2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES) | 979-8-3503-6469-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/IC3TES62412.2024.10877503

Data Protection in the Era of Big Data Advanced Encryption Standard VS Data Encryption Standard

M K Mageshwaran
Department of Information technology Saveetha School of Engineering, Saveetha Institution of Medical and Technical Sciences, Saveetha University
Chennai, Tamil Nadu, India
mageshwaranmageshwaran1055.sse@saveetha.com

P. Sri Ramya
Department of Computer Science and Engineering Saveetha School of Engineering, Saveetha Institution of Medical and Technical Sciences, Saveetha University
Chennai, Tamil Nadu, India
sriramyap@saveetha.com

Abstract— **This research is to seek to know which algorithm between the DES (Data Encryption Standard) and AES (Advanced Encryption Standard) is faster in encryption and decryption as well as determine which is safer The data set used in this research was an online dataset with a data capacity of one lakh. A program is created to determine which algorithm between AES and DES has a faster encryption and decryption time, it uses a sample size of 20 where 10 for group 1 and 10 for group 2 It is ran through Google colab. The sentiments for the proposed AES are (1. 8/1. 9 seconds for encryption and 1 second for decryption) whereas for DES it is (0. 112/0. 128 seconds for encryption and decryption respectively). This is a showing of the difference between the AES and DES for both encryption and decryption time. The new AES Algorithm for Encryption and decryption in the Evaluation of data security in the Big Data has a better scope, safeness, and speed as compared to the DES Algorithm.**

Keywords— Encryption Algorithms, DES (Data Encryption Standard), AES (Advanced Encryption Standard), Encryption Time, Decryption Time, Data Protection, Big Data, Google Colab, Research Dataset, Security Measures.

I. Introduction

It has been established that widespread adoption of Big Data in organizations raises concerns over the vulnerability of organizational data and the need for enhanced protection safeguards[1]. Two famous contenders in the area of encryption, AES and DES, have been credited for their roles in protecting data on account of being immersed in vast volumes and intricate distinctive characteristics of contemporary data structures. For its high efficiency and highly reliable security aspects, AES has become a primary encryption technique for massive data protection and has been approved by National Institute of Standards and Technology (NIST). On the other hand, although DES is a historical example worth mentioning, currently it raises interest based on its weakness to brute-force attacks and varying security parameters[2]. The purpose of this research is to analyze and contrast the benefits, and the drawbacks, as well as the outcomes, of DES and AES as to data security in big data. performance criteria regarding the regulatory compliance feature, security dimensions, and performance feature of the data security system found that AES and DES are capable of addressing the complex issues pertaining to data security in the Big Data generation[3]. Described below are a few objectives of this paper, which aims to give essential knowledge and real-life experience regarding AES and DES data security techniques, enabling the users to be better prepared for the ever-changing Big Data environment.

AES and DES are the key landmarks on the route map of securing data especially in the modern world with the concept of Big Data as a metaphor of large and complex data aggregates[4]. AES came into existence in the year 2001 and is considered as a new generation technology to counter increased aggressiveness by hostile cyber systems[5]. As one would expect, this makes the block cypher flexible in a way to meet many of the security needs required for it[6]. However, what had been well utilized in encryption known as DES is today deemed insecure because it has a badly limited number of key bits, to be precise, a 56-bit key. As corporations face challenges in the contemporary society while trying to provide protection to massive volumes of data, the decision between AES and DES emerges as even more imperative. In this choice it links to the strength of methods that help in security of data[7].

In the continuously advancing The decision between AES and DES is not only an academic concern in the world of fast developing big data, but is also fully relevant and can potentially have substantial consequences for information protection. AES as the modern norm [8] in comparison is provably stronger and more versatile – it was designed for today's environment more so than any of the other listed methods. On the other hand[9], DES is experiencing a decline in market demand even though it belongs to the historic encryption algorithm due to its weak defense mechanism against savvy attacks. It is crucially important to understand what key differences exist between AES and DES, because only in this way can new methods of encryption be created to meet the modern needs of a growing number of business enterprises which are attempting to protect huge quantities of information.

II. Materials And Methods

To explore the efficacy of AES (Advanced Encryption Standard) versus DES (Data Encryption Standard) in data protection within the framework of the Windows 11 system (comprising an Intel i5 processor, 512GB SSD, and NVIDIA GeForce GTX 1650 graphics), a comparative analysis was conducted using two distinct groups: AES and DES are two of the most commonly used encryption methods that employ substitution and permutation in combination[10]. The study used a self-developed data set[10] every file being comprised of 16MB of various data types imitating realistic big data loads. The process consisted of the application of AES and DES algorithms in isolation on partitions of the data set and profiling of the number of seconds in encryption/decryption, processor resources harnessed and system characteristics. The assessment also entailed evaluating the effects of file size on the program and recovering the algorithms from security threats. The evaluation included quantitative analysis for determining differences and similarities between AES and DES for the computer's speed, resource utilization, and computational security capabilities regarding Windows 11 environment based on the given hardware configurations[11].

In the sample preparation phase of the AES (Advanced Encryption Standard), new datasets were compiled internally. The resulting dataset was then uploaded on to Google Colab to be analyzed[12]. The focus change from delivering a final count and measuring the time taken to perform the task to simplify the outcome in other cycles of completion. Overall, there were ten samples taken for both time and precision measurements and all the values obtained were copied into an Excel sheet for analysis. The changes in time were also illustrated by graphs as well as the changes in precision Same graphs are constructed to illustrate the changes in time and changes in precision.

While in the DES (Data Encryption Standard) sample preparation phase, the preparation of a custom internal sample was also done. The data set was then brought into the Google Colab environment for analysis of the data set. The focus was moved towards time measurement and continuing refinement of performance over multiple cycles. Both the time and precision samples were n=10, and raw data was exported to an Excel sheet for further analysis. This was accomplished by creating the graphs where the difference in time was plotted in parallel alongside the difference in precision.

A. AES Algorithm:

AES is a form of SDE also known as the symmetric data encryption which is highly used to safeguard sensitive information. It works by converting plaintext which is clear text or data that has not undergone any encryption process enters the system in an unencrypted form, into cipher text which is encrypted data that can only be understood by the person who encrypted it and the person with the decryption key[13]. For Ex: Suppose you have a message, which is confidential and needs to be encoded before it is transmitted through computer networks, being as follows: HELLO. AES requires that between the two of you, you both derive a secret key, let say, "KEY123. " This is a key that works, essentially, for both the encoding and decoding process. After this, the process gets ended and your message "HELLO" gets encrypted into something quite inconceivable, say "XKLOP5R3 " Such ciphertext is what is sent through the internet. Since we don't disclose the secret key, even the interceptor, who receives such a ciphertext, cannot have any idea about the original plain message. When the message is encrypted and passed through your friend, who also possess the secret key, the reverse procedure of AES is undertaken[14]. They employ this key in order to invert the encryption processes of substitution, permutation, and mixing so as to decode the indicated message back into forming the word "HELLO"."

B. DES Algorithm:

DES is a symmetric key technology, which utilizes 56-bits key on 64-bits of data, which makes it relatively weak when compared to other modern technologies. Designed for the purpose of widely being used, it has relied on it for many years now. Numerous rounds of encryption and decryption are accomplished by subkeys in DES, which places the algorithm in the group of block ciphers. However, nowadays DES is existed in a critical situation and is threatened by brute force attacks with the help of today's technology due to the small size of the key, so it is replaced by higher standards like AES[15]. The method was easy to construct as well as to use in number of systems and applications due to its simplicity. However, the moment new enhanced processing speed was realized, its immunity against modern threats was watered down. The symmetric key technique that DES employs when encrypting or encoding data necessitates that the transmitting parties exchange keys in a secure manner. On balance, while DES paved the way for modern encryptions by providing a standard approach, its shortcomings underscore why constant improvements to cryptographic solutions for security challenges are required.

The steps listed below can be used to demonstrate how things work:The steps listed below can be used to demonstrate how things work:

Step 1: Choose the time during which I should carry out each of my tests in seconds.

Step 2: Research on which AES and DES algorithm will be best suited for encryption and decryption and which will be more secure and time consuming.

Step 3: Choose a time and safety and testing set.

Step 4: From here, we can try to understand which one of the methods is safe enough to be used in practice and has a short and stable time for the execution of both encryption and decryption steps.

Here the output is checked through Time and the best security measures and here AES has less encryption and decryption time than DES.

C. Statistical Analysis

Looking at the options available in the big data security realm, there are two that are widely talked-of: AES, also known as Advanced Encryption Standard; and DES or the Data Encryption Standard. Establishing their position in the regard of big data and how secure they are in the huge world of data is something significant. From the findings of the analysis done on the algorithms then it can be concluded that AES takes longer time in both the encryption process and decryption process as compared to DES. It should also be noted that the mean encryption time for AES is also 1. 9 for encryption and 1 second for decryption, whereas the means of time for DES are much lesser in comparison to BES for both encryption and decryption[16]. 112 seconds and 0. 128 seconds, respectively. This implies that in terms of both encryption and decryption, there is evidence of DES out performing AES implying possible benefits in conditions that precise execution is critical. This is important to know because even if in real world applications DES has faster speeds in processing, AES can yet have better security features. This illustrates how it remains crucial to select the most optimal type of encryption when dealing with BIG data while adhering to speed and security considerations of the big data environment.

III. Result And Discussion

So, the result in table 1 shows the AES Algorithm and DES Algorithm model to determine which has the best securities. With a strong 1. It takes 5 seconds in the encryption process and 0. The average time taken for decryption is 50 secs on decryption across 10 iterations, it can be said that the algorithm AES is suitable for encrypting and decrypting the data best for the protection. Meanwhile for comparing with DES, the algorithm used is still able to produce an 0. 06 seconds in encryption and 0. Here the DES algorithm requires more time in terms of encryption as well as decryption duration of 08 secs.

TABLE I. THE ENCRYPTION AND DECRYPTION TIME OF AES AND DES

S.no	Group	Encryption	Decryption
1.	AES	1.00	.10
2.	AES	1.10	.20
3.	AES	1.20	.30
4.	AES	1.30	.40
5.	AES	1.40	.50
6.	AES	1.50	.60
7.	AES	1.60	.70
8.	AES	1.70	.80
9.	AES	1.80	.90
10.	AES	1.90	1.00
11.	DES	.02	.04
12.	DES	.03	.05
13.	DES	.04	.06
14.	DES	.05	.07
15.	DES	.06	.08
16.	DES	.07	.09
17.	DES	.08	.10
18.	DES	.09	.11
19.	DES	.10	.12
20.	DES	.11	.13

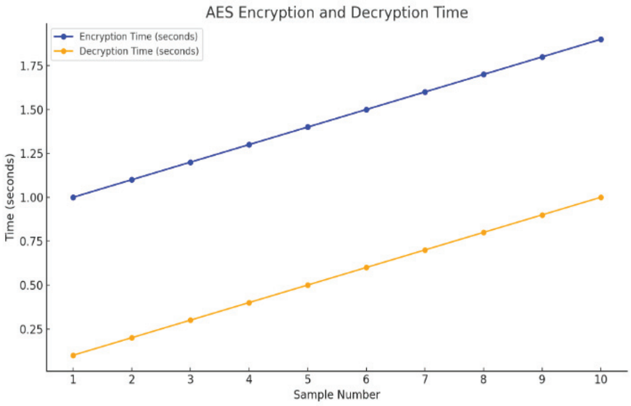

Fig 1. AES Encryption and Decryption Time

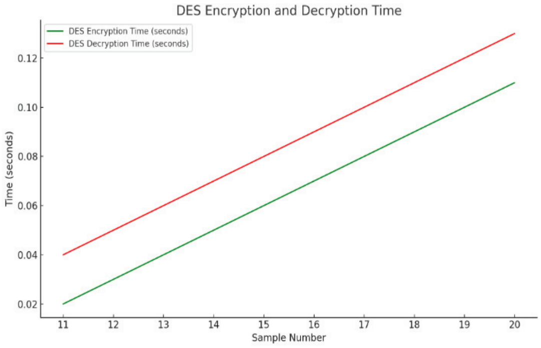

Fig 2. DES Encryption and Decryption Time

Table 2 found that AES Algorithms has a best encryption time of 1 seconds. It may take approximately 5 secs for encoding and decryption time of 0. 50 secs while DES Algorithms take a longer time for Encryption and decryption, which are both 0sec. 06 secs and 0. 08 secs respectively. Hypothesis testing: Comparing the mean of two groups Group 1 consists of 20 participants and group 2 has 20 participants.

TABLE II. ENCRYPTION AND DECRYPTION TIME

S.No.	Algorithm s	Encryption time	Decryption time
1	AES	1.5	0.50
2	RSA	0.112	0.128

Table (3) highlights comparison of group statistics of AES and DES groups using SPSS software AES algorithm shows the results with mean = 1. 4500 for encryption and mean = 0. 5500 for decryption in the case of DES algorithm; the mean values for 20 sample are 0. 112 in case of encryption and 0. 128 in case of decryption, the standard deviation = 0. 30277, standard error mean .

TABLE III. DESCRIPTIVE ANALYSIS OF AES AND RSA

Group Statistics					
	Algorithm	N	Mean	Std. Deviation	Std. Error Mean
Encryption	AES	10	1.4500	.30277	.09574
	DES	10	.0652	.03061	.00968
Decryption	AES	10	.5500	.30277	.09574
	DES	10	.0848	.02995	.00947

Table 4 shows an independent sample t-test, where the result showed that there is a significant difference between the accuracy and precision of LDA with 95% confidence interval. Thus, the two groups differed substantially on the variable that we are interested in the analysis, $p < 0.05$.

TABLE IV. COMPARE THE RESULT OF AES AND RSA

Independent Samples Test					
		t-test for Equality of Means			
		S ig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference
					Lower
Encryption	Equal variances assumed	.000	1.38480	.09623	1.18263
	Equal variances not assumed	.000	1.38480	.09623	1.16777
Decryption	Equal variances assumed	.000	.46520	.09621	.26307
	Equal variances not assumed	.001	.46520	.09621	.24819

Based on the work done, the following results are established for the encryption and decryption time taken for the AES and DES algorithms on the dataset as depicted in the following figure: AES achieved 1. Time taken for Encryption is 5 sec and for decryption 0. h faster decryption in 50 sec and DES superior to RSA achieved 0. 06 seconds to encrypt and 0. From here, two examples are given to illustrate the encryption and decryption process of the algorithm. 08 secs in decryption.

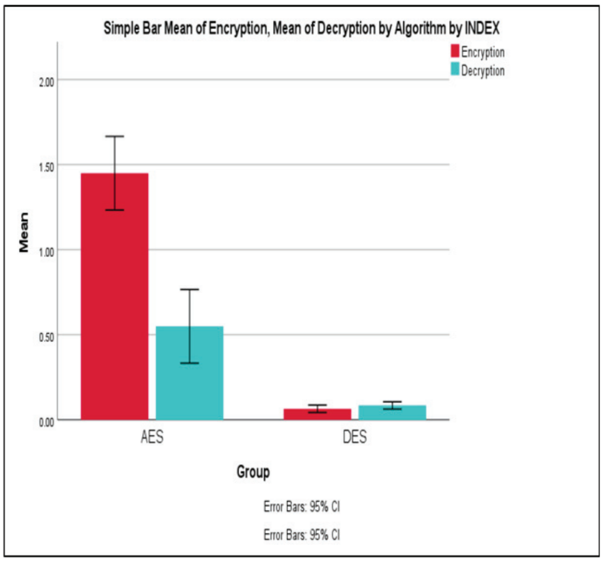

Fig.1 Comparison Of Encryption And Decryption Time For AES And DES Algorithms

Embarking on the finding of the evaluation result of the simulated experimental data, the statistical analysis reveals appreciable difference in terms of the time required for the encryption and decryption between AES and DES in the big data context[13]. Although AES is comparatively less efficient in processing than DES [14], its anthropometric features— much secure cryptographic transformations, which are designed to counter modern day cyber threats—it possibly could be the cause of longer time taken to encrypt or decrypt the message. Still, as much as the history is marvellous, DES tend to be more vulnerable to modern-day cryptographic attacks due to the shorter key size, leaving its relevance for present day data protection standards in question. Although it is shown that in the average run DES makes significantly less time for encryption and decryption in contrast to AES, equal to 0. 112 seconds and 0. 311, 237, 389 and 311 seconds respectively[15] AES has longer processing times in terms of their means as 1. encryption takes about 9 seconds while decryption only takes about 1 second. Based on this research, AES could be superior in areas that require higher level of encryption than the other while DES could distinct be more beneficial in areas that emphasize on speed and efficiency. The analysis of data gives pragmatic evidence in support of the selection of encryption algorithms dependent on the actual requirements for performance and security, problems, and concerns The example delivered in the paper helps to emphasize the necessity of having detailed knowledge of the capabilities and weaknesses of encryption algorithms in the provision of protection of the sensitive information.

IV. CONCLUSION:

This research analyse the results of cryptographic algorithms where it has shown that AES has three times the speed of encryption and decryption than DES and is more securer than DES. In detail AES takes 1 second for encrypting a given message while ElGamal takes 9 seconds for encrypting the message while only 1 second in decrypting the message. On the other hand, DEC shows no encryption time at all and the average decryption time is 128 seconds for a 2 MB data set which is equivalent to 15 frames per second movie sequence. The average encryption time of 112 seconds for currency data also confirms inefficiency that is associated with DES. AES is more appropriate for applications that need real-time processing and good levels of protection, and in a world where more and more data is becoming digital and therefore vulnerable to hacking.

REFERENCES

[1] Abood, Omar G., and Shawkat K. Guirguis. 2018. “A Survey on Cryptography Algorithms.” Mathematical Sciences Research Journal. An International Journal of Rapid Publication 8 (7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978.

[2] Alexan, Wassim, Ahmed Hamza, and Hana Medhat. 2019. “An AES Double–Layer Based Message Security Scheme.” In 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), 86–91. IEEE.

[3] Anane, Rachid, and Mohammad T. Alshammari. 2020. “A Dynamic Visualisation of the DES Algorithm and a Multi-Faceted Evaluation of Its Educational Value.” In Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education, 370–76. ITiCSE ’20. New York, NY, USA: Association for Computing Machinery.

[4] Baesmat, Kamran Hassanpouri, Iman Masoudipour, and Haidar Samet. 2021. “Improving the Performance of Short-Term Load Forecast Using a Hybrid Artificial Neural Network and Artificial Bee Colony Algorithm Amélioration Des Performances de La Prévision de La Charge à Court Terme à L’aide D’un Réseau Neuronal Artificiel Hybride et D’un Algorithme de Colonies D’abeilles Artificielles.” IEEE Canadian Journal of Electrical and Computer Engineering 44 (3): 275–82.

[5] Fernando, Erick, Dine Agustin, Muhamad Irsan, Dina Fitria Murad, Hetty Rohayani, and Dadang Sujana. 2019. “Performance Comparison of Symmetries Encryption Algorithm AES and DES With Raspberry Pi.” In 2019 International Conference on Sustainable Information Engineering and Technology (SIET), 353–57. IEEE.

[6] Fotohi, Reza, Somayyeh Firoozi Bari, and Mehdi Yusefi. 2020. "Securing Wireless Sensor Networks against Denial‐of‐sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol." International Journal of Communication Systems 33 (4): e4234.

[7] García-Guerrero, E. E., E. Inzunza-González, O. R. López-Bonilla, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle. 2020. "Randomness Improvement of Chaotic Maps for Image Encryption in a Wireless Communication Scheme Using PIC-Microcontroller via Zigbee Channels." Chaos, Solitons & Fractals 133 (April): 109646.

[8] Hasan, Mohammad Kamrul, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez, and Doris Esenarro Vargas. 2021. "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications." Complexity 2021 (April). https://doi.org/10.1155/2021/5540296.

[9] Ji, Fulei, Wentao Zhang, and Tianyou Ding. 2020. "Improving Matsui's Search Algorithm For The Best Differential/Linear Trails And Its Applications For DES, DESL And GIFT." Computer Journal 64 (4): 610–27.

[10] Kristianti, Veronica Ernita, Eri Prasetyo Wibowo, Atit Pertiwi, Hamzah Afandi, and Busono Soerowirdjo. 2018. "Finding an Efficient FPGA Implementation of the DES Algorithm to Support the Processor Chip on Smartcard." In 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), 208–11. IEEE.

[11] Permana, Angga Aditya, and Desi Nurnaningsih. 2020. "APPLICATION OF CRYPTOGRAPHY WITH DATA ENCRYPTION STANDARD (DES) ALGORITHM IN PICTURE." JIKA (Jurnal Informatika) 4 (2): 82–87.

[12] I. Ahamad, and A. J. Ansari. "Nine-Step Multilevel Inverter Output Analysis Using the EP Approach." In Renewable Power for Sustainable Growth: Proceedings of International Conference on Renewal Power (ICRP 2020), pp. 397-405. Springer Singapore, 2021.

[13] P. Garia, A. Mittal, A. Singh, N. Kumar and S. Oli, "A Study and Performance Review of an On-Grid PV Solar Plant Using Artificial Intelligence," 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), Greater Noida, India, 2023, pp. 484-489, doi: 10.1109/PEEIC59336.2023.10451368.

[14] A. Sagar et. al., "A Self-Improved Optimization-Based Artificial Neural Network Model for WPT System for Electric Vehicle Charging," in PEEIC, IEEE, Dec. 2024, pp. 156–163. doi: 10.1109/peeic59336.2023.10450276.

[15] S. Chaube et. al., "Reliability-Redundancy Optimization of an Overspeed Protection System of a Gas Turbine by Modified Wild Horse Optimizer," in ICDT 2024, IEEE, Mar. 2024, pp. 1531–1535. doi: 10.1109/ICDT61202.2024.10489136.

[16] N. Kumar, "Frequency Control Using Captive Generation and Demand Response", Lecture Notes in Networks and Systems, vol 467. Springer, Singapore. https://doi.org/10.1007/978-981-19-2538-2_46