ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Analysis on Cryptographic Algorithms for Effective Secure Implementation of Cryptosystem in Cloud

[1] S.Rajan, [2]Dr.D.S.Mahendran, [3]Dr.S.John Peter
[1] Assistant Professor and Head, Dept of Computer Science [SF], Kamaraj College (Affiliated to Manonmaniam Sundaranar University, Tirunelveli), Tuticorin, Tamil Nadu, India.
[2] Associate Professor, Dept of Computer Science, Aditanar College (Affiliated to Manonmaniam Sundaranar University, Tirunelveli), Tiruchendur, Tamil Nadu, India
[3] Associate Professor & Head of Research Center, Dept of Computer Science, St.Xavier College (Autonomous and Affiliated to Manonmaniam Sundaranar University, Tirunelveli), Palayamkottai, Tamil Nadu, India.

Abstract: Security plays an important role in all types of computer system from standalone PC to computer system in the cloud. Security can be achieved through cryptographic algorithms. Cryptographic algorithms are categorized as symmetric and asymmetric based on the type of keys used. In pubic Cloud, Data is send through an insecure channel such as internet and stored in a Datacenter which is located far away from the user. So, context effective cryptographic algorithms are needed in the public cloud for transmitting, storing and handling key management. To ensure security, good and context effective cryptographic algorithm should be identified through cryptanalysis. In this paper different cryptographic algorithms are analyzed for efficiency based on computer system used to run algorithm, memory requirement, computational cost and performance.

Index Terms — Cloud, Data, Security, Cryptographic algorithm, transmitting, storing

INTRODUCTION

Cloud is undergoing evolutionary changes in Today's Commuting world. The profitability of cloud depends on the usage of Cloud [11] and Security plays an important role in Cloud. Anything hard earned need to be protected from adversary. In cloud data may be present somewhere near to us or far away by millions of miles. The user may or may not be aware of where the computation is done or data stored in datacenter. Data plays an important role for analysis, strategic planning and decision making so protection of data is the today's necessity. Cloud may be broadly classified as public cloud, private Cloud and hybrid Cloud based on location. As Cost of public cloud is less compared to other Clouds, most enterprises, industries prefer public Cloud. Internet is used as a communication medium in public cloud. Internet is shared by millions of users who may be individuals, government, enterprises etc. As internet is an insecure channel Effective Security mechanism should be architected with cryptosystem so that confidentiality, Integrity, authentication and Non-Repudiation are maintained in our data. The five tuples of cryptosystem are (P, C, K, E, D). Cryptosystem can be formed only if for every k ϵ K ∃ a ek ϵ E and dk ϵ D such that dk (ek (c)) = c ∀ c ϵ P More over dk and ek should have computationally feasible polynomial. Cryptographic algorithm can be broadly classified as Symmetric key and Asymmetric key algorithms based on the type of key used for encryption and decryption. In this paper Algorithms are taken for study based on the literature survey and Effective algorithm is proposed for communication, storage and Key Exchange.

RELATED RESEARCH

Akashdeep Bhardwaj et al. [1], proposed AES and MD5 as best for key Encryption and key Exchange respectively after studying cryptographic algorithms such as AES, 3DES, DES, SHA256, MD5 and RSA. As AES is symmetric key encryption algorithm protecting a single key is a major task for the data owner. Jian-Jang Hwang et al. [2] proposed a model in which cloud service provider is responsible for both data storage and data encryption/decryption tasks. In this model, trusted cloud service provider is overloaded with computational tasks and no control is provided for Data Owner. Prakash et al.[3], proposed a model with Data owner, trusted third party and cloud service provider where computational work load of Cloud Provider is reduced to some extend but involving more number of parties resulted in computational overhead of authentication and decryption in the data user side. In [13] the researcher proposed a novel model for effective key management in Cloud. Dr. C.P.Agrawal et al. [4], analyzed various symmetric and asymmetric algorithms and concluded that blowfish is best in terms of speed and security level. They further

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

added security depends on key management, type of cryptography, number of keys, number of bits used in a key. Shivlal Mewada et al [5] proposed blowfish, AES and DES for performance and AES in terms of security. In [12] Researcher Proposed a MapReduce model to calculate the no of bank accounts linked to the Aadhaar number in a secure manner. Hossain et al. [6], in their paper analyzed Asymmetric\symmetric encryption and decryption algorithms and showed that AES is much better than DES and RSA algorithm. Nasarul Islam.K.V et al [7] proposed homomorphic algorithm as the alternative to AES, DES an RSA while considering security. Pradeep Semwal et al [8], done comparative analysis on different symmetric & asymmetric algorithms and concluded that Blowfish is secure and effective for embedded applications. AES is good if privacy and integrity are top priority. Dr. D.I. George Amalarethinam et al [9], proposed enhanced RSA with two additional prime numbers added to RSA to increase speed and security. S.Rajeswari et al [10] analyzed and showed that both data and storage security should be provided with less overhead in storage and computation.

Based on the literature survey, algorithms such as AES, Blowfish, DES, and 3DES are taken for studying security on transit. RSA is studied for secure data storage. SHA256 and Diffie-Hellman are studied for Key Exchange Algorithm. The performance of algorithm is analyzed based on the configuration of the system which runs algorithm, memory requirement and computational cost.

PROPOSED WORK

The players in the proposed model are Cloud provider: The cloud provider provides Infrastructure, Software, and Platform etc as service. In our Model Cloud Provider is Providing Data Storage.

Trusted Centralized Key Distribution Center: It is responsible for key generation and key Management to store, transmit and Exchange key between the transmitter and receiver. Data User will get the key only after authenticated from Data owner.

Data Owner: Data owners own the Data. The owner of the data will host his data in the Cloud through Cloud Service provider. Some data service will be provided by the Data owner through Cloud Service Provider.

Data user: Data user uses the Data from the Cloud Provider authenticated by Data owner

To give a secure transmission of data between Data user and Cloud Service Provider, the Data user should get authenticated by the Data Owner to get access to data from Cloud Service Provider.

Cryptographic Algorithms needed for storage, transmission and effective key exchange.

Analysis on Cryptographic Algorithms based on structure and Vulnerability AES, Blowfish, DES, 3DES, RSA, SHA256, MD5 and Diffie-Hellman are chosen for analysis based on the priority given by different researchers.

DES: It is a 16-round Feistel Cipher with block size of 64 bit. Encryption is done using 56 bit key. It is widely adopted by NIST. It was originally developed from LUCIFER cipher. The same function which is used for encryption is also used for decryption so there is no need for inverse function during decryption.

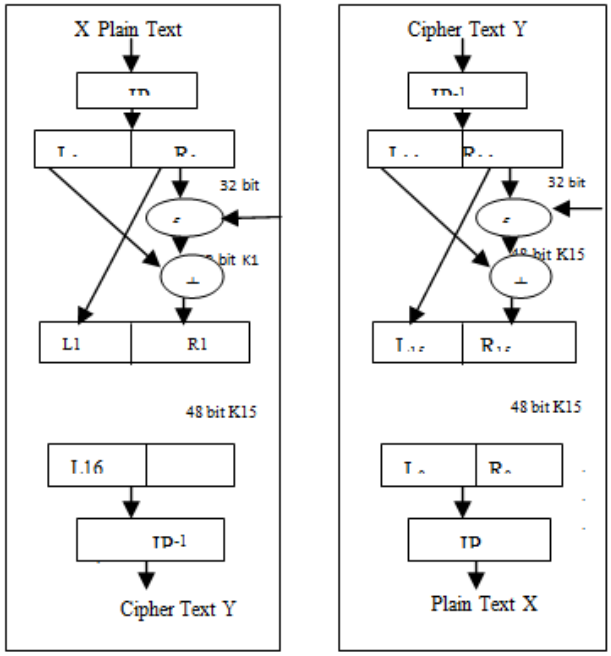


Figure 1: Structure of DES

Cryptanalysis on DES: One of the flaws in DES is there are eight S-Boxes and there is no well formed documentation for S-Boxes. The key size of DES is only

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

56 bit so it suffers from generic attack such as exhaustive search attack, time memory attack etc. It also suffers from non-generic attack such as linear attack, differential attack etc.

3DES: In 3DES, 168 bit key size is split into k1, K2 & k3 and applied to DES to form 3DES. It goes through 48 rounds for encryption and another 48 rounds for decryption. Another Variant of 3DES is 2 key triple DES with 112 bit as key size.

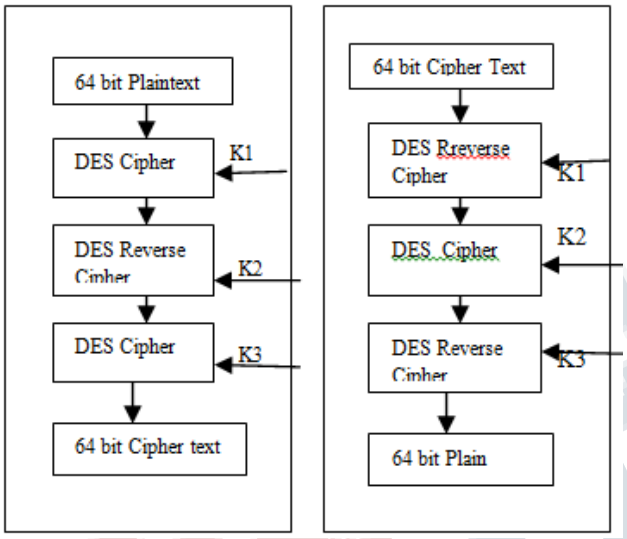


Figure 2: Structure of 3DES

Cryptanalysis on 3DES: It suffers from linear attack and differential attacks which is non-generic in nature.

Blowfish: It was developed by Bruce schneier in 1993. It is a symmetric Block cipher algorithm. It has a key length varying from 44 to 448 bits. It is used in small device [14] as it consumes less memory. It has 16 rounds of iteration.

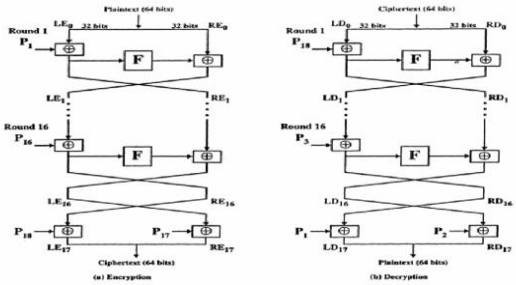


Figure 3: Structure of BlowFish

Cryptanalysis on Blowfish: It may be exposed to non-generic second order differential attack.

AES: AES was initially known by the name Rijndael which was coined from two Belgian cryptographers namely Dr.Joan Daemen and Dr. Vincent Rigmen. It is a 128 bits block cipher with keys 128, 192, 256 and rounds 10,12 and 14 respectively. The block and key can be chosen independently from 128,160,192,224 and 256 bits
.

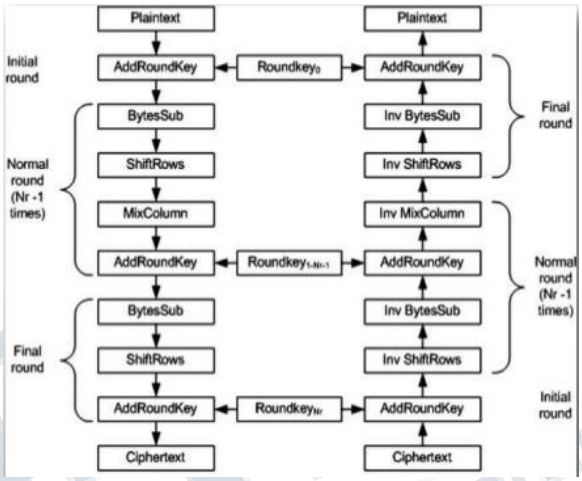


Figure 4: Structure of AES

Cryptanalysis on AES: It is vulnerable to side Channel attack. Few attacks such as boomerang and rectangle attack are also tried on AES and it affected only part of the round version but not the whole AES.

RSA: Its name derived from the developers of RSA namely Ron Rivest, Adi Shamir, and Leonard Adleman. This is an asymmetric crypto system dealing with public key and private key. Public key is used for Encryption and Private Key is used for decryption. By making Factorization hard we can make RSA highly secure.

Let p, q be large prime numbers;
n=p*q; Ø(n)=(p-1)(q-1);
e ⊥Ø(n) gcd (e, Ø(n)) = 1 ;
ed = 1 (mod Ø(n));
d = e-1(mod Ø(n));
K={n, p, q, e, d}

C = me mod n (Encryption where m is a message and C is Cipher Text)

X = Cd mod n (Decryption where X is a Plain Text and C is a Cipher Text

Cryptanalysis on RSA: Brute force attack can be avoided by choosing the large prime number with 768 and 1024 bits for casual use and commercial use respectively. Larger e and d value will yield even better result. It will take 200 years to break 200 digit numbers with best

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

known factorization algorithm with large machine. Even though [16][17] RSA is prone to attack, RSA made stronger by Digital signature concept

Diffie-Hellman key exchange: There is no secure way to transfer a private key through insecure channel in symmetric cryptographic algorithm so in 1976 Diffie-Hellman Key Agreement Protocol was developed. It gave new direction to cryptography and gave path to the development of public key cryptosystem

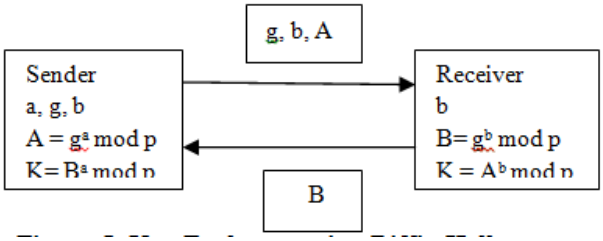


Figure 5: Key Exchange using Diffie-Hellman

Cryptanalysis on Diffie-Hellman: It lacks authentication so it suffers from active attack such as man-in-the middle attack so it is always used along with digital signature or asymmetric algorithm for authentication.

SHA-256: Its operation is similar to MD4, MD5 and SHA-1. The message to be hashed is first padded with its length to make it 512 bits long and parsed into 512-bit message block. The message blocks with 512 bit are processed one at a time beginning with a fixed initial hash value H(0) and computation is done sequentially

H(i) = H(i-1) + CM(i) (H(i-1)) where C is a SHA-256 Compression function and + means word-wise mod 232 addition. H(N) is the hash of M.

Cryptanalysis on SHA-256: It provides only 128 bit level one-way and collision resistant cryptographic hash security. Birthday attack can be launched in MD4, MD5 and SHA-1 so the attack is possible in SHA-256.
Speed Analysis on Different Cryptographic Algorithms
System Configuration on which speed test was performed.
Operating System used: Windows Xp with Service pack 3 Build 2600
Processor used: x86 Family 15 Model 107 Stepping 1 Authentic AMD 2109 MHz
Memory: 1 GB RAM

The below table shows the speed of different Symmetric algorithm in CBC Mode for different buffer size

Buffer Size		5 MB	
S.No	Algorithm	Enc Speed	Dec Speed
1	DES	45.5 MB /sec	35.7 MB/sec
2	3DES	12.8 MB /sec	12.3 MB/sec
3	BlowFish	106.4 MB /sec	106.4 MB/sec
4	AES	45.9 MB/sec	80.6 MB/sec

Table1: Benchmark analysis for buffer size 5 MB

Buffer Size		10 MB	
S.No	Algorithm	Enc Speed	Dec Speed
1	DES	40 MB /sec	37.6 MB/sec
2	3DES	13.6 MB /sec	13.1 MB /sec
3	BlowFish	91.7 MB/sec	80 MB/sec
4	AES	45.7 MB/sec	45.9 MB/sec

Table2: Benchmark analysis for buffer size 10 MB

Buffer Size		20 MB	
S.No	Algorithm	Enc Speed	Dec Speed
1	DES	35.6 MB /sec	32 MB/sec
2	3DES	12.0 MB /sec	11.7 MB /sec
3	BlowFish	80 MB/sec	85.5 MB/sec
4	AES	51.2 MB/sec	55.6 MB/sec

Table3: Benchmark analysis for buffer size 20 MB

Buffer Size		30 MB	
S.No	Algorithm	Enc Speed	Dec Speed
1	DES	33.7 MB /sec	36.2 MB/sec
2	3DES	11.9 MB /sec	12.8 MB /sec
3	BlowFish	76.9 MB/sec	80 MB/sec

ISSN (Online) 2394-2320

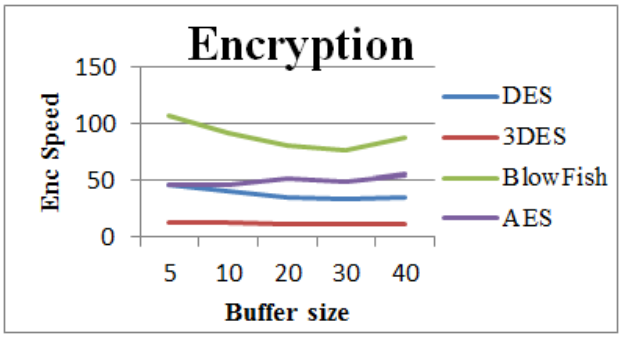
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

4	AES	49.3 MB/sec	51.9 MB/sec

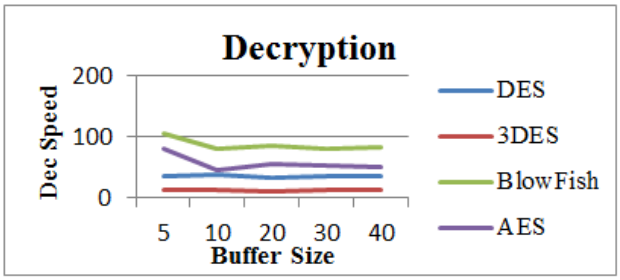
Table4: Benchmark analysis for buffer size 30 MB

Buffer Size		40 MB	
S.No	Algorithm	Enc Speed	Dec Speed
1	DES	35.6 MB /sec	35.1 MB/sec
2	3DES	11.9 MB /sec	12.4 MB /sec
3	BlowFish	88.1 MB/sec	82.6 MB/sec
4	AES	55.6 MB/sec	50.2 MB/sec

Table5: Benchmark analysis for buffer size 40 MB



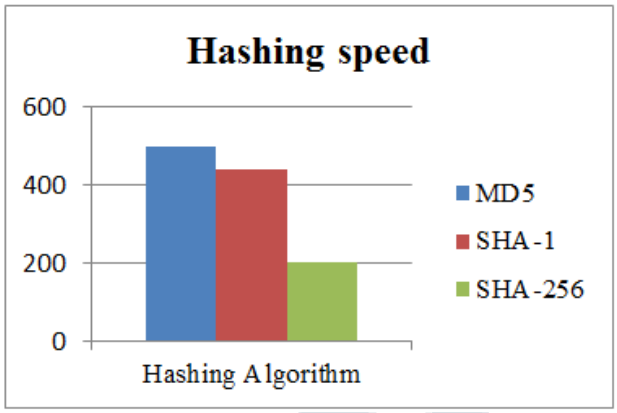
Graph1: Benchmark Analysis – Symmetric Encryption



Graph2: Benchmark Analysis – Symmetric Decryption

S.No	Algorithm	Hashing Speed
1	MD5	500 MB /sec
2	SHA-1	440 MB /sec
3	SHA-256	200 MB/sec

Table6: Hashing Algorithm – Speed Analysis

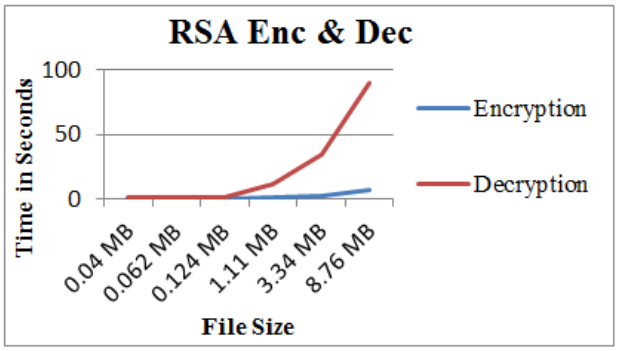


Graph3: Hashing Algorithm – Speed Analysis

File Size (MB)	Algorithm	Encryption in sec	Decryption in sec
0.040	RSA 512	0.032	0.406
0.062	RSA 512	0.047	0.640
0.124	RSA 512	0.078	1.250
1.11	RSA 512	0.782	11.359
3.34	RSA 512	2.359	34.063
8.76	RSA 512	6.187	89.718

Table7: RSA – Time taken for Encryption & Decryption based on File Size

Tools used : BestCrypt, CrypTool



Graph4: RSA – Time Taken for Encryption and Decryption based on File Size

Simulated Environment to Study – Performance, Transmission Costs and VM Cost in Cloud

Scenario – 1:

File Size: 5 MB

User Base: Asia

Data Center: North America with 5 VM and 512 MB RAM with Xen OS

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Overall Response Time Summary

	Avg (ms)	Min (ms)	Max (ms)
Overall response time:	499.87	360.26	645.30
Data Center processing time:	0.40	0.08	0.74

Cost

Total Virtual Machine Cost ($):	0.50
Total Data Transfer Cost ($):	10.92
Grand Total: ($)	11.42

Data Center	VM Cost $	Data Transfer Cost $	Total $
DC1	0.50	10.92	11.42

Scenario – II:
File Size: 20 MB
User Base: Asia
Data Center: North America with 5 VM and 512 MB RAM with Xen OS

Overall Response Time Summary

	Avg (ms)	Min (ms)	Max (ms)
Overall response time:	500.22	337.81	672.63
Data Center processing time:	0.40	0.07	0.89

Cost

Total Virtual Machine Cost ($):	0.50
Total Data Transfer Cost ($):	222.26
Grand Total: ($)	222.76

Data Center	VM Cost $	Data Transfer Cost $	Total $
DC1	0.50	222.26	222.76

Tool used for simulation - CloudAnalyst

Findings on Data Obtained

Based on study on different symmetric, asymmetric and key exchange algorithms, we found that Blow Fish is faster than DES, 3DES and AES both in encryption and decryption but it suffers from second order differential attack and it works well for embedded systems as it consumes less memory. Second place goes to AES but stable through out execution for different buffer size which is vulnerable but not completely breakable, third and fourth goes to DES and 3DES respectively. MD5, SHA-1 and SHA256 occupied first, second and third place respectively. RSA decryption time is greater than encryption time as the file size increases.

Studying on Simulated environment we found that Transmission cost increases as the distance increases and VM Processing costs remains same for increased file size.

CONCLUSION

In cloud, file size is of small and large size and involves more encryption and decryption. More over by choosing symmetric cryptosystem we can increase the speed of encryption by 30 to 40 percent when compared to Asymmetric cryptosystem as it takes more time for encryption and decryption. So the best choice is AES for transit. For Persistent storage we can use RSA as it is highly secure compared to other algorithms. For symmetric Key exchange we can use Diffie-Hellman along with RSA.

The cost of Transmission depends on the location of DC and Cost of VM depends on the processing capacity of VM Machine.

REFERENCES

Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry, "Security Algorithms for Cloud Computing", Procedia Computer Science 85 (2016) 535 – 542

Jing-Jang Hwang, Taoyuan, Taiwan, Yi-Chang Hsu, Chien-Hsing Wu, "ABusiness Model for Cloud Computing Based on a Separate Encryption and Decryption Service", international Conference on Informationscience and Applications(ICISA), Pages 1-7, 2011.

Prakash G L , Dr. Manish Prateek and Dr. Inder Singh, "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 3 Issue 4 April, 2014 Page No. 5215-5223

Dr. C.P.Agrawal, Zeenat Hasan, "Analysis of Different Cryptography Algorithms", International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-4,April 2016, ISSN: 2395-3470

Shivlal Mewada, Arti Sharivastava, Pradeep Sharma, S.S. Gautam and N Purohit, "Performance Analysis of Encryption Algorithm in Cloud Computing", International Journal of Computer Sciences and Engineering Vol.-3(2), PP(83-89) Feb 2015, E-ISSN: 2347-2693

Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "Performance Analysis of

Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering 6(3), March - 2016, pp. 659-665.

Nasarul Islam.K.V, Mohamed Riyas.K.V, "Analysis of Various Encryption Algorithms in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017, pg. 90-97.

PradeepSemwal, Mahesh Kumar Sharma, "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing", 978-15090-6403-8/17 2017 IEEE

Dr. D.I. George Amalarethinam, H. M. Leena, "Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud", 978-1-5090-5573-9/16 2016 IEEE.

S.Rajeswari, R.Kalaiselvi, "Survery of Data and Storage Security in Cloud Computing", 978-1-5090-6480-9/17 2017 IEEE S.Rajan, Dr.D.S.Mahendran, Dr.S.John Peter, "Analysis on Economic Viability of Location Based Cloud", 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X

S.Rajan, Dr.D.S.Mahendran, Dr.S.John Peter, "Analysis on Economic Viability of Location Based Cloud", 2018 International Journal of Scientific Research in Science and Technology(IJSRST) | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X

S.Rajan, Dr.D.S.Mahendran, Dr.S.John Peter, "Scalable Map Reduce Model for Aggregating the Data in the Cloud", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 4, Issue 12, December 2017

S.RAJAN, Dr.D.S.MAHENDRAN, Dr.S.JOHN PETER, "A Novel Model for Key Management on Cloud", International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 6, Issue 9, September 2017

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

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

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.

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.