# Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing

PradeepSemwal
Research Scholar (CSE),
Uttarakhand Technical University,Dehradun
Uttarakhand, India.
psemwal22@yahoo.co.in

Mahesh Kumar Sharma
Professor,Department of Computer Application
Amrapali Institute of Management& Computer Application ,Haldwani,Uttarakhand,India.
sharmamkhld@gmail.com

***Abstract*-We know that with the emergence of Internetpeople all around the world are using its services &are heavily dependent on it. People are also storing their huge amount of data over the cloud .It is the challenge for researchers to secure the private and critical data of the users,so that unauthorized person should not be able to access it and manipulate it .Cryptography is a process of converting the user useful information to a form which is insignificant to an unauthorized personso that only authorized persons can access and understands it .For ensuring privacy there are multiple cryptographic algorithms, which is selected as per requirement of user or security specification of the organization.This paperdiscusses the comparison of various cryptographic encryption algorithms with respect to its various key features & then later discusses their performancecost based on the some selected keycriteria's. Some of the algorithms chosen for the purpose are DES, 3DES, IDEA,CAST128, AES, Blowfish,RSA,ABE &ECC.**

***Keywords-Cryptography;Symmetrickey Algorithms;Asymmetric Key Algorithms; DES;3DES;AES;Blowfish;IDEA;CAST-128; RSA;ABE;ECC; Encryption & Decryption time ;Memory consumption;Avalanche effect.***

## I. INTRODUCTION

Cryptography is defined as the study of techniques for designing and analyzing algorithms that makes user private information unintelligible to an unauthorized person so that only authorized persons can access and understands it.

The three basic elements in cryptography are Plain text,Encryption/Decryption Algorithm &Cipher text. Plain text in the original data which the sender wants to send over the internet. Encryptionalgorithm converts Plain text into a form which unauthorized users cannot understand it .This form is called as encrypted text or Cipher text. Theencrypted text is converted back to its original form using Decryption algorithm.Theclassification of cryptographic encryption algorithmscan be done in two broader categories mainlySymmetricKey Encryption Algorithms[33][36] and Asymmetric Key Encryption Algorithms[1]. This paper discusses &compares different existing encryptionalgorithms specially in context of data security in the cloud .For comparison various parameters are chosen.

## II. SYMMETRIC KEY ALGORITHMS

Symmetric Key Encryption Algorithms are also called as Secret Key Encryption Algorithms. In Such algorithms the sender & receiver uses same key for encryption & decryption purpose.Importantly the exchange should be very much secure because any one can steal the data in between the transmission. One such most widely used secure key exchange method is Deffie Hellman Key Exchange Algorithm.

Different types of symmetric key encryption algorithms are in use like Data Encryption Standard (DES), Triple Data EncryptionStandard(3DES), Advanced Encryption Standard (AES), IDEAand Blowfish.

### *A. Data Encryption Standard Algorithm*

Data Encryption Standard (DES) is a Symmetrickey algorithm which works on blocks. It was developed at IBM Lab in 1972 by Horst Fiestel and his team. It was published in 1977. It uses key of size 56-bits to encrypt the plain text block of 64 bit size.Since key size is 56 bit so $2^{56}$ i.e. 72,057,594,037,927,936 attempts are required to find correct key. DES uses 19 rounds each round uses a series of S-boxes (Substitution) and P-boxes(Permutation) & XOR operation. DES is not a good algorithm to trust on as it is susceptible to brute force attack and differential cryptanalysis attack. In 1998 it was cracked only in 22 hours by the super computer Deep cracker .

978-15090-6403-8/17/$31.00 © 2017 IEEE

### B. *Triple Data Encryption StandardAlgorithm*

Triple Data Encryption Standard also called as 3-DESor T-DES was introduced by IBM in 1978.It is also is a Symmetric key algorithm which works on blocks.It performs same as like DES algorithm but three times to each data block. It uses block size of 64-bits with a key length of 56bits(total 168 bit).The secret key used can be three or two. T-DES is used in many applications e.g. used in electronic payment and also used by many applications like Microsoft one Note, Microsoft outlook, Microsoft System center configuration manager etc.
Although the algorithm is susceptible to brute force attack and differential attack,but it is comparatively more secure than DES and 2DES.It was mainly designed to make it secure form Men in Middle attack.

### C. *Carlisle Adam &Stafford Tavares [CAST-128]*

CAST-128isalso a Symmetric key algorithm which works on blocks.It was designed in 1996 by **C**arlisle **A**dam &**S**tafford **T**avares .It uses 12-16 rounds.The key size for a block varies from 40-128 bits. Ifthe key size is large than 80 bit then all 16 rounds are used otherwise not .CAST128 algorithm uses S Box,modular addition and subtraction,key dependent rotation & XOR operation.The algorithm increases resistance against both linear &differential attack but 64 bit key version of CAST is susceptible to differential attack.

### D. *International Encryption Algorithm*

In 1991 James Massey &Xuejia Lai proposes another symmetric key encryption algorithm .The algorithm is derived from Proposed Encryption Algorithm (PES). It uses only 8 rounds and each roundusesXOR,addition,multiplication operations. The total number of key used are 52 & the key size varies from 64 bit to 128 bit.IDEA is not yet cracked by any linear or algebraic attack.

### E. *Advanced Encryption Standard Algorithm*

Keeping in mind the vulnerability in DES & 3 DES & because of various reported attacks on these algorithm which revealed their weaknesses,National Institute of Standard and Technology (NIST)decided to develop a new algorithm called Advanced Encryption Standard (AES).There are three version of AES.AES having block size128 bit which uses 10 rounds,AES having 192 bit block size which uses 12 round and AES having block size 256 bit which uses 14 rounds. Each round goes through a series of steps like substitution byte, shift rows, mixed columns and add round Key. AES Algorithm is more secure and has a strong avalanche effect. AES has been used in many applications of PDA communication[9].There are many attacks tried on AES algorithm,one such attack which is acombination of boomerang and rectangle attack[10] withrelated key differentials. This attackwas able to break the round versions of AES but not complete AES. There are some attacks which occurdue to the vulnerability of S-box in AES algorithm. A modified version of AES was introduced to carry out MPEG video encryption [18]. This modified version of algorithm overcomes the calculations and computation overhead.

### F. *Blowfish Encryption Algorithm*

Blowfish Algorithm is one of the most efficient algorithm which is developed by Bruce Schneier in 1993.It is also a block cipher Symmetric algorithm, which uses 64 bits block sizeof plain text. It has a key length varying from 32-448 bit. In its first phase the algorithm uses key expansion where 448 bit key is converted into number of sub keys totaling 4168 bytes [19], which reduces the chance of brute force attack to nil.The second phase is encryption phase, a function is iterated 16 times and the encrypted text is obtained using XOR operation. Blowfish is a strong encryptionalgorithm so it has been used in password management system [21]& bit map plotting [22]. It proved to be a good algorithm on different file size and different key sizes. It is also a lighter algorithm so can be used for encryption in small devices having less memory. The published literature says that four rounds of blowfish are exposed to second order differential attack but entire algorithm is still difficult to crack.

## III. ASYMMETRIC KEY ALGORITHM

In this section we have discussed few efficient& widely used asymmetric algorithms.

Asymmetric Key Algorithms are also called Public Key Encryption Algorithm. It uses two keys ‘Private Key’ and ‘Publickey’. The senderbefore transmission encrypts theplain text with the help of public key toproduce ciphertext and the receiver decrypts this cipher text with the helpof its private key. Various asymmetricalgorithmdiscussedare RSA, CP-ABE,KP-ABE,ECC.

### A.*RivestShamir Adlemen[RSA]*

The algorithm was developed by Rivest, Shamir and Adlemen in1977. The Algorithm uses two keys, Public key used by sender to encryptand private key used by receiver to decrypt the message.The RSAconsists of some mathematical operations

through whichit can calculate the encryption and decryption keys (Eand D), after that one can easily calculate the cipher textand the plain text by the following formula.

$$C = M^{E} \bmod(n) \quad (1)$$

$$P = M^{D} \bmod(n) \quad (2)$$

Where E & D are public and private keys and value of 'n' can be calculated frommathematical operations in RSA .The calculation on positive integer 'n' is based on two pre agreed prime numbers between sender & receiver. Although RSA is a secure algorithm,but prone to private exponent attack [29], so digital signature concept was introduced incombination with RSA [27][28][30], which further strengthen the security of algorithm.

*B. Attribute Based Encryption*

It is another category of Asymmetric Key Encryption Algorithm which was proposed by AmitSahai& Brent Waters. In this algorithm private key & Cipher text are totally dependent upon the attribute of the user. Decryption is only possible only if some set of attribute of user key matches the attribute of Cipher text.It is of two types KP-ABE & CP-ABE.

In KP-ABE (Key Policy –Attribute Based Encryption) users private key are generated based on access tree that defines the privileges of that user ,whereas inCP-ABE (Ciphertext –Policy Based Encryption) uses access trees to encrypt data and users' private keys are generated over a set of attribute of user .CP-ABE is applied as access control method in EHR(Electronic Health Record) system.ABE suffers from the problem of key revocation because multiple users may have same attributes.

*C. Elliptic Curve Cryptography*

In 1985 Victor Miller from IBM &NielKoblitz from University of Washington together proposes another category of Asymmetric Key Encryption Algorithm called as Elliptic Curve Cryptography.ECC uses Elliptical Curve over finite field(not real numbers).It is used in Wireless Adhoc network to generate short key which help in quick encryption & less power consumption. A 160 bit ECC can provide security as of 1024 bit RSA.One of the drawbacks of ECC is that it increases the size of encrypted text as compare to plain text.

*D. Homomorphic Encryption Algorithm*

It is another category of Asymmetric key Algorithm which uses two key public & private. Plain text is converted into a form without losing relation between them.InHomomorphic encryption various mathematical functions are applied for encryption.

## IV. COMPARATIVE ANALYSIS

This section discusses the comparative analysis among different encryption algorithm with respect to various attributes like block size, key size, number of rounds, security level & different vulnerable attacks on them.

*Table-I*shows the comparative analysis betweendifferent symmetric and asymmetric algorithms in tabular form for easy &quick analysis.Comparing with the other algorithms DES is themost insecure algorithm as it has already been declaredinadequate to use.

TABLE-Ishows comparison of various key features of different encryption algorithms

| ***Algo & Yr*** | ***Block Size (Bits)*** | ***Key Len (Bits)*** | ***No Of Rounds*** | ***Security level*** | ***Attacks vulnerable*** |
|---|---|---|---|---|---|
| DES (1977) | 64 | 56 | 16 | Not adequate | Brute force, Differential Attack, Men in Middle attack |
| 3-DES (1978) | 64 | 112-168 | 48 | Vulnerable | Brute force, Differential Attack |
| CAST-128 (1996) | 40-128 | 128 | 12-16 | Vulnerable | 64 bit version is vulnerable to linear attack |
| IDEA (1991) | 64 | 64-128 | 5-8 | Vulnerable | Linear Attack |
| AES (2000) | 128 | 128-256 | 10-14 | Excellent | Side Channel Attack |
| Blowfish (1993) | 64 | 32-448 | 16 | High | Not yet but prone to Key related attacks Boomerang attack |
| RSA (1977) | Not Fixed | >=1024 | Nil | Very High | Brute force & Timing Attack |

Source:-www.serc-org\journal\IJSIA\vol19_no4_2015\27.pdf

## V. IMPLEMENTATION

For the implementation &comparison we have selected only DES,3DES,AES,Blowfish &

RSA.The entireselected encryption algorithms are set in ECB mode.For comparison we have used filesof different sizes like 25 KB,50 KB, 1 MB, 2 MB, 3 MB.The same input files are used for all encryption algorithms.

All the algorithms are implemented & compared using java IDE Eclipse.Various inbuilt packages of java like javasecurity&Javacrypto are used. Performance was measured in Intel core™ i3 processor (32 bit) having 2.4 GHz speed with 4 GB RAM running windows 7 operating system.

## VI. EVALUATION PARAMERTERS

Eachoftheencryption algorithms discussed above have its own strong and weak points. For evaluation of the performance of various encryption algorithms the following metrics have been chosen.

*Encryptiontime,Decryptiontime*
*Avalancheeffect,Memory consumption*

*Fig. 1* shows the results from [42] showing the encryption time of various algorithms.

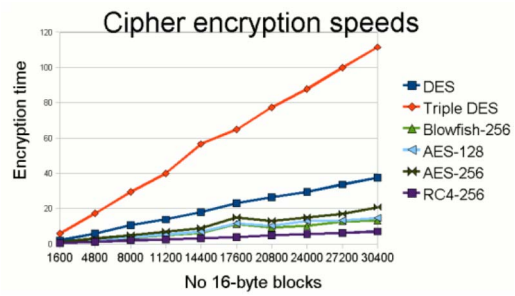


Fig.1Encryption time Vs plain text of different size of various symmetric encryption algorithms

Source:http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue1/Version-3/L017136269.pdf

The results are again verified based on our own test which we have implemented in java & based on few selected evaluation parameters which are discussed in next section.

## VII. RESULTS AND DISCUSSSIONS

This section discusses the observations and the resultsobtainedfrom implementation of the selected encryption algorithms .Results are based on above selected four evaluation parameters. The results are graphically expressed in various figures.

*Fig. 2*reveals that initially AES was consuming more encryption time as compared to other encryption algorithm when size of input file was less but when we try to implement with large size input file, RSAproves to take highest encryption time & Blowfish takes least time for the same input.

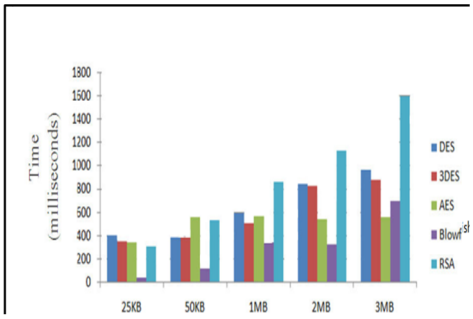


Fig.2 Encryption time Vs. File size for various cryptographic algorithms

*Fig.3* clearly reveals thatRSA proves to takethe highesttimefor decryption,andblowfishtakesleasttimeforthe same input.

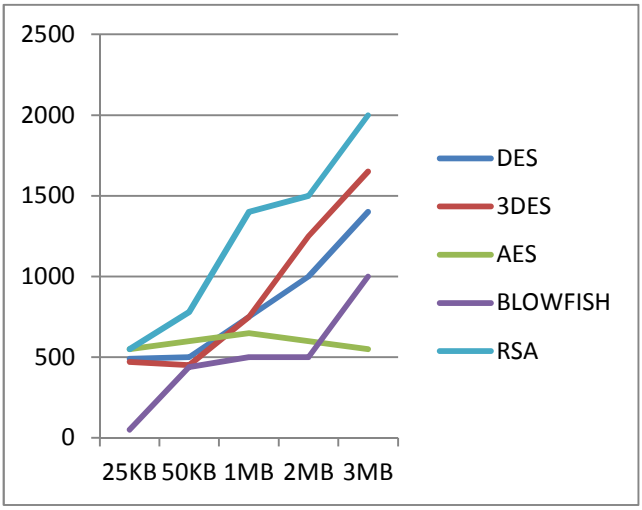


Fig.3Decryption time VsFile size for various cryptographic algorithms

Further our implementation reveals that RSA consumes maximum amount of memory & Blowfish consumes least with respect to unit operation.

TABLE. II. shows the memory used for unit operations for listed Algorithms.

| Algorithm | Memory consumed (KB)/unit operations |
|---|---|
| DES | 18.3 |
| 3DES | 20.6 |
| AES | 14.8 |
| Blowfish | 9.39 |
| RSA | 30.4 |

Another evaluation parameter we selected is the avalanche effect. In cryptography diffusion also tell about the strength of any encryption algorithm. The difference in the input (Plain text) and output(Cipher text) can be observed using avalanche effect ,which is measured using Hamming distance which can be calculated by finding the ASCII value of the characters of plain text and cipher text & then converting them into binary & then taking XOR.The algorithm having more number of one's after XOR operation will be considered having high avalanche effect.

**Hamming Distance= (Binary representation of ASCII value of each character of Plain text) XOR (Binary representation of ASCII value of each character of Cipher text)**

**Avalanche effect= (Hamming Distance / File size)**

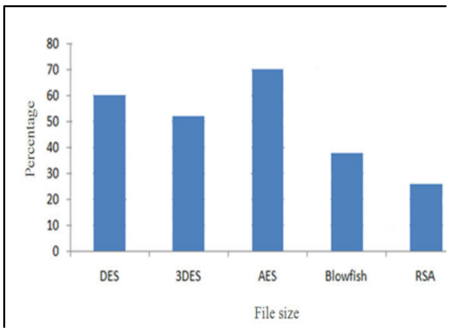


Fig.4 Shows thatAES has highestAvalanche effect whereas RSA showsleast Avalanche effect.

## VIII.CONCLUSION

Each encryption algorithm has its own strengths and weaknesses .From the experiment results shows:

a) Blowfish is best in terms of memory requirement, whereas RSA has a large memory requirement, so blowfish can fit well in small application specially in embedded application & for the devices with small memory.

b) As for encryption&decryption time is concerned RSA consumes maximum time as compare to other cryptographic algorithm whereas blowfish has least.

c) The avalanche effect of AES is high,so AES can be preferred for application where privacy and integrity of the message is of top priority.

## REFERENCES


[1]. T. Bala and Y. Kumar, "Asymmetric Algorithms andSymmetric Algorithms: A Review," InternationalJournal of Computer Applications (ICAET), pp.1-4,2015.

[2]. Patil, Priyadarshini, PrashantNarayankar, Narayan D.G., and Meena S.M.. "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", Procedia Computer Science, 2016.

[3]. W. Y. Zibideh and M. M. Matalgah, "Modified-DESEncryption Algorithm with Improved BERPerformance in Wireless Communication", IEEERadio and Wireless Symposium (RWS) Phoenix,pp.219-222, Jan 2011.

[4]. H.Yoshikawa, M. Kaminaga, A. Shikoda, and T.Suzuki,"Round addition DFA for microcontrollerimplemented the Triple DES", IEEE ConsumerElectronics (GCCE) Tokyo, pp. 538-539, October2013.

[5]. W.Y Zibideh. and M. M. Matalgah , "An OptimizedEncryption Framework based on the Modified-DESAlgorithm: A Trade-Off between Security andThroughput in Wireless Channels",IEEE Radio andWireless Symposium (RWS) CA , pp.419-422, Jan2012.

[6]. . E.Biham and A.Shamir, "Differential Cryptanalysisof the Full 16- Round DES," Proceedings ofCrypto'92,vol. 740, Santa Barbara, CA, December1991.

[7]. P. Kitsos, S. Goudevenos and O. Koufopavlou, "VLSIimplementations of the triple-DES block cipher",IEEE Electronics Circuits and Systems, Vol. 1, pp.76-79, December 2003.

[8]. NIST Special Pubilication 800-20, "Modes ofOperation Validation System for the Triple DataEncryption Algorithm," National Institute ofStandard and Technology, 2000.

[9]. LIU Niansheng , G. Donghui, and H. Jiaxiang, "AESAlgorithm Implemented for PDA SecureCommunication with Java," IEEE Anti-counter.Sec.Ident. Fujian, pp. 217-222, April 2007.

[10]. E.Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks," LectureNotes in Computer Science, vol. 3494, pp. 507-525,Berlin: Springer-Verlag,2005.

[11]. Y. A. Zhang and D.G. Feng, "Equivalent Generationof the S-box of Rijndael," Chinese J. Computers, Vol.27, no.12, pp.1593-1600, December 2004.

[12]. W. Millan, "How to Improve the Nonlinearity ofBijective S-boxes," Lecture Notes in ComputerScience, Vol. 1438,pp.181 - 192, Berlin: Springer-Verlag, 1998.

[13]. Chen and D. G. Feng, "An Evolutionary Algorithmto Improve the Nonlinearity of Self-inverse S-Boxes,"Lecture Notes in Computer Science, vol. 3506, pp.352- 361, Berlin: Springer-Verlag, 2005.

[14]. J. M. Liu, B. D. Wei, and X.G. Cheng,"An AES SBoxto Increase Complexity and CryptographicAnalysis, " IEEE Proc. of the 19th InternationalConference on Advanced Information Networkingand Applications China, Vol. 1, pp. 724-728, March2005.

[15]. Q. X. Zhu, L. li , J. Liu, N. Xu, "The analysis anddesign of accounting information security systembased on AES algorithm," IEEE Machine Learningand Cybernetics Boading , vol. 5, pp. 2713 -2718,July 2009.

[16]. S. Mare, M. Vladutiu and L. Prodan, "Secret datacommunication system using Steganography, AESand RSA," IEEE Design and Technology inElectronic Packaging (SIITME) Timisoara, pp.339-344, October 2011.

[17]. V.Mahalle , A.K Shahade , "Enhancing the DataSecurity in Cloud by Implementing Hybrid(RSA &AES ) Encryption Algorithm," IEEE Power,Automation and Communication (INPAC )Amravati,pp. 146-149,October 2014.

[18]. P. Deshmukh and V. Kolhe, "Modified AES BasedAlgorithm for MPEG Video Encryption," IEEE Information Communication and Embedded Systems(ICICES) Chennai, pp.1-5, Feb 2014.

[19]. J. Bhalla, P. Nagrath , "Nested Digital ImageWatermarking Technique Using Blowfish EncryptionAlgorithm,",ISSN International Journal of Scientificand Research Publications, Vol. 3, pp.1-6,April 2013.

[20]. A.Mousa , "Data Encryption Performance Based onBlowfish," IEEE ELMAR Symposium Zadar, pp.131-134, June 2005.

[21]. M. Wang and Y. Que, "The Design andImplementation of Passwords Management SystemBased on Blowfish Cryptographic Algorithm," IEEEComputer Science-Technology App. IFCSTAChongqing, Vol. 2, pp.24-28, December 2009.

[22]. N.Palaniswamy, D.Dugar M, D.K. Jain, R.Sarabhoje, " Enhanced Blowfish Algorithm usingBitmap Image Pixel Plotting for Security Improvisation," Education Technology and Computer(ICETC) Shanghai, Vol.1, pp.V1-533 - V1-538, June2010.

[23]. National Institute of Standards and Technology, "Clipper Chip Technology," 30 Apr 1993.

[24]. R.Rivest, A.Shamir, and L.Adleman, "A Method ForObtaining Digital Signatures and Public KeyCryptosystems," ACM Transactions onCommunications, Vol. 21, pp. 120-126, 1978.

[25]. T. Nie and T. Zhang "A Study of DES and BlowfishEncryption Algorithm," IEEE TENCON Singapore,pp.1-4, Jan 2009.

[26]. G.N. Krishnamurthy, V. Ramaswamy,G.H. Leela, "Performance Enhancement Of Blowfish Algorithm By Modifying its function," SPRINGER InnovativeAlgorithms and Techniques in Automation IndustrialElectronics Teleco,Netherlands ,pp 241-244, 2007.

[27]. Ying-yu Cao, Chong Fu, "An EfficientImplementation of RSA Digital SignatureAlgorithm," IEEE Wireless CommunicationsNetworking and Mobile Computing (WiCOM )Dalian, pp.1-4, October 2008.

[28]. Hongwei Si, YoulinCai, Zhimei Cheng, "AnImproved RSA Signature Algorithm based onComplex Numeric Operation Function," IEEEChallenges in Environmental Science and ComputerEngineering (CESCE) China, Vol.2, pp.397-400,March 2010.

[29]. Yong-HuiZheng, Yue-Fei Zhu, Hong Xu , "AnApplication of Low Private Exponent Attack onRSA,"IEEE Computer Science &Education( ICCSE), Nanning ,pp.1864-1866, July 2009.

[30]. U.Somani ,K.Lakhani , M.Mundra, "ImplementingDigital Signature with RSA Encryption Algorithm toEnhance the Data Security of Cloud in CloudComputing," ,IEEE Parallel Distributed and GridComputing (PDGC) ,Solan , pp.211-216, October2010.

[31]. LIU Dong-liang, CHEN Yan-ping, Z. Huai-ping,"Secure Applications of RSA System in the ElectronicCommerce," IEEE Future Information Technologyand Management Engineering (FITME) ,Changzhou,Vol. 1, pp.86-89, Oct. 2009.

[32]. Huafei Zhu, "Mercurial Commitments from GeneralRSA Moduli and Their Applications to ZeroknowledgeDatabases/Sets," IEEE Computer Scienceand Engineering WCSE Qingdao, Vol. 2, pp.289-292, Oct. 2009.

[33]. M. Ebrahim, S.Khan and U.B.Khalid, "SymmetricAlgorithm Survey: A Comparative Analysis,"International Journal of Computer Applications, Vol.61,pp.12-19, January 2013.

[34]. A.Nadeem and M. Y. Javed, "A performancecomparison of data encryption algorithms,"Information and Communication Technologies,ICICT 2005, pp.84-89, 2005.

[35]. Singhand and Supriya , "A Study of EncryptionAlgorithms (RSA, DES, 3DES and AES) forInformation Security, " IEEE International Journal ofComputer Applications, vol.67,pp.33-38, April 2013.

[36]. M. Ebrahim, S. Khan and U. Khalid , "SymmetricAlgorithm Survey: A Comparative Analysis,International Journal of Computer Applications,Vol.61, pp. 12-19, January 2013.

[37]. ZoranHercigonja, Drugagimnazija ,Varaždin Croatia , "Comparative Analysis of Cryptographic Algorithms",International Journal of Digital Technology & Economy, Volume 1, Number 2, page 127-134,2016.

[38] Kansal, Shaify, and Meenakshi Mittal. "Performance evaluation of various symmetric encryption algorithms", International Conference on Parallel Distributed and GridComputing, 2014

[39] W. Stallings, Cryptography and Network Security,4th Ed, pp. 58-309, Prentice Hall,2005.

[40]. www.virtru.com/resources/education/encrypting-email-fundamentals

[41]. www.en.wikipedia.org

[42]. www.iosrjournals.org/iosr-jce/papers/Vol17-issue1/Version-3/L017136269.pdf

[43]. www.serc-org\journal\IJSIA\vol19_no4_2015\27.pdf

[44]. www.ijsrp.org/research-paper-1113/ijsrp-p2397.pdf

978-15090-6403-8/17/$31.00 © 2017 IEEE