www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19596-19611

Performance Study of Key Developer Data Encryption and Decryption Algorithm (KDDEDA) with AES, DES and BLOWFISH

Miss. A.Usha, Dr. A. Subramani
M.Phil. Scholar,
Department of Computer Science,
Govt. Arts College, Dharmapuri – 636705,
E-mail:usha56chiru93@gmail.com
Assistant Professor,
Department of Computer Science,
Govt. Arts College, Dharmapuri – 636705,
E-mail:subramani.appavu@gmail.com

Abstract

Information security is an important issue in network communication. Because of the significance, accuracy and sensitivity of the information it is a big security and privacy issue, making it necessary to find appropriate solution, security and privacy has become as important concern. Cryptography is making sure to secured data protection. Cryptography concept is used facilitate for secret communication among the military communications. The present days different types of cryptography algorithm are used to secure data such AES, DES and blowfish. The traditional algorithms have some of the drawbacks like speed, key size and performance. The proposed a new cryptographic algorithm named as KDDEDA [Key Developer Data Encryption and Encryption Algorithm], The KDDEDA using to transmit confidential data for source to destination with speed data transmission and performance. KDDEDA also analyse encryption/decryption time, memory space, key size, block size and performance.

Key Words: AES, DES, BLOWFISH, KDDEDA

1. Introduction

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text.

Cryptography is a powerful tool used to protect the information in computer systems. When a browser is used for home banking, numbers of cryptographic algorithms are being used to protect data send to the bank. When someone login to computer, the password is protected by cryptographic hash functions. An email it is often encrypted using SSL while sending it [9]. In cryptography original message is basically encoded in some non readable format. This process is called encryption. The only person who

DOI: 10.18535/ijecs/v5i12.62

knows how to decode the message can get the original information. This process is called decryption [5].cryptography is basically there are three techniques: symmetric, asymmetric and hash function [6, 18]. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. The symmetric algorithm is the AES, DES, and Blowfish. In asymmetric key cryptography, there are two keys: private key and public key. Both are required to encrypt and decrypt a message. Message sender encrypts the message or data using public key that may be known to all publicly [17].

2. Literature Review

Srinivas B.L et.al (2014) describes accuracy and privacy is the big issue in multimedia data transmission. The experimental work has been performed on DES and BLOWFISH algorithm to find key length and key size. Aman Kumar et.al (2012) compared with DES secret key and RSA public key based algorithm. There are two main feature that specify and differentiate one algorithm from another are the ability to secure and protect the data against attacks and speed of encryption and decryption.

Swati Kashyap et.al (2015) discussed DES, 3DES, AES & RSA comparative analysis result shows that the throughput of the encryption is calculated by dividing the total plaintext in MB by total encryption time. Milind Mathur and Ayush Kesarwani (2013) compared with a performance evaluation of selected symmetric encryption algorithm. The selected algorithm are AES,DES,3DES,RC6,Blowfish and RC2.Nidhi Singhali and J.P.S.Raina (2011) describes to compare the AES algorithm with different modes of operation(Block Cipher) and RC4 algorithm(Stream Cipher) in terms of CPU time, encryption time, memory utilization and throughput at different setting like variable key size and variable data packet size.

Shailja kumara and Jyoti Chawla (2015) analysis on different parameters of encryption algorithms (AES, RC6, IDEA,BLOWFISH) such as Architecture, Flexibility, Reliability, Security and Limitation for information security that are essential for secure communication.Pritesh Kumar Prajapati et.al (2014) express encryption algorithm plays an important role in communication security where encryption time, memory usage and battery power are the major issue of concern. The selected encryption AES, DES and RSA algorithm are used for performance evaluation.

Kalyani P.Karule and Neha V.Nagrale (2016) show cased the selected encryption algorithm AES and RSA are used for performance evaluation files in different formats like text files, pdf files, word document and image are used and the experimental result based on encryption files size and encryption time is recorded. Youssouf mahamat koukou et.al (2016) says to compare the avalanche effect integrity checking using ECB and CBC mode of the different algorithm Blowfish, Cast-128, DES and AES for one bit change in key and one bit change in the Cipher text.

Harsh Kumar Verma and Ravindra kumar Singh (2012) discussed performance analysis of RC5, Blowfish and DES block cipher algorithms have been done on the basis of execution time and resource utilization.CPU utilization and memory Utilization both are considered for determining resource Utilization. Ms.Pallavi H.Dixit et.al (2013)define the comparison between two cryptographic algorithm AES and Blowfish algorithm on the memory size, encryption cycle and decryption cycle for both algorithm on ARM7 etc. for small embedded system like mobile, smart card etc blowfish is best algorithm for security.

Jawahar Thakur and Nagesh Kumar (2011) describe comparison between three most common symmetric key cryptography algorithms DES, AES and Blowfish such as speed, block size and key size AES showed poor performance results compared to other algorithms. Shaza D. Rihan et.al (2015) describe the performance the two encryption algorithms: AES and DES. The performance measure of encryption algorithms will be conducted in terms of processing time, CPU usage and encryption throughput on Windows and Mac platform for a different text size. 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.

Simar Preet Singh, and Raman Maini (2011) The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed.AES showed poor performance results compared to other algorithms, since it requires more processing power. Pratap Chandra Mandal (2012) comparison between four most common and used Symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of these parameters: rounds, block size, key size, encryption/decryption time, CPU process time in the form of throughput and power consumption These results show that blowfish is more suitable than AES.

Ranjeet Masram et.al (2014) describe analysis and comparison of some symmetric key cryptographic ciphers (RC4, AES, Blowfish, RC2, DES, Skipjack, and Triple DES) on the basis of encryption time with the variation of various file features like different data types, data size, data density and key sizes. Behrouz A. Forouzan, Debdeep Mukhopadhyay(2012) analysed the input data, cipher algorithms are classified as block ciphers, in which the size of the block is of fixed size for encryption and stream ciphers in which a continuous stream is passed for encryption and decryption. A.subramani and A.usha (2016) analyse the encryption and decryption conversion time Of AES,DES,BLOWFISH,RSA,RC4, RC6 and TRIBLE DES algorithms on different settings of dataset.

3. Problem Statement

A number of cryptography techniques have been proposed in the recent scenario. There are many advantages and disadvantages in those algorithms. Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form by using encryption and decryption techniques. Unsecured data that travels through different networks are open to many types of attack. The cryptography ensures that the message should be sent without any alternations and only the authorized person can be able to open and read the message. In this thesis paper I proposed new cryptographic algorithm named as Key Developer Data Encryption and Encryption Algorithm (KDDEDA) for using security algorithm in cryptography. The KDDEDA using to transmit confidential data for source to destination with speed data transmission and performance. KDDEDA also analyse encryption/decryption time, memory space, key size, block size and performance. Information security is an important issue in network communication.

4 Objective

AES Its whole 56 bit key space can be looked in roughly 22 hours.AES The size of key length is too long that makes it complex now and then.DES, some secret key frameworks secured with DES was constrained to 8 characters and would noiselessly truncate something else secure passwords (coordinate just the initial 8 characters). It's conceivable to savage power in limited time on cutting edge processors, so nobody utilizes it for anything genuine any longer .Advanced encryption standard is most testing to actualize in programming. Blowfish configuration is anything but difficult to break down which makes it impervious to usage mistake.

5. AES [Advanced Encryption Standard]

The Advanced Encryption Standard (AES), also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [4] AES encryption is fast and flexible [5]. AES can be operated in different modes of Operation like ECB [Electronic Code Book], CBC [Cipher Block Chaining], CFB [Cipher Feedback], OFB [Output Feedback] and CTR [Counter]. In certain modes of operation they work as stream cipher. AES uses various rounds in which each round is made of various stages. To provide security AES uses types of transformation, mixing, substitution permutation and key adding each round of AES except the last uses the four transformations [7,8].Advanced encryption standard can be implemented on various platforms especially in small devices Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption[5,14].

6. DES [Data Encryption Standard]

The Data Encryption Standard (DES) is feisted substitution permutation network (span) cipher. It was published in January 1977.Data Encryption Standard[DES] is a widely used method of Data Encryption using a private(secret key)that was judged so difficult to break by the U.S government that it was restricted from expiration to other countries[16]. Data encryption standard for encryption data was a symmetric algorithm know as the data encryption standard[DES][8].the bit position 8,16,24,32,40,48,56,64 discarded from the key length.DES is based on two fundamental attributes of cryptography: substitution[confusion] and Transposition[diffusion], DES is based on a cipher known as the Feistel block cipher[13].DES consists of 16 cycle, each of which called as round[9,10]. A 16 cycle feistel system is used with an overall 56 bit key permuted into 16, 48 bit sub keys, one for each cycle [3, 2]. In each cycle, data and key bits are shifted, permutated, XORed, and sent through, 8 s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process, performed in reverse [7].

7. BLOWFISH

Blowfish was designed in 1993 by Bruce Schneider as an alternative to existing encryption algorithms. Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data .It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses [14]. It is only suitable for applications where the key does not change often, like a communications link or an automatic file encryption [8].

8. Key Developer Data Encryption and Decryption Algorithm

Key developer data encryption and decryption algorithm is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. The block size is 64 bits and the key can be any length up to 48 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors with large data caches. It is suitable for applications the key does not change often, like a communication link or an automatic file encryption.

DOI: 10.18535/ijecs/v5i12.62

Table 8 KDDEDA Algorithm

Algorithm	KDDEDA
Structure	Feistel Network
Key Size	48 bit
Block Size	64 bits
Processing Round	16

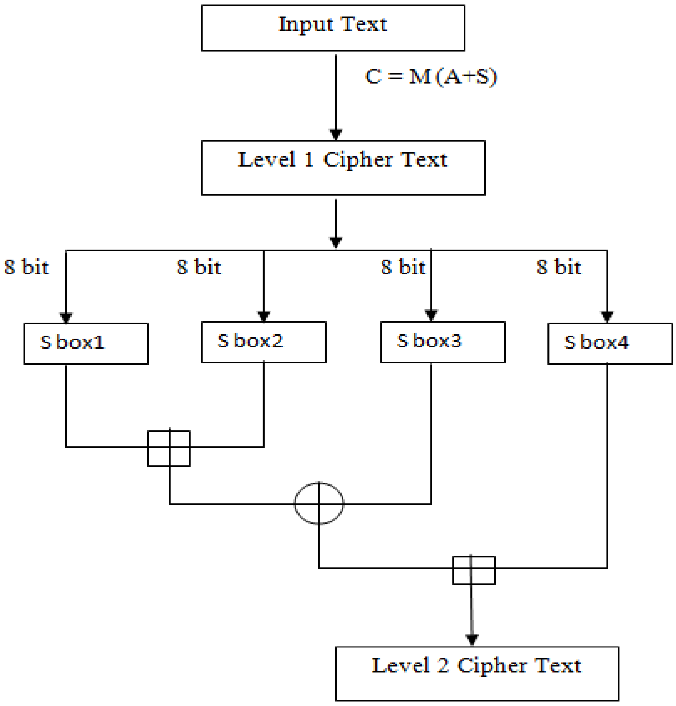

Figure 8 Methodology for EDDEDA algorithm

Some specifications of KDDEDA algorithm are as follows

- A 64 bit blocks cipher with a variable key length.
- There is a P-array and four 32-bit S-boxes. The P-array contains 18 of 32-bit subkeys, while each S-box contains 256 entries.
- The algorithm consists of two parts: a key-expansion part and a data-encryption part.

- Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes.

- The data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key and data-dependent substitution.

- All operations are XORs and additions on 32-bit words. The input is a 64 bit data element.

The process of Sub key generation is illustrated as follows

- Initialize P array and S boxes with Hexadecimal digits of Pi.
- XOR P-array with the key bits (i.e., P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key)…

- Use the above method to encrypt the all-zero string.

- This new output is P1 and P2.

- Encrypt the new P1 and P2 with the modified sub keys.

This new output is now P3 and P4.Repeat the above steps until we get all the elements of P array i.e P1, P2….

8.1 Algorithm

8.1.1 The encryption algorithm for KDDEDA is illustrated as follows

```
Algorithm KDDEDA ( )

Begin

Step 1:  Read a plain text and stored M in plain text

Step 2:  Plain text M convert into cipher text C using the formula M (A+S) whereas A as constant (1)
         and S as a plain text length+1.M is the plain text and 32 bit Pi is the key generations.

Step 3:  Divide M into two 32-bit halves: XL, XR
Step 4:  Generate a random number say Rn and set the variable Flag to 0.Represent Rn in form of 16
         bit binary string say str.
            For i = 1 to 16
            If str[i] == '0'
            Set Flag=1
            If Flag ==”1”
            XL = XL XOR Pi
           XR=XL XOR XR
 Else
       Swap XL and XR
       Step 5:    Swap XL and XR (Undo the last swap)
       Step 6:    XR=XR XOR P17
       Step 7:    XL=XL XOR P18
       Step 8:    Concatenate XL and XR
```

8.1.2 The Decryption algorithm for KDDEDA is illustrated as follows

```
Step 1:    Cipher text values
Step 2:    XL=XL XOR P18, XR=XR XOR P17
Step 3:    Step 5: Swap XL and XR (Undo the last swap)
Step 4:    For i = 1 to 16
              If str[i] == '0'
              Set Flag=1
              If Flag ==”1”
              XL = XL XOR Pi
```

```
            XR=XL XOR XR
      Else
            Swap XL and XR


Step 5:    C = M (A * S)
Step 6:    Plain Text (original Data)
```

The F function uses the substitution boxes of which there are four, each containing 256 32-bit entries. If the block XL is divided into 8-bit blocks a, b, c and d, the function F(XL) is given by the formula: F(XL)= ((S1,a + S2,b mod 2^32)   S3,c) + S4,d mod 2^32 (1) The decryption process is just reverse of the encryption process. The modified approach for blowfish algorithm consists of the same specifications as that of Blowfish algorithm except that of a random number defined as Rn .Random number Rn = rand( ) where rand is a function in NS2 that generates a random number and Rn be any integer .

This random number can be any integer without any limit. We restrict the range of this random number to be between 0 to 65535.Next consider a variable say Flag. The value of this variable can either be 0 or 1.Initially its value remains 0.Next represent Rn in binary format of 16 bit string from MSB to LSB. The positions in which a ‘0’ is encountered from MSB to LSB then set the variable Flag otherwise remains reset. Also note the position of ‘0’ in the string as a round number of blowfish algorithms. The positions in which the value of variable Flag is reset, and then encryption process remains the same as for the blowfish algorithm in that round. But when the positions of the string have value of variable Flag as set, then no F function will be applied in that round which means that value of XL is directly passed for calculation of XR.

8.2 THROUGHPUT

The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm.

$$\text{Throughput} = \frac{\text{Total Plaintext in Mega Bytes}}{\text{Encryption Time}}$$

8.3 Experimental Design:

The experiment is performed on two platforms a laptop core I5, 2.5 GH. CPU with operating system windows 7 and Intel core I5 with Linux operating system. Three performance metrics are collected: encryption time, CPU usage and encryption throughput for the two encryption algorithms AES, DES, BLOWFISH and KDDEDA Algorithm. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time. The CPU usage is the percentage of the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU usage is used in the encryption process, the higher is the load of the CPU. The experiment is performed to measure the effect of the changing data size and the platform for each cryptography algorithm.

8.4 Comparative Study Of Kddeda With Des, AES And Blowfish

Input size(KB)	AES	DES	Blowfish	KDDEDA
15	3.8000	5.0700	4.1990	3.4200
30	7.5000	17.0900	8.2875	6.7500
45	8.5000	20.9600	9.3925	7.6500
60	8.8000	22.9100	9.7240	7.9200
75	9.3300	29.9900	10.3097	8.3970
90	10.7000	38.1500	11.8235	9.6300
Average time	8.11	22.36	8.96	7.29
Throughput	8.41	2.36	7.61	9.35

Table 8.4 Comparative Study of KDDEDA with DES, AES and Blowfish

Table 8.4 represents the different size of the text files and corresponding encryption execution time taken by AES, DES, BLOWFISH and KDDEDA algorithms in seconds for the windows operating system.

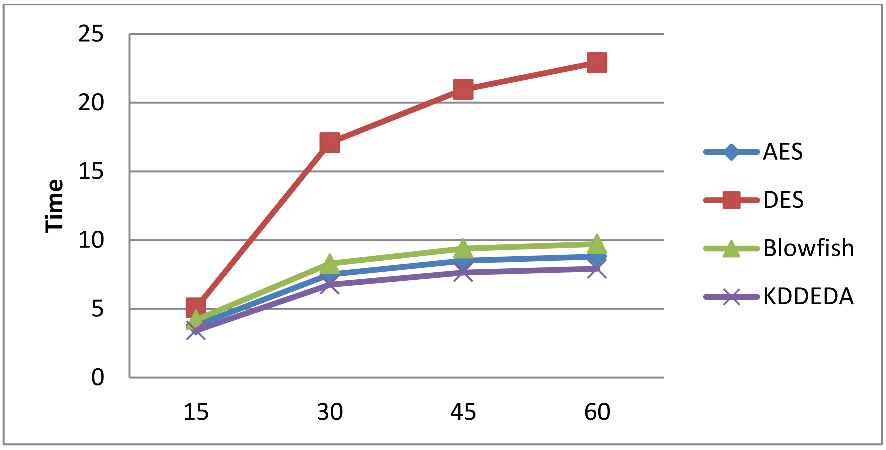

Figure 8.4.1 Encryption Time of Different Data Size in Windows Operating System

The result reveals that the encryption time taken by KDDEDA is very short as compared to other three. The figure (8.4.1) shows the encryption time taken by AES, DES, BLOWFISH and KDDEDA for different size text files for the windows operating System.

Input size(KB)	AES	DES	Blowfish	KDDEDA
15	3.08	5.01	3.40	2.414
30	5.70	15.09	6.30	4.473
45	8.60	17.44	9.50	6.745
60	8.99	25.88	9.93	7.7603
75	9.29	30.44	10.27	8.0017
90	10.01	37.13	11.06	8.5626
Average time	7.11	21.83	8.41	6.32
Throughput	8.99	2.42	8.14	9.99

Figure 8.4.1 represents the different size of the text files and corresponding encryption execution time taken by AES, DES, BLOWFISH and KDDEDA algorithms in second for the Linux operating system. The result reveals that the encryption time taken by KDDEDA is very short as compared to other three. The (figure 8.4.2) shows the encryption time taken by AES, DES, BLOWFISH and KDDEDA for different size text files for the Linux operating System.

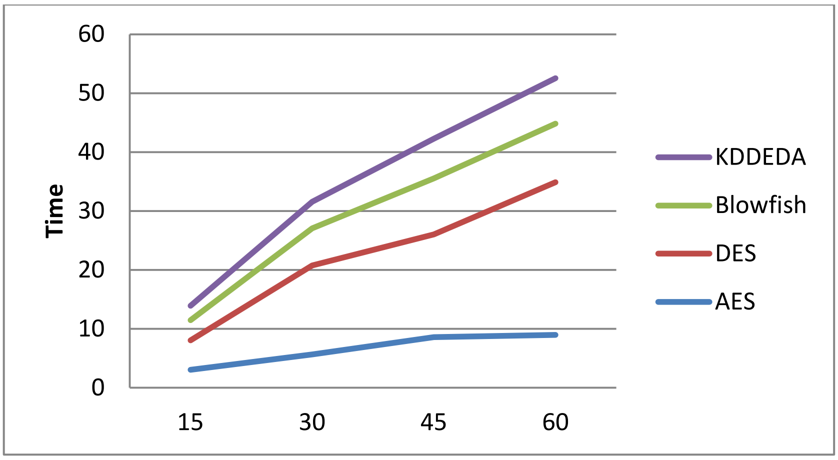

Figure 8.4.2 Encryption Time of Different Data Size in Linux Operating System

Encryption algorithms	Encryption throughput for windows	Encryption throughput for Linux
AES	8.41	8.99
DES	2.36	2.42
Blowfish	7.61	8.14
KDDEDA	9.35	9.99

Figure 8.4.3 show the encryption throughput of the AES, DES, BLOWFISH and KDDEDA four platforms. The throughput also explained that the encryption speed of AES and KDDEDA is high compared to other three algorithms. (Figure 5.3) show the comparative results.

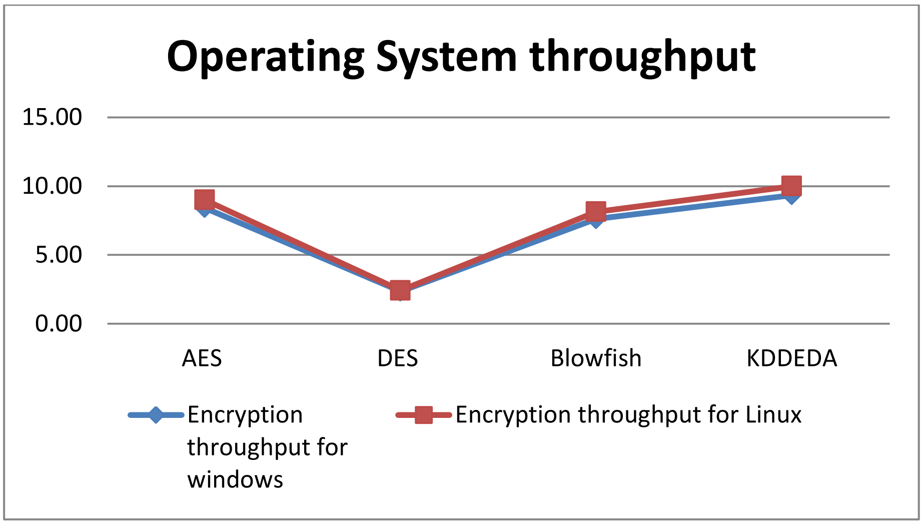

Figure 8.4.3 Encryption Time of Different Data Size in Linux Operating System

Encryption algorithms	CPU usage in	CPU usage in

	windows	in Linux
AES	2.30%	2%
DES	2%	1.90%
Blowfish	2.55%	2.10%
KDDEDA	2.80%	2.05%

Figure 8.4.4 show the CPU usage of the AES, DES, BLOWFISH and KDDEDA four platforms. The use of CPU for AES, Blowfish and KDDED is similar. But in Linux operating system KDDEDA is less compare to all others.

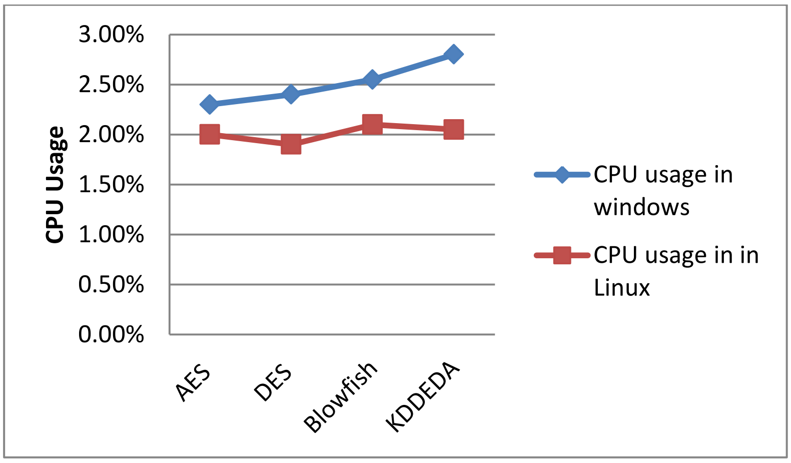

Figure 8.4.4 Comparative of CPU usages

9. Conclusion

Cryptography algorithms play a very important role in communication security. Our research evaluates the performance of the four symmetric key encryption algorithms AES, DES, BLOWFISH and KDDEDA.Key Developer Data Encryption and Decryption Algorithm(KDDEDA) is new developed symmetric encryption algorithm for improve the encryption performances and throughput. The performance measure of encryption algorithm is conducted in terms of processing time, CPU usage and encryption throughput on windows and Linux platform for a different text size. The simulation results conclude that KDDEDA is faster than AES, DES and BLOWFISH in the execution time for the four platforms. KDDEDA has high throughput than AES, DES and BLOWFISH. AES, DES and BLOWFISH consume less CPU usage than KDDEDA for two platforms. Our further research will focus on comparing and analyzing the existing other cryptographic algorithms. It will include experiments on image data will focus on improving encryption time of KDDEDA.

10. Reference

[1] A.Subramani and A.Usha,Analyse The Encryption And Decryption Conversion Time Of Various Algorithms On Different Setting Of Dataset. I-manager's Journal on Information Technology. Vol. 5 l No. 3 l June – August 2016.

[2] Srinivas B.L, Anish Shanbhag and Austin Solomon D'Souza."A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm". International Journal of Innovative Research in Computer and Communication Engineering.Vol.2, Special Issue 5, October2014.

[3] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar. "Comparative Analysis between DES and RSA Algorithm's". International Journal Of Advanced Research In Computer Science And Software Engineering. Volume 2, Issue 7, July 2012.

[4] Swati Kashyap, Er.Neeraj Madan."A Review On: Network Security And Cryptographic Algorithm".International Journal Of Advanced Research In Computer Science And Software Engineering.Volume 5, Issue 4, April 2015.

[5] Milind Mathur And Ayush Kesarwani. "Comparasion Between DES,3DES,RC2,RC6,BLOWFISH And AES". Proceeding Of National Conference Conference On New Horizons In It-NCNHIT 2013.

[6] Nidhi Singhal1, J.P.S.Raina2. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization" International Journal of Computer Trends and Technology- July to Aug Issue 2011. ISSN: 2231-280.

[7] Shailja Kumari, Jyoti Chawla " Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security". International Journal of Innovations & Advancement in Computer Science. Volume 4, Special Issue May 2015.

[8] Priteshkumar Prajapati, Nehal Patel, Robinson Macwan, Nisarg Kachhiya and Parth Shah." Comparative Analysis of DES, AES, RSA Encryption Algorithms".International Journal of Engineering and Management Research.Volume-4, Issue-1, February-2014, ISSN No.: 2250-0758.

[9] Kalyani P. Karule , Neha V. Nagrale .” Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security” International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-2, February 2016.

[10] Youssouf Mahamat koukou, Siti Hajar Othman, Maheyzah MD Siraj. Herve Nkiama. “ Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm”. IOSR Journal of Engineering (IOSRJEN)- Vol. 06, Issue 06 (June. 2016),

[11] Harsh Kumar Verma and Ravindra Kumar Singh.” Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms” International Journal of Computer Applications (0975 – Volume 42– No.16, March 2012 8887)-

[12] Ms. Pallavi H.Dixit , Dr.Uttam L. Bombale , Mr. Vinayak B.Patil. “Comparative Implementation of Cryptographic Algorithms on ARM Platform” International Journal of Innovative Research in Science, Engineering and Technology-Vol. 2, Issue 10, October 2013.

[13] Jawahar Thakur, Nagesh Kumar. “DES, AES and Blowfish:Symmetric key cryptography algorithms simulation based performance analysis”. International Journal of Emerging Technology and Advanced Engineering-Volume 1, Issue 2, December 2011.

[14] Shaza D. Rihan, Ahmed Khalid and Saife Eldin F. Osman.” A Performance Comparison of EncryptionAlgorithms AES and DES” International Journal of Engineering Research & Technology (IJERT)- Vol. 4 Issue 12, December-2015.

[15] Simar Preet Singh, and Raman Maini.” Comparison Of Data Encryption Algorithms” International Journal of Computer Science and Communication-Vol. 2, No. 1, January-June 2011, pp. 125-127.

[16] Pratap Chandra Mandal.” Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish” Journal of Global Research in Computer Science-Volume 3, No. 8, August 2012.

[17] Ranjeet Masram, Vivek Shahare, Jibi Abraham And Rajni Moona.” Analysis And Comparison Of Symmetric Key Cryptographic Algorithms Based On Various File Features” International Journal Of Network Security & Its Applications (Ijnsa), Vol.6, No.4, July 2014.

DOI: 10.18535/ijecs/v5i12.62

[18] Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 2nd Edition, Tata McGraw Hill, 2012.

Author Bibliography

A. Usha is currently doing M.Phil. Computer Science at Government Arts College, Dharmapuri and as a research scholar in Periyar University, Salem. She received her M.Sc. (CS) degree from Periyar University; Salem. She completed her UG degree at Government Arts College, Dharmapuri. Her area of research includes Mobile Ad-hoc Networks, Network Security and Data Structures.

A. Subramani is currently working as an Assistant Professor, Department of Computer Science, Govt. Arts College, and Dharmapuri and as a Research Guide in various Universities. He received his Ph.D. Degree in Computer Applications from Anna University, Chennai. He is a Reviewer of 15 National / International Journals. He is in the editorial board of 6 International / National Journals. He is an Associate Editor of Journal of Computer Applications (2010-2015). He has published more than 50 technical papers at various International, National Journals and Conference proceedings. He is a life member of MCSI, MISTE computer society. His areas of research includes High Speed Networks, Routing Algorithm, Soft computing, Wireless Communications, Mobile Ad-hoc Networks and Software Engineering.