A Comparative Study among Cryptographic Algorithms: Blowfish, AES and RSA

[1]Wafaa A. N. A. AL-Nbhany, [2]Ammar Zahary
[1]The Arab Academy for Banking and Financial Sciences – Sana'a
Computer Information Systems Department
[2]Faculty of Computer and IT, Sana'a University
Sana'a, Republic of Yemen

Emails: eng_wafaa_alnbhany@yahoo.com, aalzahary@gmail.com

Abstract: *The encryption in the field of information technology contains the conversion of data and files from the known formula to other types of files. Therefore, the original form of files cannot be traced without knowing the key that is used in the encryption process. Different types of encryption algorithms can exist with different properties. The appropriate algorithm can be chosen according to the nature of application, each application suits with a specific algorithm. In this paper, a comparative study was conducted for three types of algorithms AES, RSA, and Blowfish. Many performance metrics were used such as symmetric/asymmetric key, key size in bits, encryption speed, decryption speed and file size to determine the properties of each algorithm. Results show that RSA algorithm is very slow. Blowfish and AES treat the small files very quickly however, if the file is large, speed of algorithms will differ. The symmetric Blowfish algorithm is faster than AES and RSA algorithms. Symmetric algorithms provide higher security and higher speed for encryption and decryption, and asymmetric algorithms provide high security but with more processing time.*

Keywords: *Encryption, Decryption, Symmetric Key, Asymmetric Key, Advanced Encryption Standard (AES), Blowfish.*

1. Introduction

Encryption is the process of converting the message so it can't be read and it is a way to secure the information and data stored in the computer. The need for encryption is to ensure the security of information. With the rapid advances in information technology, the information security becomes important for information storage and transport [1]. Symmetric encryption is a very important type of the encryptions, the same key is used for encryption and decryption, and the key must be saved and kept protected. Asymmetric encryption is a type of encryptions, in which different keys are used for encryption and decryption, it is called a public key encryption, it is a very important method that is used for transmit the keys of encryption and for transmit a security data. Asymmetric encryptions are slow and it is unfeasible to be used to encrypt a large amount of data. The public key is prefer to be long as much as possible to improve the transmission security [2]. A comparison between three algorithms of AES, Blowfish and RSA was done.

2. Cryptographic Algorithm

Cryptographic algorithm is a set of technologies and equations that secure the data and network by enforcement security. Cryptography is the science of extract the appropriate ways that lead to transfer of information in secure way, the only person who can perception the message is the purposed person. The encryption is very important in communication to prevent unauthorized from read the message [5]. The process of converting the cipher text to plaintext is called the decryption process [2]. Two types of security algorithms are used, symmetric and asymmetric algorithms.

2.1 Symmetric key algorithms

The most significant type of encryption is symmetric key algorithms, in which the same key is used in

encryption and decryption. Symmetric key have the advantage of encryption speed and low using of power consumption [3]. Symmetric key algorithms are two types, the stream cipher in which one bit is encrypted at time and the block cipher in which the algorithm treats the block to be encrypted one at time, the block size is dependent on the algorithm [4].

2.1.1 Advanced Encryption Standard (AES)

It is a kind of symmetric key encryption. AES is not feistel cipher. It is uses a block cipher with 128 bits, key bits (128, 192 and 256) and uses Rounds of 10, 12 and 14 [4].

2.1.2 Blowfish algorithm

It is a kind of symmetric key encryption that uses a block cipher and key bits from 32 bits to 448 bits. It uses on block cipher 64 bits. Blowfish uses a different key sizes with 64 bits block. Data encryption process is executed by 16 rounds fiestel network, each round contain P-box and substitution s-box [10].

2.2 Asymmetric Key Algorithms

Asymmetric key algorithm is a type of the algorithms, in which different keys are used for encryption and decryption process, called private and public key, the public key used by a sender to encrypt the message and the privet key used by the receiver to decrypt the message [4].

2.2.1 RSA

The RSA (Rivest-Shamir-Adleman) algorithm is based on a public key algorithm which is known and used on a large scale. It uses a large key bit (should be more than 1024 bits). It is one of asymmetric encryption algorithms used two different keys for encryption and decryption [8].

3. RELATED WORK

Authors in [6] introduced a study for the symmetric encryption algorithms performances, the study included algorithms of AES, Blowfish and assess the encryption algorithms in different environments. It includes the volumes of data, various types of data blocks, speed of encryption and speed of decryption. The results showed that the blowfish require less time than other algorithms and the time consumption is effected by change in the key size. Authors in [7] presented an analysis comparative study between encryption algorithms includes AES and RSA. The study uses the criteria of memory size, consumption time and other criteria. The study showed that the AES least commonly used memory, and the RSA takes the longest time consumption and high memory. Authors in [11] introduced an evaluating study for the encryption algorithms performance, which includes AES and blowfish, the results showed that in term of packet size, the blowfish showed better results than other algorithms. And in term of performance the AES is better than other algorithms. Authors in [12] produced an evaluating study for the performance of encryption algorithms, which includes AES and Blowfish. The results showed that the blowfish is the best performance. Authors in [13], produced a study of various algorithms includes AES, Blowfish. The study showed that in term of throughput performance the Blowfish is the best. Authors in [9], introduced a performance study of encryption algorithms AES and Blowfish. The criteria are time consumption and encryption performance. The study was done on different types of files and images. The study conclusion was reach to that the Blowfish is better performance than AES in all cases. Authors in [14] proposed a study on the performance of encryption algorithms including AES, RSA in cloud computing. The study showed that the RSA the most time consuming and less speed, AES is the higher speed and encryption speed depend on the file size, the lower the file size the more speed of encryption.

4. The Methodology of the Comparative Study

In this paper, data were analysed using Advanced Encryption Package 2015 and Oracle software. Oracle software was used to calculate the count of character in each RSA decryption message. Encryption Package 2015 was used to determine the performance (encryption speed, decryption speed, file size) of each algorithm to make comparison among algorithms (Blowfish, AES) and apply to different types of files such as mp4, pdf, txt, jpg files, and to detect RSA algorithms behaviours on different bits key sizes, size of message and size of output message.

Figures 1, 2 show the diagrams of symmetric and asymmetric algorithms used in this paper.

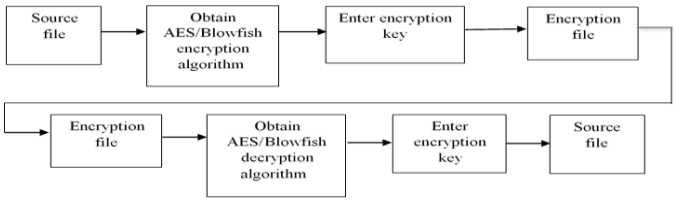

Figure 1: Symmetric algorithms (AES, Blowfish) diagram used in this paper

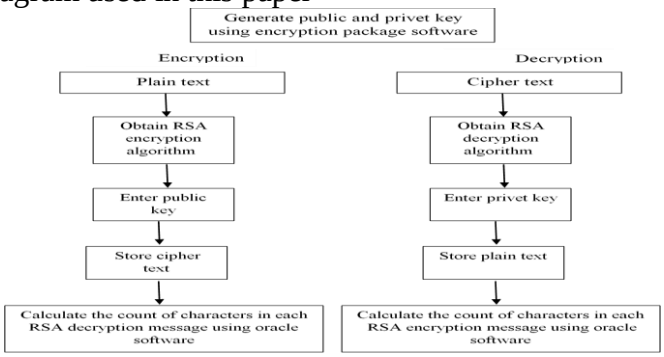

Figure 2: Asymmetric algorithm (RSA) diagram used in this paper

5. RESULTS STUDY AND EVALUATION

This section presents the results and evaluation of the comparative study conducted in this paper for the three cryptographic algorithms namely Blowfish, AES, and RSA. The following performance metrics (algorithm (symmetric or asymmetric), Security, key size in bit, encryption speed, decryption speed) were used. Encryption Package 2015 encryption software was used to determine the performance of (encryption speed, decryption speed, file size) of each algorithm to make comparison among algorithms (Blowfish, AES) and to detect RSA algorithm behavior on different key bit size, size of message and size of output message, oracle software was used to calculate the count of character in each RSA decryption message.

5.1 Blowfish Algorithm

Blowfish algorithm was tested by the following metrics (448 key bits, block size 64 bits, 16 rounds)

Table 1: Results summary of Blowfish encryption and decryption

Blowfish encryption and decryption				
File name with	File size	Encrypted File	Encryption speed	Decryption speed
extension	(kb)	size (kb)	(kb/s)	(kb/s)
1.txt	0.101	0.317	0.101	0.101
4.jpg	4.4	4.6	4.4	4.4
1.jpg	8.13	8.34	8.13	8.13
3.jpg	23.5	23.7	23.5	23.5
2.jpg	68.3	68.6	68.3	68.3
1.pdf	533	533	533	533
3.pdf	892	892	892	892
2.mp4	3250	3250	3250	3250
2.flv	5390	5390	5390	5390
1.flv	6780	6780	6780	6780
3.flv	7650	7650	7650	7650
1.mp4	9100	9100	4550	4550
2.pdf	42800	42800	5350	4750

From the results of Table 1 and Figures 3, 4:

1. The size of encrypted files is bigger than the size of source files for small files, however the size of encrypted files is equal to the size of sources files for large files.
2. The encryption algorithm treats the small files so quickly, the speed of encryption is equal to the file size per second, but if the file is large, the speed of the algorithm will be different.
3. The decryption algorithm treats the small files so quickly, the speed of decryption is equal to the file size per second, but if the file is large, the speed of the algorithm will be different.
4. Speed of encryption is more than speed of decryption.

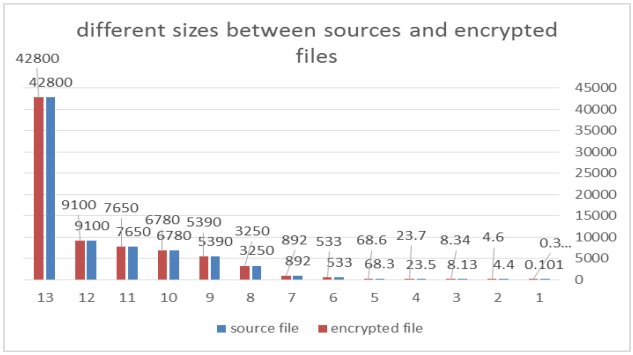

Figure 3: Summary of the different sizes between sources and encrypted files

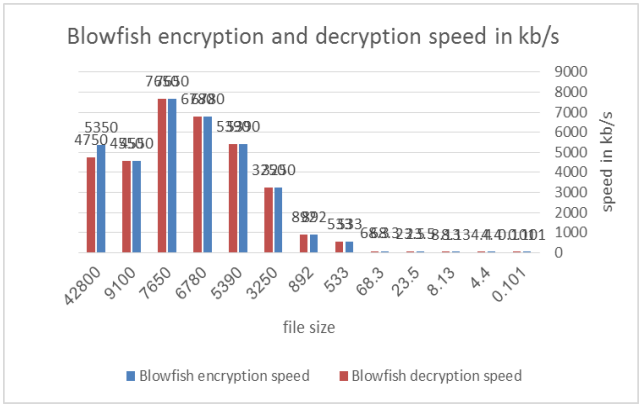

Figure 4: Summary of Blowfish encryption and decryption results

5.2 AES Algorithm

It is a kind of symmetric key encryption. AES algorithm was tested by the following metrics (256 key bits, block cipher with 128 bits, 14 rounds).

Table 2: Results summary of AES encryption and decryption

AES encryption and decryption				
File name with extension	File Size (kb)	Encrypted File size (kb)	Encryption speed (kb/s)	decryption speed (kb/s)
1.txt	0.101	0.317	0.101	0.101
4.jpg	4.4	4.6	4.4	4.4
1.jpg	8.13	8.34	8.13	8.13
3.jpg	23.5	23.7	23.5	23.5
2.jpg	68.3	68.6	68.3	68.3
1.pdf	533	533	533	533
3.pdf	892	892	892	892
2.mp4	3250	3250	3250	3250
2.flv	5390	5390	5390	5390
1.flv	6780	6780	6780	6780
3.flv	7650	7650	7650	3830
1.mp4	9100	9100	4550	4550
2.pdf	42800	42800	4750	4750

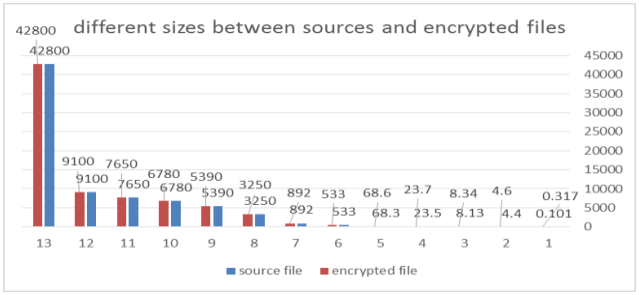

Figure 5: Summary of the different sizes between sources and encrypted files

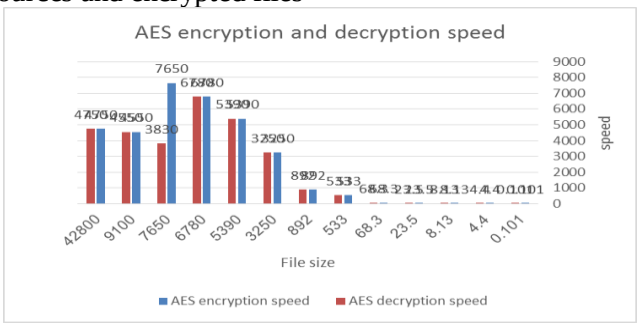

Figure 6: Summary of AES encryption and decryption results

From the results of Table 2 and Figures 5, 6

1. The size of encrypted files is bigger than the size of source files for small files, however the size of encrypted files is equal to the size of sources files for large files.
2. The encryption algorithm treats the small files so quickly, the speed of encryption is equal to the file size per second, but if the file is large, the speed of the algorithm will be different.
3. The decryption algorithm treats the small files so quickly, the speed of decryption is equal to the file size per second, but if the file is large, the speed of the algorithm will be different.
4. The speed of encryption is more than the speed of decryption.

5.3 RSA Algorithm

It is one of asymmetric encryption algorithms. RSA algorithm was tested by the following metrics (512 bits key, 678 bits key, 1024 bits key and 2048 bits key). The results were obtained by Copy the message that generated by RSA encryption, oracle database was used

to calculate a count of characters in each RSA decryption message.

As RSA algorithm is very slow, so small messages sizes (rang from 1 to 20 characters) were used to examine the performance of RSA algorithm with different keys sizes (512, 768, 1024, and 2048).

Generate public and privet key:

At the first generate the public and private key by uses the Encryption Package software.

RSA algorithm encryption:

After the public and private keys were created, the RSA encryption algorithm was performed. The results were obtained by copy the message that generated by RSA encryption. Oracle database was used to know the number of characters in each message.

Oracle database steps:

1. Create a Table.
2. Insert the message that created from RSA encryption algorithm into a Table.
3. Perform a select query to determine the number of characters in each encrypted message. The summary of the results of RSA encryption algorithm will be presented here. The results of Table 3 were obtained by different key bits and different lengths of input. Oracle database was used to calculate the count of characters in each RSA encryption message.

Table 3: Summary of the results of RSA encryption algorithm

Key bit	Length of source message (character)	Length of encrypted message (character)
512	1	516
512	10	532
512	20	532
768	1	557
768	10	581
768	20	581
1024	1	601
1024	10	622
1024	20	622
2048	1	772
2048	10	792
2048	20	797

The summary of the results of RSA decryption algorithm will be presented here. As shown in Table 4, the results of key bit, length of input encryption message and length of output decryption message were obtained.

Table 4: Summary of the results of RSA decryption algorithms

Key bit	Length of encrypted message (character)	Length of decrypted message (character)
512	516	1
512	532	10
512	532	20
768	557	1
768	581	10
768	581	20
1024	601	1
1024	622	10
1024	622	20
2048	772	1
2048	792	10
2048	797	20

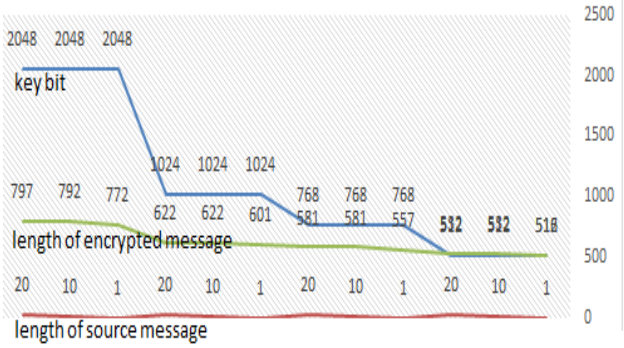

Figure 7: Summary of the results of RSA decryption algorithms

From the results of Tables 4, 5 and Figure 7:

The increase in the key length will increase the length of encrypt message and security.

5.4 Comparison of Encryption Techniques

A comparison between algorithms was done by analysis the results of the comparison algorithms. As RSA algorithm is very slow, so small messages sizes (rang from 1 to 20 characters) were used. The Blowfish and AES algorithms were tested with a different data types such as (text, pdf, mp4, jpg, flv) and sizes (rang from 101 byte to 42.8 Megabyte) to make comparison between algorithms. Table 5 shows the results of encryption algorithms (AES, Blowfish) and Table 6 shows the results of decryption algorithms (AES, Blowfish).

Table 5: Comparison between AES and Blowfish encryption algorithms

AES and Blowfish encryption algorithms			
File name with extension	File Size (kb)	AES encryption speed (kb/s)	Blowfish encryption speed (kb/s)
1.txt	0.101	0.101	0.101
4.jpg	4.4	4.4	4.4
1.jpg	8.13	8.13	8.13
3.jpg	23.5	23.5	23.5
2.jpg	68.3	68.3	68.3
1.pdf	533	533	533
3.pdf	892	892	892
2.mp4	3250	3250	3250
2.flv	5390	5390	5390
1.flv	6780	6780	6780
3.flv	7650	7650	7650
1.mp4	9100	4550	4550
2.pdf	42800	4750	5350

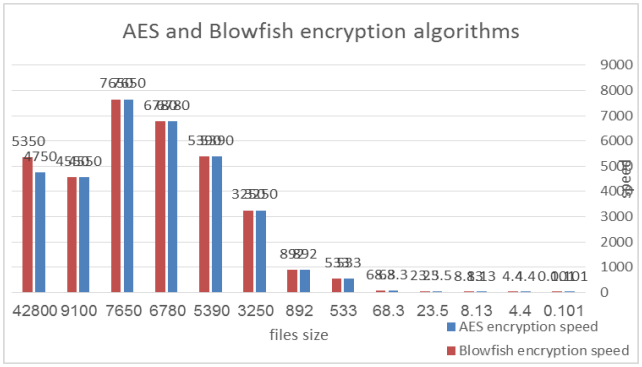

Figure 8: Comparison between AES and Blowfish encryption algorithms

Table 6: Comparison between AES and Blowfish decryption algorithms

AES and Blowfish decryption algorithms			
File name with extension	Encrypted File Size (kb)	AES decryption speed (kb/s)	Blowfish decryption speed (kb/s)
1.txt.aep	0.317	0.101	0.101
4.jpg.aep	4.6	4.4	4.4
1.jpg.aep	8.34	8.13	8.13
3.jpg.aep	23.7	23.5	23.5
2.jpg.aep	68.6	68.3	68.3
1.pdf.aep	533	533	533
3.pdf.aep	892	892	892
2.mp4.aep	3250	3250	3250
2.flv.aep	5390	5390	5390
1.flv.aep	6780	6780	6780
3.flv.aep	7650	3830	7650
1.mp4.aep	9100	4550	4550
2.pdf.aep	42800	4750	4750

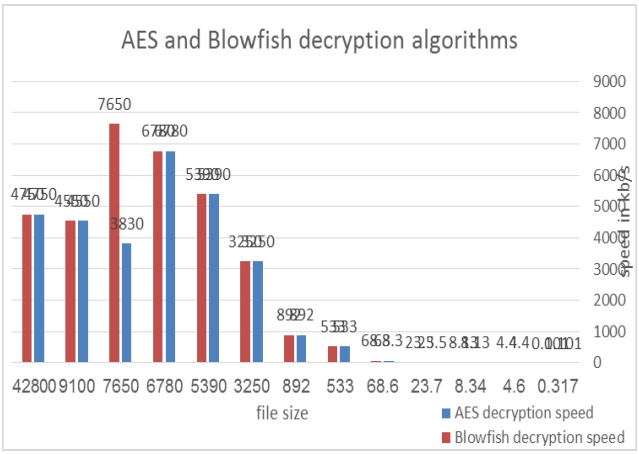

Figure 9: Comparison between AES and Blowfish decryption algorithms

From the results of Tables 5, 6 and Figures 8, 9:

1. The algorithms of AES and Blowfish treat the small files so quickly, the speed of algorithms is equal to the file size per second, but if the file is large, the speed will be different.
2. The size of encrypted files is bigger than the size of source files for small files, however the size of encrypted files is equal to the size of sources files for large files
3. The speed of encryption is more than the speed of decryption in both algorithms of AES and Blowfish.
4. The encryption speed of Blowfish algorithm is more than the speed of AES encryption algorithm.
5. The decryption speed of Blowfish is more than the decryption speed of AES.

6. CONCLUSION

This paper presents a comparative study among different cryptographic algorithms Blowfish, AES and RSA using many metrics such as symmetric or asymmetric key, key size in bits, and encryption and decryption speed. For Blowfish and AES algorithms, results show that the size of encrypted files is bigger than the size of source files for small files, however the size of encrypted files is equal to the size of sources files for large files. It was

clear that Blowfish and AES encryption and decryption algorithms treated the small files very quickly, but if the file is large, the speed will differ. Encryption algorithm is faster than decryption algorithm. In RSA, results show that increasing the key length will increase the length of encrypt message and consequently the security will increase. As a comparison, Blowfish encryption and decryption is faster than AES and RSA because it takes the lowest processing time, and AES algorithm is faster than RSA algorithm in terms of encryption and decryption speed. In addition, symmetric algorithms provide high security with high speed of encryption and decryption, and asymmetric algorithm can provide high security but with more processing time. The future work should be concerned with more studies of algorithms to improve the algorithms properties, encourage of choosing the best algorithm especially for critical application, and perform another study that enhanced on methods that increase the security level of the application.

REFERENCES

[1] Gurpreet Singh and Supriya, "*A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security*", International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, 2013.

[2] AL.Jeeva, Dr.V.Palanisamy and K.Kanagaram, "*Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms*", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3, 2012.

[3] Pinal Salot, "*A Survey Of Various Scheduling Algorithm In Cloud Computing Environment*", International Journal of Research in Engineering and Technology ISSN 2319-1163, 2013.

[4] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "*A Survey of Cryptographic Algorithms for Cloud Computing*", International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, 2013.

[5] N. Islam, M. H. Mia, M. F. I. Chowdhury and M. A. Matin, "*Effect of Security Increment to Symmetric Data Encryption through AES Methodology*", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

[6] Diaa Salama Abdul.Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "*Performance Evaluation of Symmetric Encryption Algorithms*", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, 2008.

[7] Shashi Mehrotra Seth, Rajan ishra, "*Comparative Analysis of Encryption Algorithms for Data Communication*", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, 2011.

[8] Anjula Gupta and Navpreet Kaur Walia, "*Cryptography Algorithms: A Review*", Department of Computer Science, Sri Guru Granth Sahib World University, India, IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939, 2014.

[9] Tingyuan Nie Teng Zhang, "*A study of DES and Blowfish encryption algorithm*", Tencon IEEE Conference, 2009.

[10] J. V. Shanta, "*Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard)*", IJCEM International Journal of Computational Engineering & Managemen, vol. 15, no. 4, pp.43-49, 2012.

[11] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader and Mohiy Mohamed Hadhoud, "*Evaluating the Performance of Symmetric Encryption Algorithms*", International Journal of Network Security, Vol.10, No.3, PP.213, 2010.

[12] Gurjeevan Singh, Ashwani Kumar Singla and K.S. Sandha, "*Through Put Analysis of Various Encryption Algorithms*", IJCST Vol. 2, Issue 3, 2011.

[13] National Conference on Computer Communication & Informatics, "*Performance Analysis of AES and Blowfish Algorithms*", School of computer science, RVS college of arts and science, 2012.

[14] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "*Evaluation and Comparison of Security Issues on Cloud Computing Environment*", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183, 2012.