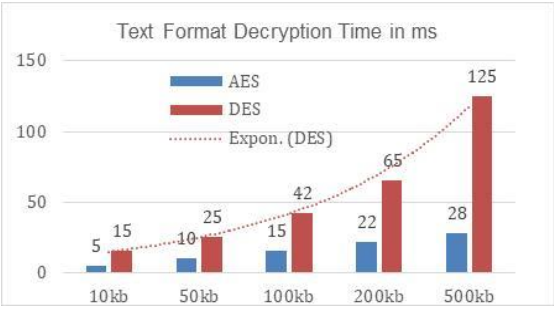

Figure 3. Time based analysis on decryption text files

3.2. Experiment 2: Image File Format

In this experiment, 5 different file sizes of image format were used. The files were 1mb, 1.3mb, 1.5mb, 2mb and 3.1mb. of sizes. These file sizes were from the files that is in the computer, and it can test any different file in the user's system.

3.2.1 Encryption and Decryption Image File Format

The Figure 4, shown the analysis of the time needed to encrypt on various file sizes by two algorithms. The graph had shown that DES algorithm takes much more time while comparing at processed time used by AES algorithm. The graph had indicated that DES algorithm took at least three times longer than AES and the increase time taken for the increasing file sizes are almost in linear trend.

Table 1 below shows the different time taken during the decryption the voice file. Even though the file sizes difference is not obvious, the decryption time is showing a big leap. The result is shown better by the graph in Figure 5.

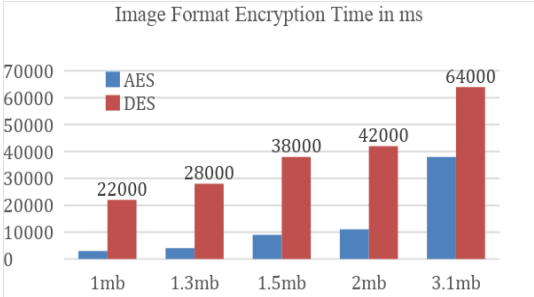

Figure 4. Analysis time based on encryption image files

Table 1. Comparison based on Decryption Image Files

File Size	DES decryption (Time in msec)	AES decryption (Time in msec)
1mb	21013	18842
1.3mb	30244	27323
1.5mb	27044	26267
2mb	59663	39588
3.1mb	60030	20089

The Figure 5 shows data of time taken during decryption process for all five image files. The graph indicated that AES once again perform better than DES in term of shorter time to decrypt the files especially in file size 2mb and bigger. AES and DES seem to have similar time taken in files size smaller than 2mb. Examining the trendline, it is shown that DES has a linear trend of time increase according to the increase of file sizes.

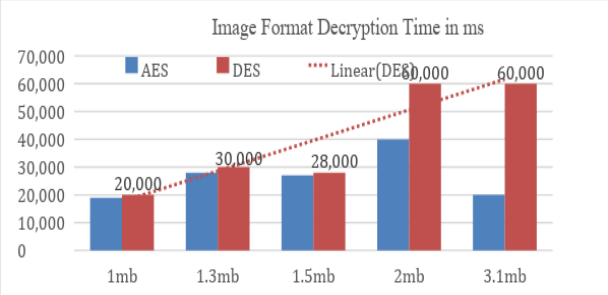

Figure 5. Analysis time based on decryption image files

3.3. Experiment 3: Voice File Format

The third experiment used voice file format as the input data. Five different audio format size were used with sizes of 30 kb, 64 kb, 168 kb, 230 kb and 300 kb. These file sizes were from the files that is in the computer, and it can test any different file in the user's system.

3.3.1 Encryption and Decryption Voice File Format

The Table 2 shows the comparison time taken between DES and DES in encrypting the information in voice format. The Figure 6, shows the time taken by AES and DES algorithm on encryption using for audio files. Encryption process of 30 kb took longer than the other four bigger size files for both AES and

DES. But file size of 64kb took less time than 168 kb size file. The trend of the time taken for the four files seem to be increasing as the files size increase. The overall result shows that once again AES took shorter time in encrypting process.

Table 2. Comparison based on Encryption Voice Files

File Size	DES encryption (Time in msec)	AES encryption (Time in msec)
30kb	20643	4733
64kb	2789	244
168kb	6352	454
230kb	7439	590
300kb	8748	1266

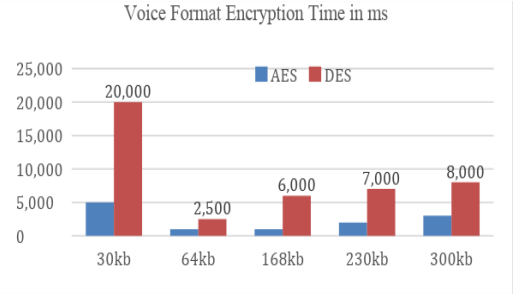

Figure 6. Analysis time based on encryption voice files

The Figure 7, shows the AES and DES comparison of execution time b on different file size using "kb" on voice files. Similar to encryption process, both the AES and DES took much longer time in decrypting the smallest file. The overall performance shown that AES still have shorter time taken in decryption process.

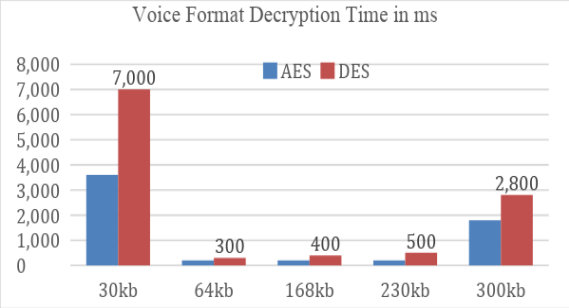

Figure 7. Analysis time based on decryption in voice files

4. CONCLUSION

This paper had exhibited the time performance on two cryptosystem algorithm AES and DES with regards of three different file format and sizes. The analysis of the result of encryption process had shown that DES requires longer time than AES to perform the operation. Similar result was found in the decryption process where DES also requires longer processing time. Nevertheless, some inconsistency was found in voice format. The trendline of encryption and decryption time was not in linear with file sizes nor it was exponential. Both algorithms shows irregularities in the result. In the future, more experiment should be carried out to figure out the reason of such irregularities.

REFERENCES

[1] P. R. M. Rao, "Challenges in Privacy Preserving Data Analytics," *International conference of Electronics, Communication and Aerospace Technology (ICECA)* pp. 185–188, 2017.
[2] C. Scoon, "The Data Privacy Matrix Project : Towards a Global Alignment of Data Privacy Laws," *IEEE Trustcom/BigDataSE/ISPA*, pp. 1998–2005, 2016.
[3] K. Somsuk, "The Improving Decryption Process of RSA by Choosing New Private Key," *8th Int. Conf. Inf. Technol. Electr. Eng.*, pp. 1–4, 2016.
[4] Punam M. C, *et al*, "An efficient implementation of enhanced key generation technique in data encryption standard (DES) algorithm using VHDL," *International Conference on Computing Methodologies and Communication (ICCMC)*, 2017.
[5] P. K. Dey and T.K Dey, "Analysis of the security of aes, des, 3des and idea nxt algorithm," *Int. J. Eng. Sci. Res. Technol.*, pp. 177–181, 2015.

[6] M. Sharma and R. B. Garg, "DES : The Oldest Symmetric Block Key Encryption Algorithm," in *International Conference System Modeling & Advancement in Research Trends (SMART)*, pp. 53–58, 2016.
[7] M. Noura, H. N. Noura, A. Chehab, M. M. Mansour, and R. Couturier, "S-DES : An Efficient & Secure DES Variant," in *IEEE Middle East and North Africa Communications Conference (MENACOMM)*, pp. 0–5, 2018.
[8] B. Indrani, M. Karthigai Veni, "An efficient algorithm for key generation in Advanced Encryption Standard using sudoku solving method," in *International Conference on Inventive Systems and Control (ICISC)*, pp. 1–8,2017.
[9] Flevina Jonese D'souza; Dakshata Panchal. "Advanced Encryption Standard (AES) Security Enhancement Using Hybrid Approach", *International Conference on Computing, Communication and Automation (ICCCA),* pp. 647-652, 2017.
[10] Prakhar Kaushik ; Rana Majumdar, "Timing attack analysis on AES on modern processors" *6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* pp 462-465,2017.
[11] K. Kalaiselvi ; Anand Kumar, "Enhanced AES Cryptosystem by using Genetic Algorithm and Neural Network in S-box," in *IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, pp. 1–6., 2016.
[12] N. Mathur and R. Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection," *Procedia Computer. Sci.*, vol. 79, no. December, pp. 1036–1043, 2016.
[13] B. N. Rao, D. Tejaswi, K. A. Varshini, K. P. Shankar, and B. Prasanth, "Design of modified AES algorithm for data security," *Int. J. Technol. Res. Eng.*, vol. 4, no. 8, pp. 1289–1292, 2017.
[14] P. S. Athinarayanan, S. N. Priya, and R. Supriya, "Secure Data with Key Managers by Using Shamir Scheme and AES Algorithm," *International Journal of Computer Science Trends and Technology (IJCST)* vol. 5, no. 2, pp. 298–301, 2017.
[15] N. Surayati, M. Usop, A. F. Abidin, F. A. Wahab, and N. U. Kamaruddin, "Securing File Transferring System by Implementing AES Algorithm," *World Applied Sciences Journal* vol. 35, pp. 122–132, 2017.
[16] B. Bhat and A. W. Ali, "DES and AES Performance Evaluation," in *International Conference on Computing, Communication & Automation*, pp. 887–890, 2015.
[17] R Chen & X Cheng. "Research on Improved Data Encryption Algorithm Based on AES," *Proceedings of the 3rd International Conference on Intelligent Information Processing,* pp 198-201, 2018.
[18] Soufiane Oukili ; Seddik Bri, "High Speed Efficient Advanced Encryption Standard Implementation," *International Symposium on Networks, Computers and Communications (ISNCC),* pp 1-4, 2017.
[19] Ye Yuan ; Yijun Yang ; Liji Wu ; Xiangmin Zhang, "A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," I*EEE International Conference on Electron Devices and Solid State Circuits (EDSSC),* pp 1-2, 2018.
[20] T. Teja and V. Hemalatha, "Encryption And Decryption – Data Security For Cloud Computing – Using Aes Algorithm," *SSRG Int. J. Computer. Trends Technology*, pp. 80–83, 2017.
[21] Sheetal U. Jonwal ; Pratibha P. Shingare, "Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop," *International Conference on Trends in Electronics and Informatics (ICEI).* Pp 64 – 67, 2017.
[22] G. Raj, R. C. Kesireddi, and S. Gupta, "Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256bit Encryption in Cloud," in *1st International Conference on Next Generation Computing Technologies (NGCT)*, pp. 374–378, 2015.
[23] F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA*, pp. 647–652.,2017.
[24] Z. Kouser, M. Singhal, and A. M. Joshi, "FPGA implementation of advanced Encryption Standard algorithm," in *International Conference on Recent Advances and Innovations in Engineering, ICRAIE*, 2017, pp. 1–5,2016.
[25] Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", Systems Journal, IEEE (Vol: 9, No 3), pp. 805-815, 2015.