Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Performance Analysis of Different Cryptography Algorithms

Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz
Computer Science and Engineering Department, Jessore University of Science & Technology, Bangladesh

Abstract*— Data security has been a major concern in the today's information technology era. Especially it becomes serious in the cloud environment because the data is located in different places all over the world. Encryption has come up as a solution and different encryption algorithms play an important role in data security on cloud. Encryption algorithms is used to ensure the security of data in cloud computing. The purpose of securing data is that only concerned and authorized users can access it. In this paper we describes the basic characteristics (Key Length, Block size) of symmetric (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA, Diffie-Hellman, EI-Gamal, Pailier), Hashing (MD5, MD6, SHA, SHA256) algorithms. Also we implemented five well-known and widely used encrypt techniques like AES, DES, BLOWFISH, DES, RC4, RSA algorithms and compared their performance based on the analysis of their encryption and decryption time for different file sizes in the local system.

Keywords*— Cryptography algorithms, Encryption, Decryption. Symmetric key, Asymmetric key, Hashing Algorithms, Key length

I. INTRODUCTION

Cloud Computing is a set of IT Services such as network, storage, hardware, software, resources and these services are provided to a customer over a network. Benefits of cloud storage are easy access means access to your knowledge anyplace, anytime, anyhow, availability, cost efficiency, and high reliability of the data. For these benefits each and every organization is transferring its data to the cloud. For this reason there is a need to protect that data against unauthorized access, alternation or interchanging. Security is considered as one of the most critical feature for cloud computing due to sensitively and importance of data stored on the cloud. Encryption is a well-known technology for protecting sensitive data. Encryption/Decryption process, in modern days is considered combination of three types of algorithms. They are (i) Symmetric-key algorithms where same key used for encrypts and decrypts of data, (ii) Asymmetric-key algorithms where a public key is used by sender to encrypts data and a private key is used by receiver for decryption , and (iii) Hashing. Integrity of data is ensured by hashing algorithms. This paper evaluates five different encryption algorithms namely: AES, DES, RC4, BLOWFISH, RSA, the performance measure of encryption schemes will be conveyed in terms of data types (text or documents), various sizes of the input data on local platform and evaluates their own performance for different input files.

The rest of the paper is organized as follows: Section 2 describes some Cryptography algorithms which are widely used in cloud computing, experimental methodology and environment are given in section 3. In section 4 shows the experimental results and measurements the performance of each algorithms. Section 5 explains the conclusion and future works.

II. CRYPTOGRAPHY ALGORITHMS

Cryptography means "secret writing" which is the science and art of transforming messages to make them secure and immune to attacks by unauthorized user. The original data/message, before being transformed is called cipher text. An encryption is a process to transform the plaintext into cipher text and decryption transforms the cipher text back into plaintext. The sender uses an encryption algorithm and the receiver uses a decryption algorithm. Thus, encryption and decryption help to secure transmission of the message and protect the message from unauthorized users [1].
There are three types of cryptography algorithm that are given below [2] [21]:

- Symmetric key cryptography algorithm
- Asymmetric key cryptography algorithm
- Hashing cryptography

2.1 Symmetric (Secret) Key Cryptography

This cryptographic method uses of two different algorithms for encryption and decryption respectively, and a same key is used both the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt that data [19] [20].
The description of some widely used Symmetric key cryptographic algorithms are given below:

AES

AES (Advanced Encryption Standard) is a symmetric block encryption standard recommended by NIST (National Institute of Standards and Technology) [3] [5] is used for securing information. It uses the same key for both encryption

and decryption. . It has variable key length of 128, 192, or 256 bits; default 256 [4]. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. [14] [7] [10] [11].

DES

DES (Data Encryption Standard) is a symmetric block encryption standard to be recommended by NIST [3]. The DES algorithm is the most broadly used encryption algorithm in the world. The same algorithm and key are used for encryption and decryption, with minor differences. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block [13] [28].

3DES

Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetric-key block cipher standard which is similar to DES method but increase encryption level 3 times than DES [6]. As a result this is slower than other block cipher methods. The block size of 3DES is 64 bit with 192 bits key size [7] [27].

BLOWFISH

Blowfish is a symmetric key cryptographic algorithm that encrypts 64 bit blocks with a variable length key of 128-448 bits. Blowfish is the better than other algorithms in throughput and power consumption [8] [22].

RC4

The RC4 (Rivest Cipher 4) is an encryption algorithm that is a shared key stream cipher algorithm requiring a secure exchange of a shared key [9] [25] [26]. The RC4 encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using 40 and 128-bit keys. To generate the key stream, the cipher makes use of a secret internal state which consists of two parts [6]:

1. A permutation of all 256 possible bytes (denoted "S" below).
2. Two 8-bit index-pointers (denoted "i" and "j").

The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA).

2.2 Asymmetric (public) Key Cryptography

This cryptographic method makes use of two different algorithms for encryption and decryption respectively, a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message by the sender. The receiver decrypts the cipher text with the help of a private key.

The description of some widely used Asymmetric key cryptographic algorithms are given below:

RSA

RSA (Rivest-Shamir-Adleman) is broadly used an asymmetric encryption /decryption algorithm which involves a public key and a private key. The public key can be informed to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. It secured user data assimilate encryption before to storage, user authentication procedures prior to storage or retrieval, and making secure channels for data transmission [4] [29] [30] [24]. 4096 bit key size is used for execution of RSA algorithm.

RSA algorithm involves these steps:

1. Key Generation
2. Encryption
3. Decryption

DIFFIE-HELLMAN

The scheme was first revealed by Whitfield Diffie and Martin Hellman in 1976. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys [6]. It permits two parties that have no prior knowledge of each other to jointly make a shared secret key over an insecure communications channel. This key can then be used to encrypt posterior communications using a symmetric key cipher.

PAILLIER

The Paillier cryptosystem is an asymmetric algorithm. It has homomorphic property permits this scheme to do normal addition operations on several encrypted values and achieving the encrypted sum, the encrypted sum can be decrypted later without even knowing the values ever that made up the sum.

2.3 Hashing Cryptography

Hash functions are a fundamental elementary in the field of cryptography, used widely in a broad spectrum of important applications involving: message integrity and authentication [15] [16], digital signatures [17], secure time stamping, and countless others. A hash function H is an efficiently-computable algorithm that takes as input an arbitrary-length message M and potentially a fixed-length key K (considering a keyed hash function), and makes a fixed-length output D called the message digest.

H (K, M) = D

Here, D = Message Output, K = Fixed Key Length, M = Input Message Length.

The description of some widely used Hashing cryptography algorithms are given below:

MD5

MD5 (Message Digest5) is a broadly used cryptographic hash function with a 128-bit hash value. It processes a variable-size message into a fixed-length output of 128 bits [3]. The input message is divided into chunks of 512-bit

blocks; then the message is padded for making its length divisible by 512[4]. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

MD6

The MD6 Message-Digest Algorithm is a cryptographic hash function. MD6 makes use of a substantially different tree-based mode of operation that allows for greater parallelism [18]. MD6 may be viewed as a tree-like construction, with a 4-to-1 compression function reducing the overall length of the message at each level [23].

SHA

SHA (Secure Hashing Algorithm) is a hashing algorithm. SHA-1 is most extensively used SHA hash function, but very quickly it is going to be replaced by the newer and stronger SHA-2 hash function. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP.SHA1 outputs a 160-bit digest of any sized file or input. SHA-256 algorithm produces an almost-unique, fixed size 256-bit (32-byte) hash [6]. This creates it suitable for password validation, challenge hash authentication, anti-tamper, digital signatures. SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available. SHA-256 hash functions computed with 32-bit words.

Table-1: Characteristics of Cryptography Algorithms

Scheme	Algorithm Type	Contributor	Key Length	Rounds	Block Size
AES	Symmetric	Rijindael	128,192, 256	10 or 12 or 14	128 bits
DES	Symmetric	IBM 75	56-bits	16	64 bits
3DES	Symmetric	IBM 78	168, 112 bits	48	64 bits
BLOWFISH	Symmetric	Bruce Schneier 93	128-448 bits	-	64 bits
RC4	Symmetric	Ronald Rivest 87	40-128-bits	-	-
RSA	Asymmetric	Rivest,Shamir, Adleman 77	1024	1	Minimum 512 bits
DSA	Asymmetric	NIST 91	-	-	-
Diffie-Hellman	Asymmetric	Diffie, Hellman 76	-	-	-
EI-Gamal	Asymmetric	Elgamal 84	-	-	-
Paillier	Asymmetric	Paillier 99	-	-	-
MD5	Hashing	Rivest 91	128	-	512 bit
MD6	Hashing	Prof. Rivest 08	-	-	-
SHA	Hashing	NIST 95	160	-	-
SHA256	Hashing	-	256	-	32 bit

In the table-1 shows a comparative summary between AES, DES, 3DES, BLOWFISH, RC4, RSA, DSA, Diffie-Hellman, EI-Gamal, Paillier, MD5, MD6, SHA and SHA256 is presented in to five factors which are Algorithms, Contributor, Key Length, Rounds and Block Size.

The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits. The key size of AES algorithm is 128, 192, 256 bits. The key size of Blowfish algorithm is 128-448 bits. The key size of RSA algorithm is 1024 bits.

III. EXPERIMENTAL METHODOLOGY & ENVIRONMENT

In this experimental performance analysis of the given algorithms on the basis of the following parameters on local system at different input size. In this section describes the experimental parameters, platforms and key management of experimental algorithms.

a) Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

1. **Encryption Time:** The encryption time considered the time that an encryption algorithm takes to produces a cipher text from a plain text.
2. **Decryption Time:** The decryption time considered the time that a decryption algorithm takes to produces a plain text from a cipher text.

b) Evaluation Platforms

Performance of encryption algorithm is evaluated considering the following system configuration.

1. **Software Speciation:** Experimental evaluation on Eclipse Jee Mars with Java Development Kit 8 Update 65, Matlab version 2014, Windows 8.1 Pro 64 bit Operating System.
2. **Hardware Speciation:** All the algorithms are tested on Intel Core i5 (2.40 GHz) fourth generation processor with 4GB of RAM with 1 TB-HDD.

c) Key Management of algorithms

Key management is the central and more important aspect for security data in cryptosystem. If the key is strong and secure from unauthorized access the cryptography algorithms will more effective able. In our experience we use the key size of AES is 256 bit, Blowfish is 128 bit, DES is 56 bit, RC4 is 64 bit, RSA 1024 bit.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental result for encryption algorithm AES, BLOWFISH, DES, RC4, RSA are shown in table-2 which have been implemented several input file sizes: 329 bytes, 778 bytes and 2048 bytes. Key size of each algorithms that is used in this experiments is also mentioned in the table. All the results are obtained with due care, for achieving higher accuracy hundred (100) samples of total execution time were taken then an average of hundred samples were taken for the measurement and comparative analysis among algorithms and for the graph plotting as well. Encryption and Decryption time is calculated in millisecond and the input size is taken in kilobytes. All the respective observation readings and graph are shown for all the analysed algorithms on single system.

Table-2: Performance Comparison of Different Algorithms

S. No	Algorithm	Key Size (bit)	File Size (bytes)	Average (100 Times) Encryption Time (Millisecond)	Average(100 Times) Decryption Time (Millisecond)
1	AES	256	329	287	293
			778	299	304
			2048	300	297
2	Blow-fish	128	329	293	290
			778	287	278
			2048	283	279
3	DES	56	329	284	280
			778	292	282
			2048	303	317
4	RC4	64	329	282	286
			778	283	280
			2048	313	292
5	RSA	1024	329	462	499
			778	541	450
			2048	488	491

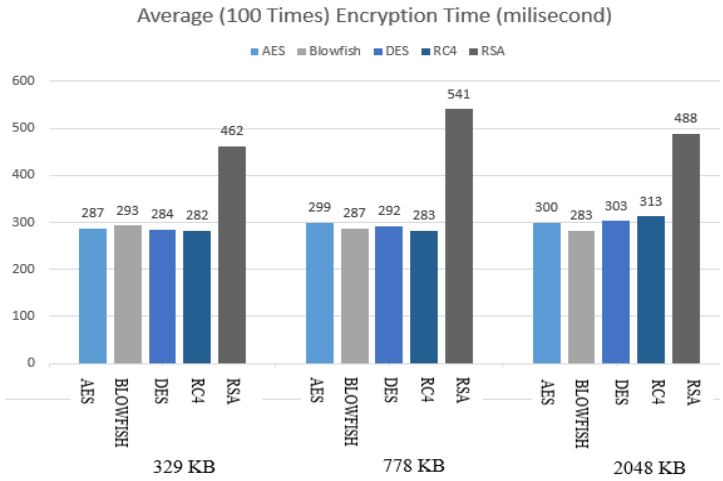

Fig-1: Encryption Time of different Algorithm (Column Based)

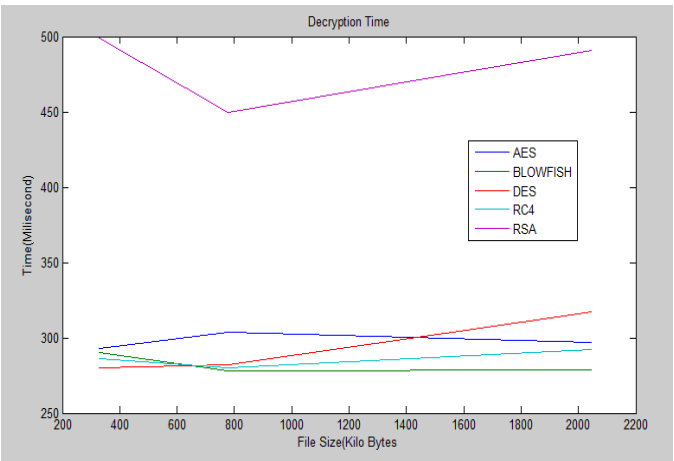

Fig-2: Encryption Time of different Algorithm (Line Based)

In figure-1 and 2 represent the encryption time and figure-3 and 4 also show the decryption time both of symmetric algorithms (AES, BLOFISH, DES and RC4) and asymmetric algorithms (RSA). Generally, from the above figures we can conclude that the symmetric encryption/decryption techniques are faster than the asymmetric encryption/decryption techniques. Moreover, all algorithms in both categories (symmetric and asymmetric) enjoy the proportion relation between the running time and input file size, except the DES and RSA algorithms. The DES and RSA running time changes slightly with input file size increase. By analysing table-2 Time taken by RSA algorithm for both encryption and decryption process is much higher compare to the time taken by AES, BLOWFISH, DES and RC4 algorithms.

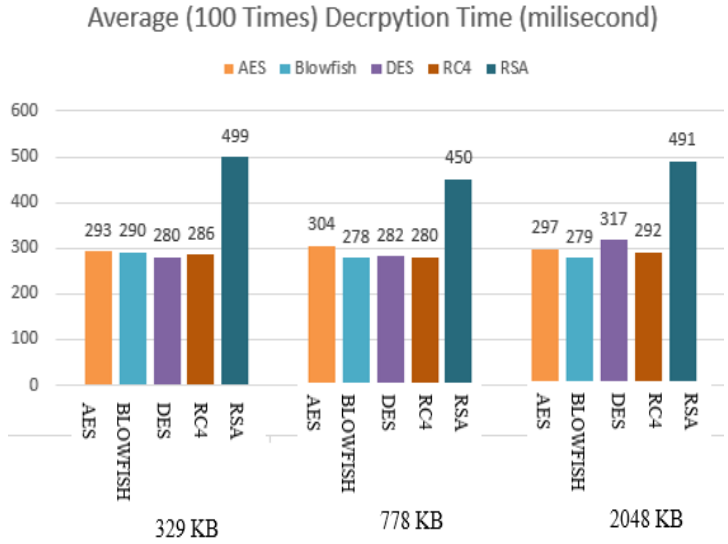

Fig-3: Decryption Time of different Algorithm (Column Based**)**

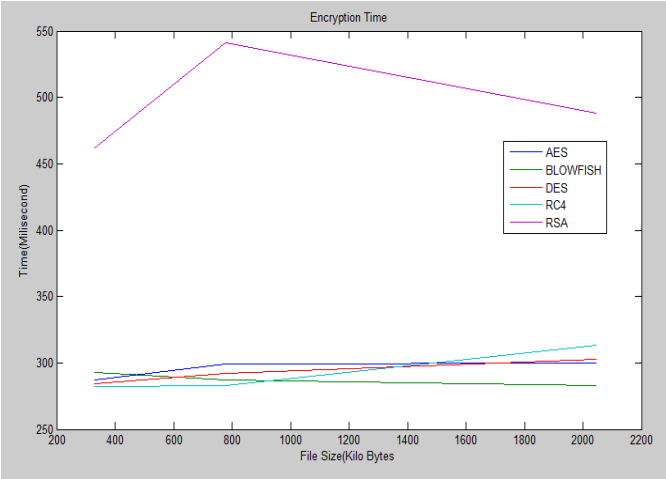

Fig-4: Decryption Time of different Algorithm (Line Based)

V. CONCLUSION AND FUTURE WORKS

Encryption algorithm keeps very important contribution in communication security. Our research work showed the performance of widely used encryption techniques like AES, DES and RSA algorithms. Based on the text files used and the experimental result it was decided that AES algorithm consumes least encryption and RSA consume longest encryption time. We also showed that decryption of AES algorithm is better than other algorithms. From the analytical result, we can say that AES algorithm is much better than DES and RSA algorithm. By taking image and audio data as input next we will compared and analysed existing cryptographic algorithm like AES, DES and RSA and focus will be to improve encryption time and decryption time.

REFERENCES

[1] Mudassar Aslam, Christian Gehrmann, Mats Bj¨orkman, "Security and Trust Preserving VM Migrations in Public Clouds", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 869 - 876, Print ISBN: 978-1-4673-2172-3, DOI: 10.1109 /TrustCom.2012.256.

[2] S C Rachana, Dr. H S Guruprasad, "Emerging Security Issues and Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014, and ISSN: 2319-5967.

[3] Vineet Kumar Singh, Dr. Maitreyee Dutta "ANALYZING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK" International Journal of advanced studies in Computer Science and Engineering IJASCSE Volume 3, Issue 6, 2014.

[4] Priyanka Arora, Arun Singh, Himanshu Tyagi " Evaluation and Comparison of Security Issues on Cloud Computing Environment" in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.

[5] Dr. Prerna Mahajan & Abhishek Sachdeva , "A Study of Encryption Algorithms AES, DES and RSA for Security ", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

[6] https://en.wikipedia.org

[7] Randeep Kaur, Supriya Kinger "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014, ISSN 2319 – 4847.

[8] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[9] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[10] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[11] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[12] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[13] http://www.vocal.com/cryptography/rc4-encryption-algoritm/

[14] Gurpreet Kaur, Manish Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms ", Gurpreet Kaur et al. Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.782-78.

[15] M. Bellare, R. Canetti, and H. Krawczyk. The HMAC Construction. RSA Laboratories CryptoBytes, 2(1):12–15, 1996.

[16] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying Hash Functions for Message Authentication. In Neal Koblitz, editor, CRYPTO, volume 1109 of Lecture Notes in Computer Science, pages 1–15. Springer, 1996.

[17] Mihir Bellare and Phillip Rogaway. The Exact Security of Digital Signatures -How to Sign with RSA and Rabin. In EUROCRYPT, pages 399–416, 1996.

[18] Ronald L. Rivest. The MD6 Hash Function. To be released fall 2008.

[19] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Efficiency of Modern Encryption Algorithms in Cloud Computing", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 6, November – December 2013 ISSN 2278-6856.

[20] Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", Rachna Arora, Anshu Parashar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[21] Shakeeba S.Khan , Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Compute and Communication Engineering, Vol. 3, Issue 1, January 2015.

[22] Manpreet Kaur, Rajbir Singh "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013.

[23] Christopher Yale Crutchfield "Security Proofs for the MD6 Hash Function Mode of Operation", Massachusetts Institute of Technology 2008.

[24] A. Dharini, R.M. Saranya Devi, and I. Chandrasekar, "Data Security for Cloud Computing Using RSA with Magic Square Algorithm", International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 11 No. 2 Nov. 2014, pp. 439-444.

[25] Vijay. G.R, A.Rama Mohan Reddy, "Data Security in Cloud based on Trusted Computing Environment", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[26] Iram Ahmad and Archana Khandekar, "Homomorphic Encryption Method Applied to Cloud Computing", International Journal of Information & Computation Technology.ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530.

[27] Nagesh M.Wankhade, Kiran A. Sahare, Prof. Vaishali G. Bhujade, "SECURE CLOUD SIMULATION USING TRIPLE DES", International Journal of Research in Advent Technology, Volume 2, Issue 1, January 2014.

[28] Prashanti.G, Deepthi.S & Sandhya Rani.K. "A Novel Approach for Data Encryption Standard Algorithm". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249- 8958, Volume-2, Issue-5, June 2013, pp. 264.

[29] Kalpana Parsi, Singaraju Sudha. "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012. pp. 145.

[30] Sunitha K, Prashanth K.S. "Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm". IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5 (Jul. - Aug. 2013). pp. 64.

