JCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-12 E-ISSN: 2347-2693

Identifying High Performing Symmetric Key Algorithms in Transferring Data into Cloud

Ashok Sharma

PG Department of Computer Science, MIET, Jammu

Available online at: www.ijcseonline.org

Received: 21/Nov/2017, Revised: 06/Dec/2017, Accepted: 14/Dec/2017, Published: 31/Dec/2017

Abstract- The drastic amount of data is transferred into public cloud at every moment and securing data while transferring into cloud has become a tradition and in this paper we present scope of improvement for using optimized symmetric key algorithm for cloud environment. After careful investigation AES, 3DES, RC6, Twofish, Blowfish algorithms, In this paper, we proposed an approach to select optimized algorithm for deciding the use of efficient algorithm in cloud depending upon the outcomes of investigations carried. The future work can be carried out in the direction of replacement of conventional key expansion routine with the genetic concept routine in the identified algorithm.

Keywords: Conventional Key Expansion, AES, Blowfish, Twofish, Genetic Operation

I. INTRODUCTION

We have observed that symmetric algorithms and their usage in securing and storing data in cloud [1] and the issues in investigation of efficient cryptic algorithm with respect to varied file types and file size in cloud storages in terms of various parameters[2] and depending upon the same framework has been proposed by researchers and some of the result shows AES is better in some cases whereas Blowfish is performing better under some conditions.

II. OUTCOME OF SYSTEMATIC RESEARCH CARRIED IN STORING IMAGES IN CLOUD

As per the analysis of literature and state of approaches, it has been found that there is a need to design and develop a framework and device a mechanism to test behavior of multiple cryptic algorithms based on various parameters and so as an outcome, cloud based Crypter tool came into existence. We have introduced this Crypter tool with feature of adding cloud user's files and for tuning characterstics of cloud algorithm (CCA-i) where CCA= {AES, 3DES, RC6, Twofish, Blowfish}. These algorithms [CCA-I] are integrated with the tool itself for convenience.

The increasing trend of usage of static and time variant contents including Text files, Image files, audio files and video files by clients and storing these files in cloud has led to investigate efficient cryptic algorithm in terms of user specified parameters. To analyze these algorithms CCA-i with varied parameters has been presented.

III. OUTCOME OF SYSTEMATIC RESEARCH CARRIED IN STORING AUDIO AND VIDEO IN CLOUD

Similarly, the investigation for the contents which are variable with respect to time is presented using cloud based cryptic tool. For generic cloud data, with respect to need and size of key, the performance of cryptic algorithms on specified parameters and their comparative analysis has been presented. To make usage of cryptic algorithm in adaptive manner, one specific algorithm is not sufficient for all user's need. However, current practices in industries are doing so. Industries are deploying only one type of algorithm. The contribution of this research work is making the system more optimal and adaptive, by giving directions to use cryptic algorithm according to file type and parameters decided by the system and industries.

IV. COMPARATIVE ANALYSIS OF PERFORMANCE OF SYMMETRIC KEY ALGORITHMS IN ALL CASES OF DATA STORING IN CLOUD

Alternatively, the conclusion of this research work is presented in the form of a decision table specified in Table 1. This table contributes the body of knowledge by denying the statement that one algorithm fits for all, means one type of cryptic algorithm is not sufficient for all type of clients file (Text, Image, Audio and Video) depending upon parameters encryption time, decryption time, memory utilization and throughput.

Table 1 Optimized cloud cryptic algorithm in terms of different parameters

		Parameters			
		R_1	R_2	R_3	R_4
File Types	**Text type cloud information**	X	X	X	X
	Image type cloud information	X	X	X	X
	Audio type cloud information	X	X	X	X
	Video type cloud information	X	X	X	X
Cloud Cryptic Algorithms	**CCA-1**	✓	✓		
	CCA-2				✓
	CCA-3				
	CCA-4				
	CCA-5			✓	

The Restriction or demand of the system (As a decision making criterion) are as under:

R_1-Encryption Time E_t (in Seconds)
R_2-Decryption Time D_t (in Seconds)
R_3-Throughput
R_4-Memory Utilisation for Enciphering and Deciphering

The cloud based cryptic algorithm deployed on Amazon /Digital Ocean cloud were:

CCA-1 Cryptic Cloud Algorithm –AES
CCA-2 Cryptic Cloud Algorithm-3DES
CCA3-Cryptic Cloud Algorithm-Twofish
CCA-4 Cryptic Cloud Algorithm-RC6
CCA-5 Cryptic Cloud Algorithm-Blowfish.

The research work carried out in chapter 4, chapter 5 and chapter 6 concludes that AES and Blowfish are better in comparison to RC6, Twofish and 3DES algorithm on most of parameters considered for investigation in cloud storages except memory utilization.

Moreover, AES is found better in encryption time and decryption time for all formats of data files in cloud but the performance of Blowfish is better than AES if we consider throughput as parameters and 3DES is better in terms of memory utilisation among all cipher provided channel of communication is secure.

Therefore, we have concluded that there is no single cryptic algorithm, which is efficient in terms of all four parameters encryption time, decryption time, memory utilisation, and throughput in cloud and cloud users can select among AES, 3DES and Blowfish depending upon their selection of parameters.

Since AES is more secured in comparison to Blowfish and 3DES. Therefore, for deciding between these ciphers, we prefer to review the working of AES algorithm and can look into the scope of enhancement in AES if possible as AES is secured among all ciphers.

Since Advance Encryption Standard (AES) algorithm is one of the symmetric key algorithms which is widely adopted by industry for data encryption and decryption process and if we go in detail, a key expansion routine is the main ingredient of any ciphering algorithm that expands small cipher key into a larger set of keys called round keys and it is very well understood that a strong round key yields strong cipher which is more defiant to both linear cryptanalysis and differential attacks.

V. CONCLUSION

As we have found that, there is no single algorithm, which is efficient in terms of all parameters mentioned for encrypting/decrypting data files of different format and different types in cloud. Since AES is more secure than any cryptic algorithm but being not good in terms of Throughput and memory utilization in comparison to blowfish, Future work can be done in the direction of optimization of Cloud cryptic algorithms under various parameters like GPU based Processing, divide and conquer approaches for parallel platforms.In addition, Cloud cryptic algorithms can be optimized using evolutionary computing approaches such as Genetic and Swarm approaches. The GA has been widely used in information security areas especially in cryptic algorithms for data security by various researchers [3, 4, 5, 6, 7,8, 9].

Encryption or Decryption is a process of substitution and Transformation and in case of AES, Various transformation and substitution processes can be replaced with Genetic operations like Selection or Reproduction Operation, Crossover Operation, Mutation Operation. In future, the key expansion function of AES may be replaced by Genetic operations. This function will use GAs process to generate successive keys for the AES rounds. Genetically modified AES can be proven better candidate under most of parameters including memory utilisation and throughput to overcome the blowfish algorithm.

REFERENCES

[1] Ashok Sharma, Ramjeevan Singh Thakur, Shaliesh Jaloree, "Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud", International Journal of Scientific Research in Computer Science and Engineering,Vol.4(5), pp.5-11, 2016 ISSN: 2320-7639.

[2] Ashok Sharma, Ramjeevan Singh Thakur, Shaliesh Jaloree, "Investigation of Efficient Cryptic Algorithm for Video files Encryption in Cloud", International Journal of Scientific Research in Computer Science and Engineering,Vol.4(6) pp.8-14, 2016 ISSN: 2320-7639.

[3] Yaseen I , Sahasrabuddhe H., "A Genetic Algorithm for the Cryptanalysis of Chor Rivest Knapsack Public Key Crypto System (PKC)" in proceeding of third International Conference on Computational Intelligence and Multimedia Application, September 23-26, New Delhi 1999.

[4] Mathews R., "The use of Genetic Algorithm in Cryptanalysis", Cryptologia, Vol.17(4), 1993.

[5] Spillman R, "The Use a Genetic Algorithm in the Cryptanalysis of Simple Substitution Ciphers" Cryptologia, Vol.17(1), 1993

[6] Bagnall A, "The Application of Genetic Algorithm Cryptanalysis", Master Degree Thesis in School of Information Systems, University of East Anglia 1996

[7] McKeon G. and Rayward-Smith V., "The Cryptanalysis of a Three Rotor Machine Using Genetic Algorithm" available at http://citeseer.nj.nec.com/162166.html

[8] http://dip.sun.ac.za/~vuuren/papers/genetic.ps.

[9] Rashed Abdali, "Using Modified Genetic Algorithm to Replace AES Key Expansion Algorithms", Journal of Applied Mathematical Sciences, Vol.7 (144), pp.7161-7171, 2013.