Performance Evaluation for DES and AES Algorithms- An Comprehensive Overview

Sriperumbuduru Srilaya
Project Assistant
Department of computer science
CR RAO AIMSCS
University of Hyderabad
India
Srilaya789@gmail.com

Sirisha velampalli
Assitant Professor
Department of computer science
CR RAO AIMSCS
University of Hyderabad
India
sirisha.crraoaimscs@gmail.com

Abstract— Now–a- days there is fast evolution of internet and network applications so information security is very much important for secure transmission of data over an electronic way. Cryptography plays a very important role in providing information security and protecting system from malicious attacks. It has many encryption algorithms to scramble the data and convert it to an unreadable format. Each algorithm differs based on few characteristics such as ability to protect from attacks, performance and speed, memory usage, power consumption. The main aim of designing a cryptographic algorithm is to accomplish security. Each algorithm differs by simulation time, memory usage and power consumption. In this work we evaluate two most commonly used symmetric algorithms namely DES (Data Encryption Standard), AES (Advanced Encryption Standard). A comparative analysis has been done using performance evaluation metrics of each algorithm based on input size. The metrics are encryption/decryption time, throughput, power consumption, memory consumption, simulation time.

Keywords—Cryptography, Symmetric cryptography, DES (Data Encryption Standard), AES (Advanced Encryption Standard).

I. INTRODUCTION

Transmission of digital data in an electronic way has been very enormous due to increase in usage and applications of internet over the wireless network in all the fields. Data security plays an vital role for secure transmission of data over an unsecure channel. In order to transmit sensitive data over the channel, few security measures are required for fast and secure communication. It can be achieved effectively by Cryptography [1]. Cryptography is a field of mathematics and computer science which focuses on secure transmission of data between two parties when third party is present. It is based on methods like encryption, decryption and pseudo random numbers etc. Cryptology consists of two branches namely *i.Cryptography ii. Cryptanalysis*. The word Cryptography is defined as Crypto means *secret* and graphy means *writing*. Cryptography is area of constructing cryptosystems. Cryptanalysis is area of breaking the cryptosystems. The goals of cryptography are confidentiality, authentication, non-repudiation, data integrity, availability and access control. We can attain security if all the goals are achieved successfully. All these factors influence to establish security for different aim of data transmission over the internet. Cryptography provides many security measures for authentication and secure transmission [2] of data over insecure channel. Cryptography includes appropriate techniques to scramble the data so that it can be restored only by an intended user. Encryption is process of translating data into a secret code, so that it attains effective security. The data can be encrypted by using key and encryption algorithm and converted to cipher text which is in unreadable format. Cipher text is given as input to decryption algorithm with a decryption key and plain text is obtained.

The main objective in designing an encryption algorithm is security and performance [3]. The complexity of encryption process depends on the type of algorithm used and key used in encryption and decryption [4] process of particular algorithm. For secure data transmission over the public network data can be protected by encryption. Basic diagram of cryptography is shown in Figure1.

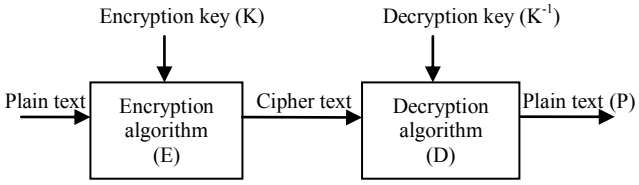

Figure 1: Basic Diagram of Cryptography

The aim of this work is to evaluate performance analysis of DES and AES algorithms based on different metrics. In this work the performance [10] of DES and AES algorithms is calculated for given input size. Performance of encryption algorithm depends on various factors such as encryption time, decryption time, throughput power consumption, speed and efficiency. Based on the performance each algorithm has its own significance and mode of application. Level of security also depends on performance.

Rest of the paper is organized as follows:
In Section II, we will discuss basic terminology of symmetric cryptography. In section III, we will explain overview of literature .In Section IV, we will explain about existing vs proposed work. In Section V, we will discuss about DES algorithm. In Section VI, we will discuss about AES algorithms. In section VII, we will discuss about

978-1-5386-2440-1/18/$31.00 ©2018 IEEE

implementation details. In section VIII we will discuss experimental design. In Section IX, we will discuss about evaluation parameters followed by experimental results and comparative analysis in Section X.

II.BASIC TERMINOLOGY

a. Key

It is value or piece of information which is applied on cryptographic algorithm to convert from plain text to encrypted text.

b. Plain text

The readable data is called as plain text.

c. Cipher text

The text which is obtained after encryption process is called cipher text.

d. Shared key

Shared key or secret key is the identical key which can be used for both encryption and decryption process.

e. Encryption algorithm

The algorithm used to covert from plain text to cipher text with key as input is called encryption algorithm.

f. Decryption algorithm

The algorithm used to covert from cipher text to plain text with key as input is called decryption algorithm. In symmetric cryptography there is shared secret key for encryption and decryption.

III. OVERVIEW OF LITERATURE

A. Classification of cryptography

Cryptography is securing the data from unauthorized access by converting data to an unreadable form. Data which contains the information in readable format is called plain text (P). The plain text is encoded to cipher text(C) by using an encryption algorithm and an encryption key (K) and this process is called encryption (E). The cipher is converted to plain text by using a decryption algorithm and a decryption key (K^{-1}) .The process of converting cipher text to plain text is called decryption (D) There are many types of cryptographic algorithms [3] based on key distribution. Performance of algorithm is based on efficiency and speed. The main purpose of cryptography is to secure the data from unintended access. Based on the key distribution the cryptography is classified into two types. They are I. *Symmetric cryptography II Asymmetric cryptography*. In symmetric key [1] cryptography identical key is used for encryption and decryption process. This cryptography is also called as Secret key or shared key cryptography. Some examples are DES, 3DES, AES, Blowfish, Serpent, IDEA, RC4, Two fish, Three fish etc. In asymmetric cryptography [1] different key is used for encryption and decryption process.

Encryption process is done by recipient's public key which can be known to anyone and decryption process is done by recipient's private key which is kept secret. This is also called public key cryptography. Some examples are RSA, Diffie-Hellman, ECC, EIGamal[4]. Asymmetric encryption algorithms are slower than symmetric because they require more processing power.Classification of cryptographic algorithms is shown in Figure 2.

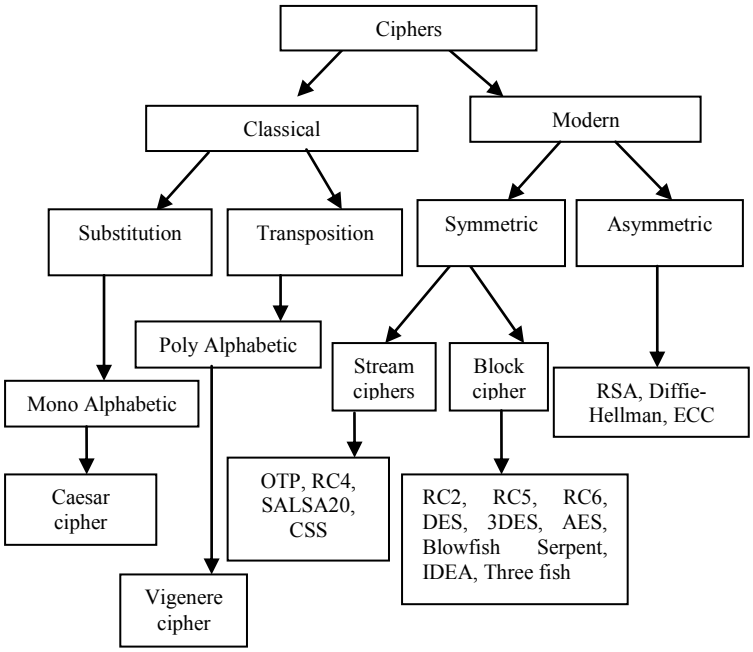

Figure 2: Classification of Cryptographic Algorithms

B. Symmetric Cryptography

In this same key is shared for encryption and decryption process, so this cryptography is called as shared key cryptography or private key cryptography. The primary function of symmetric cryptography is confidentiality. This can be achieved by two ways. They are stream ciphers block ciphers. Stream ciphers: In stream ciphers [2] a bit/byte of plain text is encrypted at a time. In block ciphers the complete block of plain text is encrypted at once. Algorithms in stream cipher are Rc4, Salsa20, CSS, and OTP. Algorithms in block cipher are DES, 3DES, AES, Blowfish, Serpent, IDEA, Two fish and Three fish [5] etc. Strength of encryption algorithm depends on size of key used. If the key size is large then it is complexity of encryption increases. For a particular algorithm encryption done with a larger key is complex to break than a smaller key. The key size varies for each and every algorithm. Example DES uses 64 bit key, AES use 128/192/256/, RC2 uses 64 bit key, Blowfish uses 32-448 bit key. Diagram for Symmetric cryptography is shown in Figure 3.

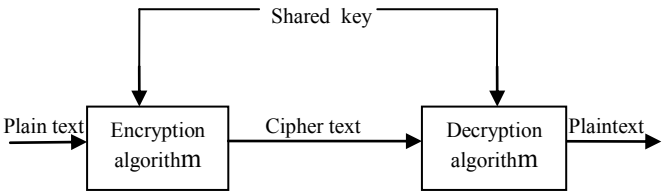

Figure 3: Diagram for Symmetric Cryptography

IV.EXISTING WORK vs PROPOSED WORK

The performance comparison has been done for various algorithms such as DES, 3DES, AES in C# programming language, java, .NET framework. The main draw back in using these programming languages is slow speed because it does not generate machine code, so that it needs an interpreter to run. Unlike existing work the proposed work is implemented in python scripting language and complied in Pycharms 2017.3 IDE. To increase the speed and performance and to get effective results these algorithms are to be implemented in python. We executed DES and AES algorithms in python scripting language and evaluated performance based on various metrics. For a plain text of 32 bytes we calculated encryption time, decryption time, simulation time and throughput for encryption and throughput for decryption.

V. DES ALGORITHM

Data Encryption Standard (DES) algorithm was designed by IBM in the year 1972. It is symmetric block cipher algorithm. The DES uses 64bit key for encryption process. Later, it was confined to 56 bit key by NSA. It uses 56 bit key for encryption of 64bit block. It can be operated in CFB, OFB, CBC, and ECB modes.DES [6] is mostly used in banking sectors.

The processing of DES algorithm is done as follows: The DES algorithm takes 64 bit long plaintext and 56 bit key as input and generates 64 bit cipher text. The mode of operation is called ECB (Electronic code Book) mode if each 64 bit block is encrypted individually. From 64 bit key 8 bits are removed as parity bits from key by subjecting to key permutation.

a. *Encryption process*

1. The 56 bit key is divided into two halves such as 28 bit left half and 28 bit right half.
2. Left circular shift is applied on each half of the key is shifted by one or two bits depending on the round.
3. These two halves are combined and subjected to compression permutation such that 56 bit key is reduced to 48 bit key. This 48 bit compressed key obtained is used to encrypt the plain text block of this round.
4. The data block is divided into two halves i.e. each of 32 bit.
5. One half of block is subjected to expansion permutation to increase the size of the block to 48 bits
6. Output of step 5 is XOR'ed with compression key of 48 bits which is obtained in step 3.
7. Output of step 6 is fed to S-box, which substitutes key bits and reduces 48 bit block to 32 bit block.
8. The output of S box is subjected to P- box for permutation of bits
9. The output of P box is XOR'ed with other half of data block.
10. Then the two blocks are swapped and becomes input for the next round.
11. The rotated key halves obtained from step 2 are used in next round.

b. Key generation process

1. In DES key generation process initially key size is 64 bit then the key is permuted and reduced to 56 bits.
2. The 56 bit key is divided into left part and right part each 28bits.
3. Left circular shift is applied on both the parts and then permuted choice 2 is applied on 56 bit key and reduced to 48 bit final key.

c .Decryption process

1. In DES decryption process is basically same as encryption process.
2. Cipher text will be input to DES algorithm and we get the corresponding plain text.
3. Here the use of key is in reverse order i.e. round 1 with K_{16}, round 2 with K_{15} and round 16 with K_1. Block diagram of DES is shown Figure 4 and Key generation process is shown in Figure 5.

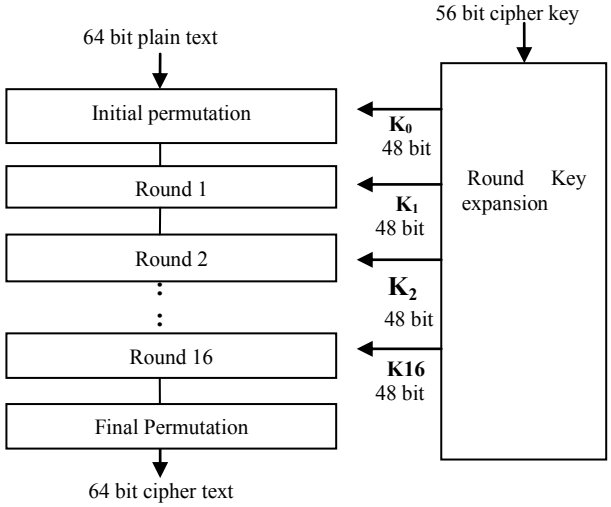

Figure 4: Block diagram of DES

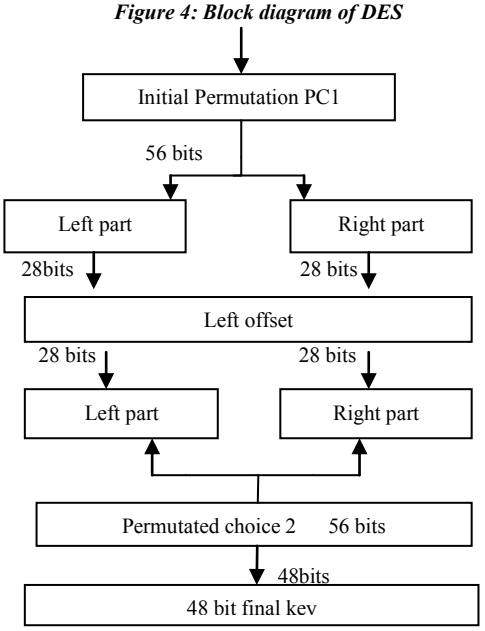

Figure 5: Key generation of DES

VI. AES ALGORITHM

DES has small key size and less processor power and advancement of DES [7] algorithm is AES [9] (Advanced Encryption Standard), its original name is Rijndael. It is designed by Joan Daemen and Vincent Rijmen. It was first published in the year 1998. AES[7] is block cipher and has fixed number of bits in block .It has block size of 128 bit and generates cipher text of 128 bit block[8].It supports key length of 12/192/256 bit. No of rounds that convert plain text to cipher text depends on key length i.e. 10 rounds of repetition for 128 bit key ,12 rounds of repetition for 192 bit key and 14 rounds of repetition for 256 bit key. The principle of AES [13] algorithm is substitution-permutation network. The AES [12] algorithm is rich in security and speed [11].

The processing of AES is done as follows:

The block size is fixed and only the key size varies, all the transformations are done on the states. The results in states are intermediate. Following are the operations applied on state during each round. The following process is for encryption of 128 bits.

a. Common rounds

From round 1 to 9 all the below operations are done

- Substitution rounds
- Shift rows
- Mix columns
- Add round key

b. Final round

Round 10 is the final round in 128 bits key size and the final round doesn't have mix columns operation.

- Substitution rounds
- Shift rows
- Add round key

It is 10^{th} round. Execute all operations except Mix columns in final round.

c. Encryption process

In this process each round consists of four operations.
Substitution rounds: Non linear substitution done with the help of (s-box) substitution.

Shift rows: The bytes in last three rows are shifted cyclically depending upon the row location. This is simple byte transposition.

Mix columns: A matrix is multiplied with each column vector. This round is Multiplication of matrix of each column of state to new column. These operations are done at column level

Add round key: This is a XOR operation between present state and round key.

d. Decryption process

It is reverse of encryption process. In this operations performed are

- Inverse Substitution rounds
- Inverse Shift rows
- Inverse Mix columns
- Inverse Add round key

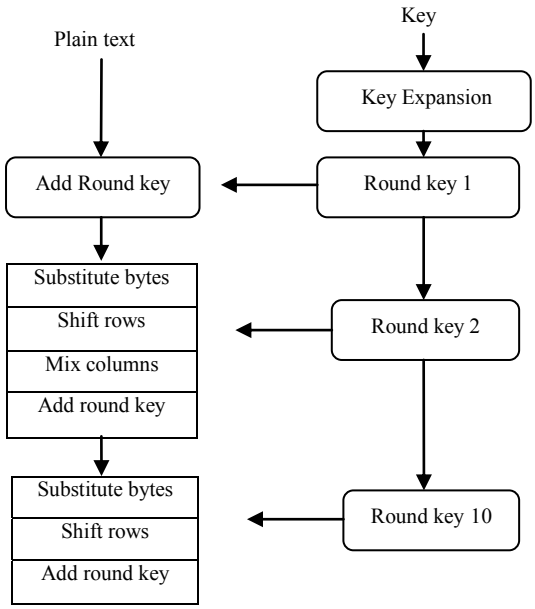

Figure 6: Block diagram of AES

The encryption operations have few steps. Firstly add around key operation is performed then round key is applied to block consisting of substitution bytes, shift rows and mix columns, Add round key. This operations are performed iteratively KN_r times depending on the key size.

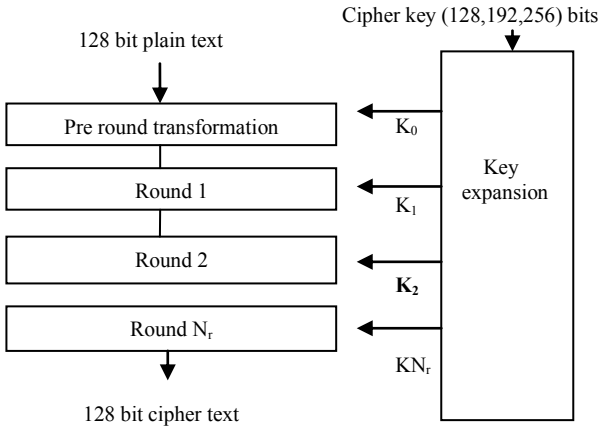

Figure 7: AES structure

VII.IMPLEMENTATION DETAILS

Code is implemented in python 3.6.4 scripting language and compiled in Pycharm 2017.3 IDE. The implementation is tested and optimized for maximum performance evaluation. The following are some of the main reasons why python is used:

- Python is an interpreted language which executes code line by line so that it makes debugging easy.
- Python is a high level programming language it provides many classes and built-in methods so that it assist a programmer to implement the cryptographic algorithms. Packages used are os, time and psutil.

The primary goal of this work is to compare the performance of DES and AES algorithms where each algorithm is implemented in python and various performance metrics are calculated.

VIII.EXPERIMENTAL DESIGN

Hardware specifications for our experiments are as follows:
We used a laptop of Processor: Intel (R) Core(TM) i5-3337U CPU@1.80 GHz in windows 8 environment in which performance is evaluated.Installed Memory (RAM): 4.00 GB System type: 64-bit Operating System. The following task is to be done:

- Comparative study of DES and AES based on encryption, decryption time, simulation time, Throughput for encryption and decryption time for a given plain text of 32 bytes.

IX. EVALUTION PARAMETERS

a. Encryption time
The Encryption time is defined as the time the encryption algorithm takes to convert from original text to cipher text.

b. Decryption time
The Decryption time is defined as the time the decryption algorithm takes to convert from cipher text to original text.

c. Memory required for implementation
Memory size depends on type of encryption algorithm used for implementation. The algorithm with less memory size is beneficial. The memory size depends on types of operations performed in algorithm.

d. Simulation time
The time required for an algorithm to process completely over the data is called stimulation time It mainly depends on speed of the processor and also complexity of the algorithm.

e. Throughput of Encryption
It is calculated as T_p (Total plain text in bytes) divided by (E_t is the encryption time in seconds). It specifies the speed of the encryption.

f. Throughput of Decryption
It is calculated as T_p (Total plain text in bytes) divided by (E_t is the decryption time in seconds).

g. Power consumption
As the throughput of the encryption increases then the power consumption decreases.

X. EXPERIMENTAL RESULTS

By execution of each algorithm in python the following results are obtained. Comparative analysis of DES and AES when plain text is 32 bytes is shown in Table 1 Comparative analysis is shown graphically in Figures 8, 9, 10, 11, 12 and 13.

TABLE 1: Comparative Analysis among DES and AES when plain text is 32 bytes

Evalution parameters	**DES**	**AES**
Plain text size	32 bytes	32bytes
Cipher text size	48bytes	50bytes
Encryption time	0.006sec	0.022sec
Decryption time	0.011sec	0.023sec
Stimuation time	0.017sec	0.045sec
Throughput for encryption	53333.3	1454
Throughput for decryption	2909	711.1

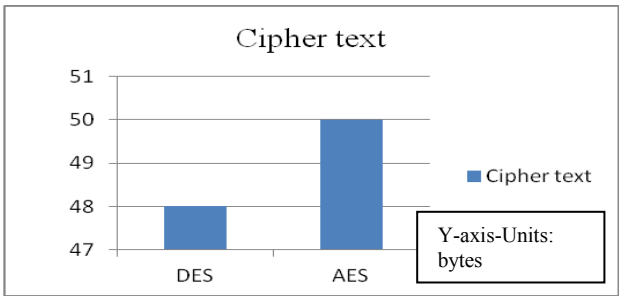

Figure 8: Comparison of cipher text-DES vs AES

In figure 8, the cipher text size of DES is less compared to AES. For 32 bytes of plain text the cipher text obtained in DES is 48 bytes were as in AES is 50 bytes.

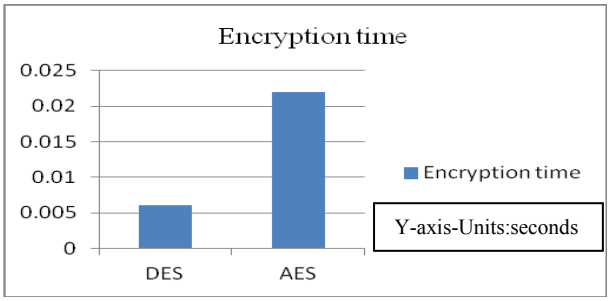

Figure 9: Comparison of Encryption time -DES vs AES

In Figure 9, Encryption time for DES is less compared to AES.

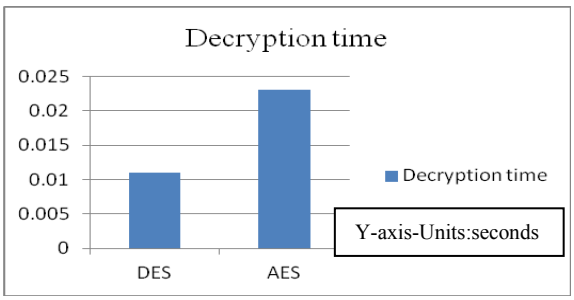

Figure 10: Comparison of Decryption time-DES vs AES

In Figure 10, Decryption time for DES is less compared to AES.

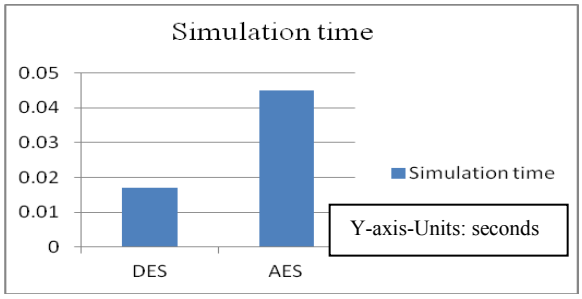

Figure 11: Comparison of Simulation time -DES vs AES

In Figure 11, Simulation time for DES is less compared to AES.

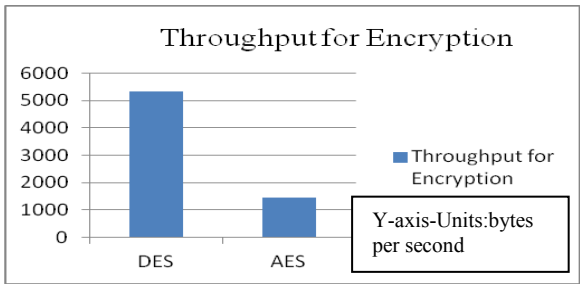

Figure12: Comparison of Throughput for Encryption - DES vs AES

In Figure 12, Throughput of Encryption for DES is more compared to AES.

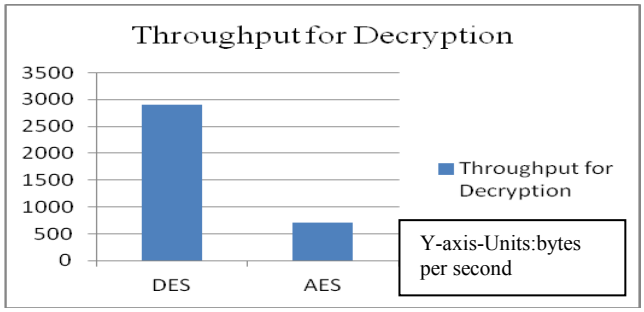

Figure13: Comparison of Throughput for Decryption - DES vs AES

In Figure 13, Throughput of Encryption for DES is more compared to AES.

TABLE 2: Comparison of DES and AES

Comparison of DES and AES algorithms based on key size, block size, rounds, level of security and attacks is shown in table 2.

Methods	**DES**	**AES**
Developed by	IBM	Vincent Rijmen, Joan Daemen
Year	1977	2002
Key size	56bits	128/192/256bits
Block size	64bits	128bits
No of rounds	16	10,12 or 14
Algorithm structure	Feistel structure	Substitution permutation
Security	Comparatively less secured	Secured
Attacks	Brute–force attack	Key related attack, Side channel attack

XI. CONCLUSION

In cryptography, efficiency and speed of the algorithm is very much important. It only depends on the performance of the algorithms. Operations performed for encryption and decryption process plays a major role in measuring the performance. In this work, we evaluated performance of DES and AES algorithms based on few important parameters. Based on plain text of 32bytes it was concluded that encryption and decryption time DES is least compared to AES. Throughput of encryption and throughput of decryption of DES is more compared to AES. From our work it was concluded that performance of AES is better than DES.

In future we will do performance analysis by implementing them using OpenMP distributed programming model in a HPC cluster and compare sequential vs parallel implementation of the algorithms.

XII. ACKNOWLEGEMENT

I would like to express my deep gratitude to **Dr. D.N. Reddy, Director, CR Rao Advanced Institute of Mathematics, Statistics & Computer Science** for giving me great opportunity to do this work.

REFERENCES

[1] Schneier, Bruce. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[2] Buchmann, Johannes. *Introduction to cryptography*. Springer Science & Business Media, 2013.

[3] Delfs, Hans, Helmut Knebl, and Helmut Knebl. *Introduction to cryptography*. Vol. 2. Berlin etc.: Springer, 2002..

[4] Mollin, Richard A. *An introduction to cryptography*. Chapman and Hall/CRC, 2006.

[5] Potlapally, Nachiketh R., Srivaths Ravi, Anand Raghunathan, and Niraj K. Jha. "A study of the energy consumption characteristics of cryptographic algorithms and security protocols." *IEEE Transactions on mobile computing* 5, no. 2 (2006): 128-143.

[6] Han, Seung-Jo, Heang-Soo Oh, and Jongan Park. "The improved data encryption standard (DES) algorithm." in *Proceedings of IEEE International Spread Spectrum Techniques and Applications Proceedings, 1996,* pp. 1310-1314.

[7] Yassein, Muneer Bani, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *Proceedings of* IEEE *International Engineering and Technology (ICET) Conference,* 2017, pp. 1-7

[8] Alfadel, Mahmoud, El-Sayed M. El-Alfy, and Khaleque Md Aashiq Kamal. "Evaluating time and throughput at different modes of operation in AES algorithm," in *Proceedings of IEEE* 8th *International Information Technology (ICIT) Conference*,2017, pp. 795-801.

[9] García, Daniel F. "Performance Evaluation of Advanced Encryption Standard Algorithm," in *Proceedings of IEEE Second International Mathematics and Computers in Sciences and in Industry (MCSI) Conference, 2015* , pp. 247-252.

[10] Kansal, Shaify, and Meenakshi Mittal. "Performance evaluation of various symmetric encryption algorithms," in *Proceedings of IEEE International Parallel, Distributed and Grid Computing (PDGC) Conference, 2014* , pp. 105-109.

[11] Mandal, Akash Kumar, Chandra Parakash, and Archana Tiwari. "Performance evaluation of cryptographic algorithms: DES and AES," in *Proceedings of IEEE Electrical, Electronics and Computer Science (SCEECS) Students' Conference , 2012*, pp. 1-5.

[12] Bhat, Bawna, Abdul Wahid Ali, and Apurva Gupta. "DES and AES performance evaluation," in *Proceedings of IEEE International Computing, Communication & Automation (ICCCA) Conference, 2015 on*, pp. 887-890.

[13] Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms," in *Proceedings of* IEEE *First international* In *Information and communication technologies conference, 2005. ICICT 2005*, pp. 84-89.