International Journal of Pure and Applied Mathematics
Volume 118 No. 6 2018, 85-94
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Comparative Study on various Symmetric Key Algorithms for enhancing Data Security in Cloud Environment

D.I. George Amalarethinam[1] and H.M. Leena[2]

[1] *Jamal Mohamed College (Autonomous), Tiruchirappalli–620 012. di_george@ymail.com*
[2]*Holy Cross College (Autonomous), Tiruchirappalli–620 002. leena_raja@yahoo.co.in*

Abstract

Cloud computing environment perform challenging tasks for storing sensitive data. Securing data in an efficient way is a tedious process in cloud. The Cloud Service Providers use usual Symmetric Cryptographic Algorithms for encryption and decryption. Most of the cloud customers avoid trusting the providers and use their own proprietary algorithms for securing their sensitive data. Speed is considered as a major issue, while using the proprietary algorithms. So it is recommended to use proprietary algorithms for key management rather than data encryption. Key generation and management is a vital part in encryption process. Genetic algorithms bring optimal solution for most of the optimization problems. Thus Key Generation Genetic Algorithm was proposed to generate an optimal key. The generated key is encrypted using the Asymmetric Addition Chaining Cryptographic Algorithm, a proprietary algorithm to strengthen the key for encryption process. The encrypted key can be sent to one of the Symmetric key algorithms like AES, DES, Blowfish etc., for data encryption. The proposed comparative study helps to identify the well suited algorithm for data encryption based on its speed. Thus the study shows that the Blowfish algorithm has better speed than others for data encryption in cloud.

Key Words and Phrases: Cloud Computing, Symmetric Key Algorithms, Speed, Data Security, Proprietary Algorithms.

1 Introduction

Now-a-days Cloud technology is playing a vital role in offering the various services like Infrastructure, Software and Platform based on demands of the users. The Cloud Service Providers (CSPs) take the responsibility of providing these services with limited security. Even though these providers move to the proficiency of servicing, there still exist some challenges and issues faced by the cloud customers. When the customer selects the appropriate provider for storing their data, the providers uses some standard cryptographic algorithms for securing users' data. Symmetric Key algorithms and Asymmetric Key algorithms are major two subdivisions of Cryptographic algorithms. It is also efficient to use standard algorithms approved by formal Standards body like National Institute of Science and Technology (NIST) for data encryption than proprietary algorithms. Symmetric encryption involves the use of a single secret key for both the encryption and decryption of data. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data. It would be highly unusual to use an asymmetric algorithm for this encryption use case [1]. Selecting one Symmetric Key Algorithm from various available algorithms like AES, DES, 3DES, Blowfish etc., is an important task. The task can be accomplished by applying the speed factor. The algorithm having the high speed can be used for encrypting the data. While considering the key to be used for encryption and decryption, it is difficult for the CSPs to properly manage all the customers' key. So, the main concentration is on how the keys are managed and by whom. Key Generation and Management are the two main processes that are to be considered in encryption process. Generating a optimal key must be done carefully. Genetic Algorithm is a powerful tool for optimization problems. Thus it is better to generate an optimal key using the genetic algorithm. The security strength of the cryptographic mechanism used is at least as strong as the security strength required for the keys being managed [2]. Thus the generated optimal key is strengthened by the process of encryption. After the key is encrypted it is further can be used for data encryption which is encrypted by any one of the Symmetric Key Algorithms chosen based on its speed.

2 Related work

Randeep Kaur et al. [3] discussed the various number of existing techniques used to implement security in cloud. The algorithms are classified as symmetric and asymmetric algorithms. In future Symmetric algorithms can give better performance in terms of speed as compared to asymmetric algorithm. Researchers can consider security problems related to existing security algorithms and implement a better version of DES, 3DES, AES, RSA, IDES, Blowfish etc.,

Punam V. Maitri et al. [4] suggested asymmetric algorithms provide better security as compared to symmetric algorithms. Blowfish algorithm gives better performance in terms of speed as compared to AES algorithm but AES algorithm require minimum amount of time for encryption and decryption than RSA.

Omer K. Jasim et al. [5] analyses the importance of security to cloud. Comparison was made on seven algorithms, five algorithms for symmetric algorithm and two

for asymmetric algorithm for data security in cloud. Moreover, it is concluded that the algorithms implemented are more efficient on cloud environment.

Rashmi Nigoti et al. [6] showed the comparison of DES, Triple-DES, AES, and Blowfish which are symmetric algorithms. DES and AES are mostly used symmetric algorithms. DES is quite simple to implement then AES. RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange are used to generate encryption keys for symmetric algorithms. But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data.

Shakeeba S. Khan et al. [7] proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using single level encryption.

3 Proposed system

The KGGA [8] is used to generate the Key that is to be used for Encryption and Decryption. The KGGA algorithm produces a prime optimal key 7757 after the 100th iteration by setting the population size as 10, cross over rate as 0.5 and mutation rate as 0.1 The generated optimal key is then encrypted using a proprietary algorithm called Asymmetric Addition Chaining Cryptographic Algorithm (ACCA) [9]. The aim of this algorithm is to reduce the time taken for encrypting the key by replacing the modular exponentiation of encryption and decryption processes of RSA by the concept of Addition Chaining.

This encrypted key is given to the selected symmetric key algorithms like AES, DES and Blowfish. The results are analyzed to choose the best symmetric algorithm for encryption.

4 Comparative analysis

The file sizes chosen for encryption are 128, 256, 512 and 1024 KB. The varying key sizes of the respective algorithms with encryption and decryption time is shown in table III.

It is observed that the key sizes of 128 and 192 are applicable for AES and Blowfish, but not for DES. Thus the comparison is considered only for AES and Blowfish based on their similar key sizes. Table III shows only the comparison between AES and Blowfish.

It is revealed from table III that the Blowfish algorithm has better speed than AES algorithm. Thus the Blowfish algorithm is chosen for data encryption.

Figures 1a, b, c and d depict the encryption and decryption time of AES and Blowfish algorithms for key sizes 128 and 192 respectively.

The encryption time of both AES and Blowfish Algorithms are found and compared.

Table 1: Encrypted values of the key 7757 using ACCA. Key generated by KGGA (4 digits): 7757.

Key size of ACCA (bits) for Encryption and Decryption	Encrypted value of the Key
64	5039270317385696211156239300821812074 23 65007903032734662632893471942544647240
128	187213772152031871532025125172867563757268275110825618811218 641300975821784348430847437512728678263655229074991194524979 228954408239372445184538333500737287213772152031871532025125 172867563757268275110825618811218641300975821784348430847437 512728678263655229074991194524979228954408239372445184538333 500737216105411958023997650998231649283672753941050736337714 507812383551896866568341268968932533326847619900167385996361 768689376035891294945671991073418391444418721377215203187153 202512517286756375726827511082561881121864130097582178434843 084743751272867826365522907499119452497922895440823937244518 45383335007372
256	886390530346664964924099723059959260654991258943622758348983 091475919029741648365813721368722169763230965667862759597883 240299601939638287613667149945355087148561035775201557390815 827251204573085166484566401901129635487494344819708305145709 367955453026440096061138423338229266764960743998216440816027 751722588639053034666496492409972305995926065499125894362275 834898309147591902974164836581372136872216976323096566786275 959788324029960193963828761366714994535508714856103577520155 739081582725120457308516648456640190112963548749434481970830 514570936795545302644009606113842333822926676496074399821644 081602775172252246980456635583278537775755257997589571234519 192592589573211507547676363968063571979279819912401698215711 221457530199004091412598778849558677987656273840503745763735 752753312085348888666316426723602134190809835160259941736981 948773243721664852541148053852684361240592273676408518726941 628333907688449607652188639053034666496492409972305995926065 499125894362275834898309147591902974164836581372136872216976 323096566786275959788324029960193963828761366714994535508714 856103577520155739081582725120457308516648456640190112963548 749434481970830514570936795545302644009606113842333822926676 496074399821644081602775171225

Table 2: Comparison of encryption and decryption time of three symmetric algorithms with different key and file sizes. ET: Encoding time, DT: Decoding time.

File	AES			DES			Blowfish		
size	Key size	ET	DT	Key size	ET	DT	Key size	ET	DT
(kB)	(Bits)	(ms)	(ms)	(Bits)	(ms)	(ms)	(Bits)	(ms)	(ms)
128	128	234	15	64	245	16	128	209	12
	192	234	31	–	–	–	192	211	12
256	128	234	15	64	312	27	128	210	17
	192	243	24		–	–	192	237	17
512	128	250	32	64	286	63	128	229	24
	192	281	31		–	–	192	230	27
1024	128	249	63	64	371	97	128	258	44
	192	293	59		–	–	192	260	47

Table 3: Comparison of encryption and decryption time of the symmetric algorithms with similar key sizes. ET: Encoding time, DT: Decoding time.

File	Key	AES		Blowfish	
size	size	ET	DT	ET	DT
(kB)	(Bits)	(ms)	(ms)	(ms)	(ms)
128	128	234	15	209	12
	192	234	31	211	12
256	128	234	15	210	17
	192	243	24	237	17
512	128	250	32	229	24
	192	281	31	230	27
1024	128	249	63	258	44
	192	293	59	260	47

Table 4: Relationship between plain text and cipher text of blowfish algorithm.

Statistical metrics	Existing system		Proposed system	
	Plain text	Cipher text	Plain text	Cipher text
Mean	104.5384615	152.5384615	104.5384615	122.6923077
Std. Dev.	15.25677655	72.919608	15.25677655	68.63476356
Covariance	475.7869822		225.6272189	
Correlation Coefficient	0.463305601		0.233424625	

From the graphs of Fig. 1, it is clear that the Blowfish algorithm performs better in both encryption and decryption processes.

5 Results and discussions

The strength of the security of the Blowfish algorithm is tested mathematically by calculating Mean, Standard Deviation, Covariance and Correlation Coefficient. These Statistical metrics can be used to identify the relationship between any two data sets. Thus, these metrics are applied to find the relationship between the plain text and the cipher text.

In the existing system, the Blowfish algorithm generates its own key for data encryption. The proposed system uses the key generated by KGGA and encrypted by ACCA algorithm. The statistical metrics are performed on both the systems to identify the relationship between the plain text and cipher text.

Illustration

The formulas for calculating Mean, Standard Deviation, Covariance and Correlation Coefficient are given in (1) through (4).

$$\text{Mean } (\mu) \qquad \mu = \sum_{i=1}^{n}(X_i)/n \tag{1}$$

$$\text{Standard Deviation } (\sigma) \qquad \sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu)^2} \tag{2}$$

$$\text{Covariance } (\text{cov}(x,y)) \qquad \text{cov}(x,y) = \frac{\sum_{i=1}^{n}(x_i-\mu_x)(y_i-\mu_y)}{(n-1)} \tag{3}$$

$$\text{Correlation coefficient } (\rho_{x,y}) \qquad \rho_{x,y} = \frac{\sum_{i=1}^{n}(x_i-\mu_x)(y_i-\mu_y)}{(n-1)\sigma_x\sigma_y} \tag{4}$$

The values of Correlation Coefficient normally are $-1, 0$ or 1.
Minus one indicates that there is no relationship between the two data sets.
Zero specifies that the two data sets just aren't related.
And one denotes that there is a relationship between two data sets.

The absolute value of the correlation coefficient gives the relationship strength. The smaller the number, the lesser the relationship is. The correlation coefficient

of the existing system is approximately 0.463 where for the proposed system it is 0.233. This reveals that in the proposed system, there is a minimum relationship between the plain text and cipher text than the existing system.

This indicates that it is difficult to recognize the plain text even though the cipher text is captured by the intruder.

6 Conclusion and future work

Among the three Symmetric algorithms AES, DES and Blowfish, Blowfish algorithm has better speed than others. So it is obvious that the data that is stored in the cloud is more secured by using proper key management and data encryption algorithms. In future, these algorithms can be offered as services to the cloud consumers who want to use the proper key for data encryption.

References

[1] Tim Mather, Subra Kumaraswamy, Shahid Latif, *Cloud Security and Privacy*, O' Reilly online edition.

[2] Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, *Cryptographic Key Management Issues & Challenges in Cloud Services*, National Institute of Standards and Technology Interagency or Internal Report 7956 35, 2013.

[3] Randeep Kaur, Supriya Kinger,*Analysis of Security Algorithms in Cloud*, International Journal of Application or Innovation in Engineering & Management Computing, **3**(3)(2014),171-176.

[4] Punam V. Maitri, Aruna Verma, Enhancing File Security using Cryptography Algorithms in Cloud Computing: A Survey, *International Journal of Innovative Research in Computer and Communication Engineering*,**3**(10)(2015),9611–9615.

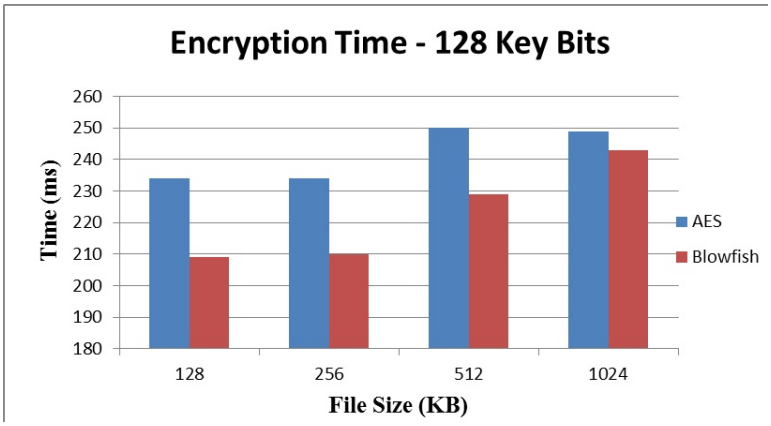
[5] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, Efficiency of Modern Encryption Algorithms in Cloud Computing,*International Journal of Emerging Trends & Technology in Computer Science*,**2**(6)(2013),270–274,.

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

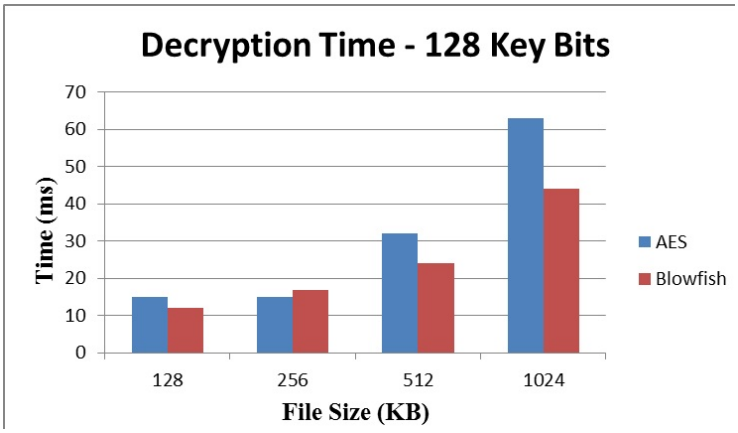
[7] Shakeeba S. Khan, Prof.R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms, *International Journal of Innovative Research in Computer and Communication Engineering*, **3**(1)(2015), 148–154, .

[8] D. I. George Amalarethinam, H. M. Leena, A New Key Generation Technique Using GA for Enhancing Data Security in Cloud Environment, ıInternational Journal of Cloud Computing, 2017.(accepted to be published).

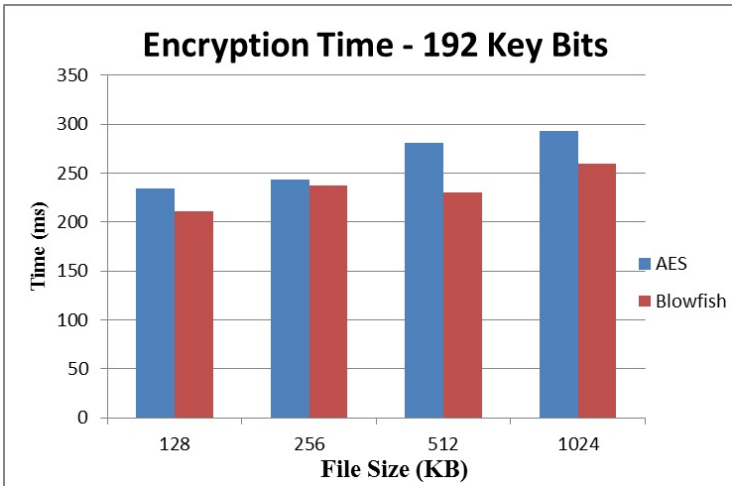
[9] D. I. George Amalarethinam, H. M. Leena, *Asymmetric Addition Chaining Cryptographic Algorithm (ACCA) for Data Security in Cloud*, Springer Verlag, 2017. (accepted to be published).



Encryption Time of AES and Blowfish Algorithms for 128 key bits.



Decryption Time of AES and Blowfish Algorithms for 128 key bits.



Encryption Time of AES and Blowfish Algorithms for 192 key bits.