Simulation Based Performance Evaluation of Symmetric Key Cryptographic Algorithms: DES, 3DES, AES and Blowfish

Kumari Sarita[1], Jawahar Thakur[2]
[1, 2] Dept of Computer Science
[1, 2] Himachal Pradesh University, Shimla.

Abstract- *Cryptography is the study of secret writing and the art of transforming messages to make them secure and immune to attacks. In this research paper, the symmetric key cryptography algorithms (DES, 3DES, AES and Blowfish) are simulated, evaluates and compare their performance on the basis of small text message size (0 Kb- 20 Kb) and large text message size (20Kb- 50 Kb). The algorithms were simulated and implemented in Java environment jdk 1.8 and NetBeans 8.2 IDE. The comparison parameters of these symmetric key cryptographic algorithms are encryption/decryption time, CPU process time, memory usage and total execution time. Simulated and evaluated results shows that the blowfish algorithm performed better with the above listed comparison parameters.*

Keywords- Cryptography, Symmetric key: DES, 3DES, AES, BLOWFISH, Encryption, Decryption.

I. INTRODUCTION

Cryptography is the field of network security which provides methods or algorithms to secure the information by hiding its meaning. It means that cryptography can convert the information from its readable form to unreadable form and vice-versa [1]. There are various types of cryptography algorithms:

1) Symmetric Key Cryptography Algorithms
2) Asymmetric Key Cryptography Algorithms
3) Hashing

Mode of operation

A mode of operation is a technique that employee the modern block ciphers such as DES and AES.

Electronic Code Block: is a purely block cipher technique. The plaintext is divided into blocks of N bits. The cipher text is made of blocks of N bits. The value of N depends on the type of cipher used.

Cipher Block chaining: when a block is completely enciphered, the block is sent, but a copy of it is kept in a register to be used in the encryption of the next block. There is no ciphertext block before the first block. In this case a phony block called the initiation vector (IV) is used.

Cipher Feedback: was created for those situations in which user need to send and receive *r* bits of data, where *r* is a number different from the underlying block size of the encryption cipher used. The value of *r* can be 1, 4, 8 and any number of bits. Since all ciphers work on a block of the data at a time. The cipher encrypt a block of bits and use only the first *r* bits as a new key to encrypt the *r* bits of user data.

Output Feedback: is very similar to the CFB mode with one difference. Each bit in the cipher text is independent of the previous bit or bits. This avoids error propagations. If an error occurs in transmission it does not affect the future bits [6].

Symmetric-Key Algorithms

Symmetric key algorithm uses the same key for encryption and decryption. Symmetric key Algorithms include DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard) and Blowfish.

Data Encryption Standard: The DES (Data Encryption Standard) is type of block cipher symmetric key algorithm. DES was designed by IBM and adopted by the U. S. government as the standard encryption method for nonmilitary and non classified use. At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. DES has two transposition blocks (P-box) and 16 complex round ciphers (they are repeated). Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key [5].

The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64- bit input and permutes them according to predefined values. Each round of DES is a complex round cipher.

DES Function: The heart of the DES is the DES function. The DES function applies a 48- bit key to the rightmost 32 bits R_i to produce a 32-bit output. This function is made up of four operations: an XOR, an expansion permutation, a group of S-boxes and a straight permutation.

Triple Data Encryption Standard (3DES): This algorithm has been designed to replace DES algorithm. Critics of DES contend that the key is too short. To lengthen the key, Triple DES or 3DES has been proposed and implemented.

This uses three DES blocks. The encrypting block uses an encryption-decryption-encryption combination of DESs, while the decryption block uses a decryption-encryption-decryption combination. Two different versions of 3DES are in use: 3DES with two keys and 3DES with three keys. To make the key size 112 bits and at the same time protect DES from attacks such as the man-in-the-middle attack, 3DES with two keys was designed. In this version the first and the third keys are the same ($Key_1 = Key_3$). This has the advantage in that a text encrypted by a single DES block can be decrypted by the new 3DES. It uses 3 rounds of encryption instead of one and uses 16 iterations within each round [1].

Advanced Encryption Standard (AES): Advanced Encryption Standard is a symmetric- key block cipher. AES is a non-Feistel cipher. It was designed because DES's key was too small. Although Triple DES (3DES) increased the key size, the process was too slow. The National Institute of Standards and Technology (NIST) chose the Rijndael algorithm, named after its two Belgian inventors, Vincent Rijmen and Joan Daemen, as the basis of AES. AES is a very complex round ciphers. AES is designed with three key sizes: 128, 192, 256 bits. AES encrypts data with block size of 128-bits. It uses 10, 12, or 14 rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits. The block size, rounds and key size are shown in table 1.1 [6].

Table 1.1: AES Configuration

Size of Block Data	Number of Rounds	Key Size
128 bits	10	128 bits
	12	192 bits
	14	256 bits

Blowfish: Blowfish was developed by Bruce Schneier in 1993. The block size is 64 and the key size between 32 bits (4 bytes) and 448 bits (56 bytes). The advantage of this algorithm is that it is highly secure and has not been cracked yet. It is suitable and efficient for hardware implementation.

The algorithm has two parts – Key Expansion and Data encryption. The key expansion step converts 448 bit key into 4168 bytes. A P array of size 18 and 4 S-boxes whose size is 256 each of which are initialized to hexadecimal digits of pie. XOR each entry in P array and S boxes with 32 bits of the key. There are total 16 rounds of data encryption, in each round a 32 bit subkey is XORed with left most of 32 bits of plaintext and the result is passed to the F function of Blowfish [5].

The key of the blowfish algorithm is 448 bits, so it requires 2^{448} combinations to examine all keys. The advantage of blowfish algorithm is that it is simple to implement since all operations carried out are XOR and addition [6].

In this paper, the symmetric key cryptography algorithms (DES, 3DES, AES and Blowfish) are simulated, evaluates and compare their performance on the basis of small text message size (0 Kb- 20 Kb) and large text message size (20Kb- 50 Kb). The comparison parameters of these symmetric key cryptographic algorithms are encryption/decryption time, CPU process time, memory usage and total execution time.

This paper is organized as follows: Section II gives a brief idea of all the concerned research papers. Section III described the performance of symmetric key cryptography algorithms: DES, 3DES, AES and Blowfish. Section IV will give the conclusion.

II. LITERATURE SURVEY

Thakur et al. [1] discussed a fair comparison between three most common symmetric key cryptography algorithms: DES, AES and Blowfish. The main concern was the performance of the algorithms under different settings, the presented comparisons takes into consideration the behavior and performance of the algorithms when different data loads are used. The comparison was made on the basis of these parameters: speed, block size and key size. Simulation program was implemented using java programming. It was concluded that blowfish has better performance than other common encryption algorithms used.

Agrawal et. al [2] discussed the cryptography and presents a detailed study of symmetric key encryption

techniques with their advantages and limitations over each other. The symmetric key algorithms i.e. DES, 3DES, AES and Blowfish are compared on the basis of Key size, block size, rounds, attacks, algorithm structure and security rate on theoretical basis.

Mandal Pratap Chandra l [3] provided a fair comparison between four most common and easily used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of different parameters: number of rounds, block size, key size, encryption/decryption time, and throughput and power consumption. It was concluded that Blowfish is best algorithm.

Akashdeep Bhardwaj et al. [4] provided a brief overview and comparison of Cryptographic algorithms such as Symmetric key algorithms and hashing algorithms which was used for cloud based applications and services that required data and link encryption. It was analyzed that in Symmetric key algorithms, AES is best for key encryption and MD5 is faster when encoding.

Aarti Devi et al. [7] provided the comparison between three symmetric key cryptographic techniques namely as DES, AES and Blowfish algorithms in terms of time and security by using image simulation. The tool used for the work was Net Beans IDE 7.4. It was observed that Blowfish algorithm took least time for simulation of encryption and decryption.

Shweta Singh [8] surveyed and analyzed the performance of AES, DES and RSA on the basis of packet size, encryption time and decryption time. It was observed that AES algorithm consumes least encryption time and RSA consumes largest encryption time. It was concluded that AES is better algorithm.

Omer K. Jasim et al. [9] provided the various encryption algorithms Symmetric Key Algorithms such as AES, DES, 3DES, Blowfish and Asymmetric Key algorithms like RC4, RSA and Diffi-Hillman. The performance parameter for algorithms was input block data size, which observed that how the change in size of the files took place after encryption was complete. It was concluded that the symmetric key encryption are faster than asymmetric key algorithm.

Odeh Ashraf [10] provided comparison among symmetric key algorithms and Secure Watermark System. DES, AES and Blowfish are symmetric key algorithms. Packet size, CPU time, memory used and power consumption were analyzed in this implementation. The implementation was done on Windows 8, XP and Linux OS.

III. PERFORM ANCE OF SYMMETRIC KEY ALGORITHMS: DES, 3DES, AES and BLOWFISH.

The implementation is done on the available hardware and software configuration of the system. The minimum requirement for experimental setup are windows 2007, 64 bit operating system with 4 GB RAM, processor Intel® Core™ i3-2367M CPU @ 1.40 GHz. The simulation program is compiled using the default settings in jdk 1.8 development kit for Java and Netbeans IDE 8.2. The symmetric key algorithms DES, 3DES, AES and Blowfish are simulated in Java environment. The text message was used as an input and it was categorized into two types as small text message size (0 Kb- 20 Kb) and large text message size (20 Kb- 70 Kb). The Java Cryptography Extension (JCE) and Java Cryptography Architecture (JCA) are used for encryption, decryption, generating key. The symmetric key cryptography algorithm's encryption/decryption time, execution time, memory usage and CPU process time are observed.

1) For small text message (0 Kb-20 Kb)

- **Encryption Time for small text message (0 Kb-20 Kb)**

The cryptographic symmetric key algorithms were simulated on text message of different size and its encryption time was observed. Encryption is the process of converting plaintext into cipher text. The results obtained regarding the encryption time for text message in which the size may be from 0 Kb- 20 Kb. The figure 1 is showing the encryption time as:

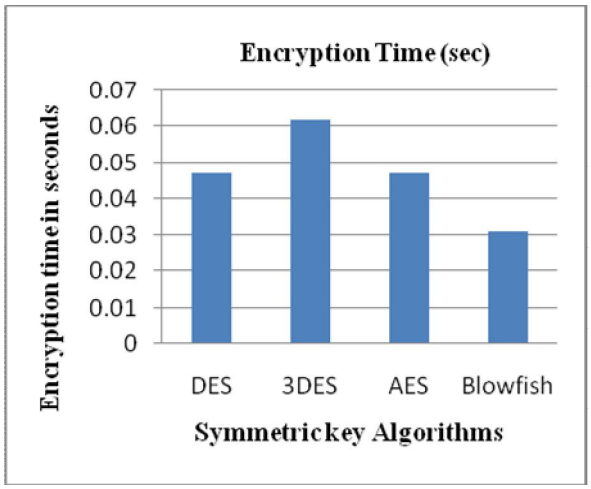

Figure 1: Encryption time for small text message

From figure 1, it is seen that the 3DES takes maximum time to encrypt the text message. While the Blowfish has least encryption time as compared to AES, DES and 3DES for small type of text messages. It is clear from the data obtained that the Blowfish has the good encryption time. AES and DES have approximately same encryption time and they are better than 3DES.

Decryption Time for small text message

The decryption time is the process of converting ciphertext to plaintext which is shown in figure 2 as:

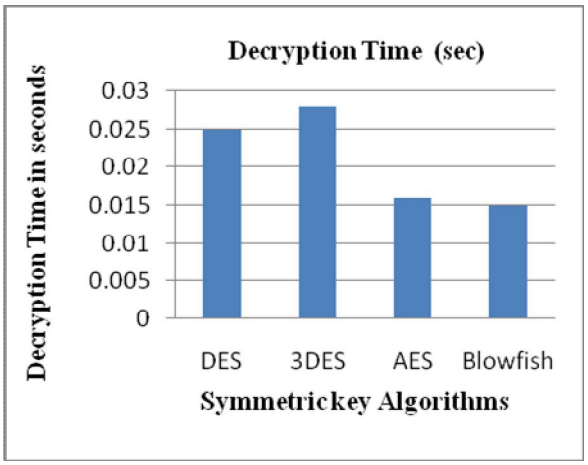

Figure 2: Decryption time for small text message

From figure 2, it is observed that the 3DES takes maximum time to decrypt the text message. DES also takes more time for decryption. Blowfish has least decryption time as compared to AES, DES and 3DES for small type of text messages. It is clear from the data obtained that the message is decrypted very quickly through Blowfish as compared to other algorithms.

Execution Time for algorithms

Execution time or run time is the time during which a algorithm is running. It has three cycles such as compile time, link time and load time.

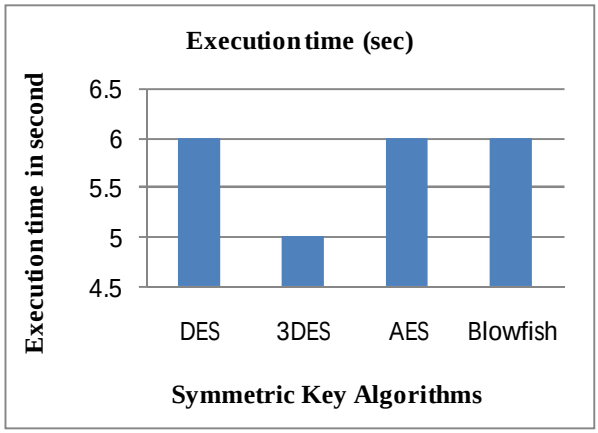

Figure 3: Execution time for Algorithms

From figure 3, it is observed that the execution time of the 3DES algorithms has least time for small text message as compared to DES, AES and Blowfish algorithm. In this simulation setup the execution time was measured in seconds.

Memory Usage

Symmetric key cryptography algorithms: DES, 3DES, AES and Blowfish required memory for their execution. Memory usage class is constructed by methods that are used to obtain memory usage information about individual memory pool of the java virtual machine. The maximum utilized size of memory is used to calculate the total number of Bytes. Figure 4 shows the memory usage by algorithms in MB..

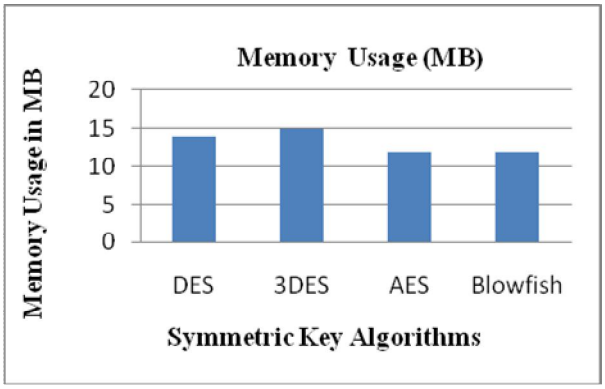

Figure 4: Memory usage for small text message

From figure 4, it is concluded that the memory used by the Blowfish and AES algorithms were approximately similar in size. 3DES consume large memory size as compared to DES, AES and Blowfish. The memory size was calculated in Megabyte (MB).

CPU Process Time

The CPU process time is the amount of time for which a central processing unit (CPU) was used for processing instructions of a computer program or operating system. CPU process time is calculated in the milliseconds to show the CPU utilization by the processes. Figure 5 is showing the results as:

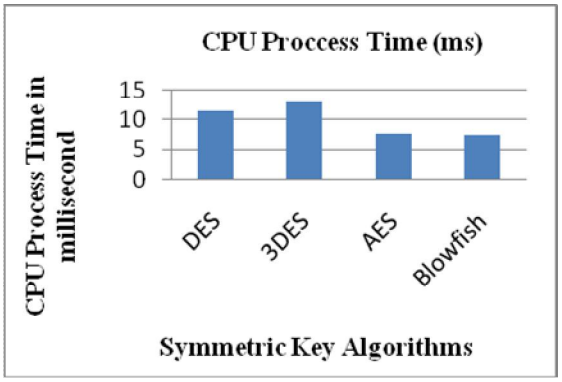

Figure 5: CPU Process time for small text message

From figure 5, it is depicted that the CPU process time of AES and Blowfish are very fast.3DES has highest CPU processing time. Blowfish and AES are better than DES and 3DES in case of CPU process time.

For large type of text messages (20 Kb-70 Kb)

The analysis of the symmetric key algorithms is obtained by providing the different size of text messages as an input on the simulation setup. The maximum size for large text message is 70 Kb. And the minimum size is 20 Kb. For large text message size, the symmetric key cryptography algorithm: DES, 3DES, AES and Blowfish was simulated in java programming language. The various parameters such as encryption/decryption time, execution time, memory usage and CPU process time are used in simulation setup by symmetric key algorithms.

Encryption Time for large text messages

For large text messages, the encryption time is calculated on the same simulation setup. A bulk of data was entered in an input prompt box for encryption of message. Figure 6 is showing encryption time as:

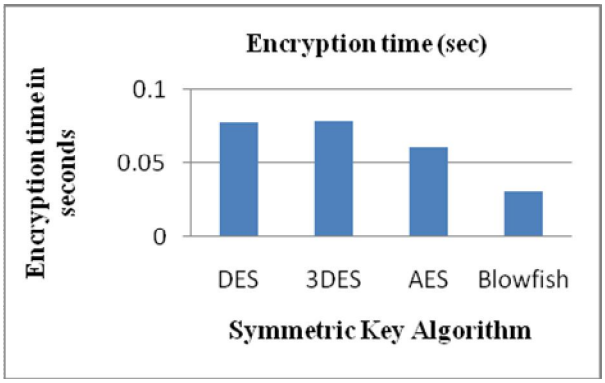

Figure 6: Encryption time for large text message

From figure 6, it is seen that for large text message the 3DES takes the maximum time to encrypt the message. DES has second high encryption time. While the Blowfish has least encryption time as compared to AES, DES and 3DES for large type of text messages. It is clear from the data obtained that the Blowfish has the good encryption time and AES is better than DES, 3DES.

Decryption Time for large text message

Decryption of message is the process of converting coded text into original form. The decryption time is as shown in following figure 7:

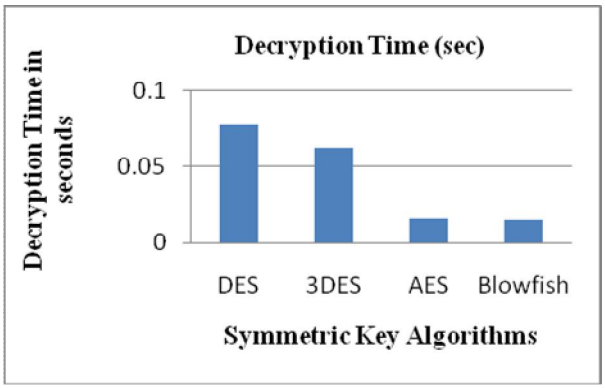

Figure 7: Decryption time for large text message

From figure 7 it is observed that the DES has the maximum decryption time. 3DES has second high decryption time. Blowfish and AES have least decryption time for large type of text messages. It is clear from the data obtained that the message is decrypted very quickly through Blowfish and AES on the standalone machine.

Execution Time for algorithms

This also shows that the large type of message takes long time to execute. The execution process of algorithms is obtained by the figure 8 as shown:

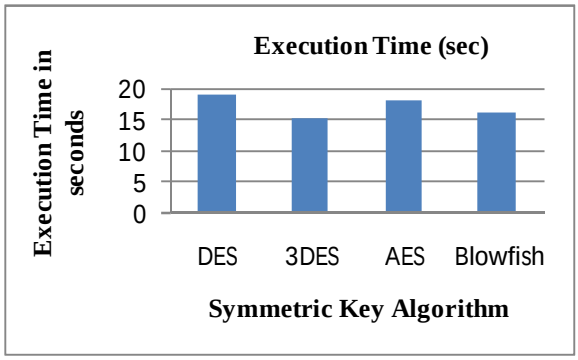

Figure 8: Execution time for Algorithms

From figure 8, it is analyzed that the execution time of the 3DES algorithm is very small while blowfish has second least execution time. DES algorithms have highest execution time for large text messages.

Memory Usage

In Java the memory usage is measured in MB to show the used heap size or memory for the algorithms. The following figure 9 showing the results as:

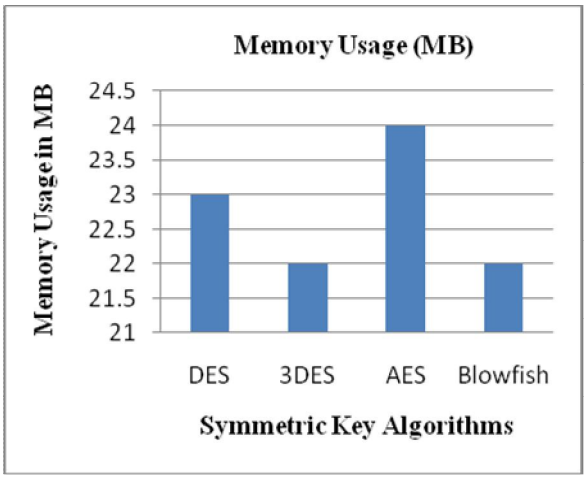

Figure 9: Memory usage for large text messages

From figure 9, it is concluded that the memory used by the Blowfish and 3DES algorithms are approximately similar in size. AES consume large memory size as compared to DES, 3DES and Blowfish. The Blowfish and 3DES consume least memory size.

CPU Process Time

The CPU process time is the amount of time for which a central processing unit (CPU) was used for processing instructions of a computer program or operating system as in figure 5.10

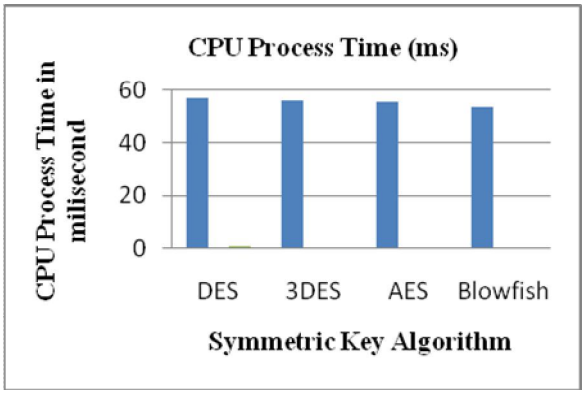

Figure 10: CPU Process time for large text message

From figure 10, it is observed that the CPU process time of Blowfish is very fast. DES has slow CPU processing time. 3DES has more CPU time as compare to AES but less than DES.

After obtaining all the results the analysis shows that the different message size gives different results for symmetric key algorithms i.e. DES, 3DES, AES and Blowfish. When small and large size of messages are entered in the input box then the encryption and decryption time is very fast in case of Blowfish algorithm. Encryption and decryption time for 3DES algorithm is very poor. AES has good encryption/decryption time as compared to DES but less than Blowfish algorithm. Overall, observation of the symmetric key cryptography algorithms shows that the blowfish is better among other algorithms.

IV. CONCLUSION

Cryptography is the study of secret writing and transforming the message into unreadable form. Some cryptographic algorithms are used for hiding the messages. These algorithms are symmetric key algorithms (DES, 3DES, AES), asymmetric key algorithms and hashing. In this research paper, the symmetric key cryptography algorithms (DES, 3DES, AES and Blowfish) are simulated, evaluate and compare the performance on the basis of small text message size (0 Kb- 20 Kb) and large message text (20Kb- 50 Kb). The algorithms were simulated and implemented in Java environment jdk 1.8 and NetBeans 8.2 IDE. The comparison parameters of these symmetric key cryptographic algorithms are encryption/decryption time, CPU process time, memory usage and total execution time. Simulated results show that the blowfish algorithm performed better with the above listed comparison parameters.

REFERENCES

[1] Thakur Jawahar, Kumar Nagesh, "DES, AES and Blowfish Symmetric Key Cryptography algorithm simulation based Performance Analysis", *IJETAE,* vol. 1, Issue 2, DEC. 2011, pp. 6-12.

[2] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", *International Journal of Computer Science and Engineering (IJCSE),* vol. 4, 05 may 2012.

[3] Mandal Chandra Pratap, "Evaluation of Performance of the Symmetric Key Algorithm: DES, 3DES, AES and Blowfish" *Journal of Research in Computer Science,* Volume 3, No. 8, August 2012.

[4] Bhardwaj Akashdeep, Subramanyam GVB, Avasthi Vinay, Sastry Hanumat, "Security Algorithms for Cloud Computing", *International Conference on Modeling and Security"* 2016.

[5] www.google.com//whatiscryptography.com

[6] Forouzan Behrouz A, "Data Communication and Networking", Fourth Edition, 2006, New York: Tata McGraw- Hill.

[7] Devi Aarti, Sharma Ankush, Rangra Anamika, "Performance Analysis of Symmetric Key Algorithms: DES, AES and Blowfish for image encryption and Decryption", *International Journals of Engineering and Computer Science,* Volume 4. Issue 6, June 2015.

[8] Singh Shweta, Sharma Amita, "Security Layer Implementation in EnDeCloudReports Simulator Tool through Modified AES" *International Journal of Engineering Technology Science and Research (IJETSR),* Volume 4, Issue 8, August 2017.

[9] Omer Jasim K, Abbas Safia, M El-Sayed. Horboaty El and Salem Abdel-Badeeh M., "Efficiency of Modern Encryption Algorithm in Cloud Computing", Volume 2, Issue 6, November-December 2013.

[10] Ashraf Odeh, "A Performance Evaluation of Common Encryption Techniques with Secure Watermark System", *International Journal of Network Security and its Applications (IJNSA),* Vol.7, No.3, May 2015.

[11] Mewada Shivlal, Sharivastva Arti, Sharma Pradeep, Gautam S. S. and Purohit N, " Performance Analysis of Encryption Algorithm in Cloud Computing", *International Journal of Computer Sciences and Engineering,* Volume-3, Issue-2.