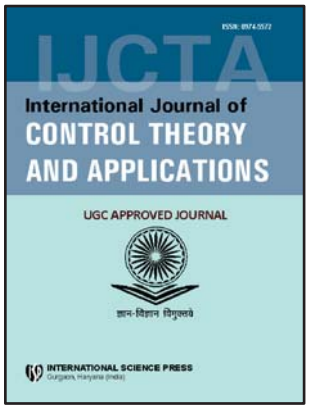

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 32 • 2017

Enhancing the Security of Data Transaction Under the Cloud by using Compression and Encryption Mechanism

Sheik Saidhbi[a] and Komati Thirupathi Rao[b]

[a]*Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu*

E-mail: sfajju.syed@gmail.com

[b]*Professor and Associate Dean-Academics, K L University, AP.*

E-mail: profktrao@gmail.com

Abstract : Cloud Computing provides an excellent environment for the resource sharing mechanism in each and every cloud user's perspective and also reduce the cost of resource utilizations. If the data is going to be store in a third party network by multiple users consumption bring an attention to the secure data transaction. Usually the way to secure cloud data is accomplished with the help of cryptographic algorithms (such as AES -Advanced Encryption Standards, DES-Data Encryption Standards, etc..,). At the same moment, compression algorithms are applied to save the storage space for multimedia data or information's. In this research paper give a initiation to secure the data transaction under the cloud services with the combination of compression mechanism and Crypto graphic algorithms. The combination of two mechanisms provides a complimentary environment regarding to save the storage space as well as to secure the data transaction.

Keywords*: Encryption, Compression, Cloud, Security and Data.*

1. INTRODUCTION

The major objective of the, cloud secure data transaction is carried out by different researchers in different perspective with the help of encryption algorithms in standalone. Especially in this research paper essentially focus on effectively consider the data components of multimediainformation resides cloud servers. Diversity of multimedia content, the data has to be taken into account for secure transaction under the cloud services.

The concepts of compression are almost considered as the process of saving storage space or packing more data into the same size space. Before to store the data into the cloud server, it will be compressed and to apply the encryption mechanism on the compressed data in order to protect it from unauthorized access. There are varieties of compression algorithms exist (such as Arithmetic coding, Huffman coding, etc..,) as well as crypto algorithms are using for effective secure data transactions. It's described in the related work and usually the concept of Security in cloud computing consisting the following characteristics:

1.1. Privacy

It is considered as an important content in the cloud storage of different user's confidential data or information. In general, the categorization of secure level either it may be confidential or unclassified to make it as a public one is the responsibility of the user. If the incoming date or information is request a storage allocation in the cloud server, it will be scheduled according to level of its security assignment.

1.2. Data Confidentiality

The level of security assignment for the data or information is going to be store in a cloud server is determined by the owner. Based on the level of security assignment the data is handled by the cloud servers [1]. The data or information encryption is used for most of the situations to prevent residing data from un-authorized access. Before it deliver to the cloud users, it get decoded form and to produce an original message. The following diagram (figure 1) obliviously stipulate the principle behind the proposed framework.

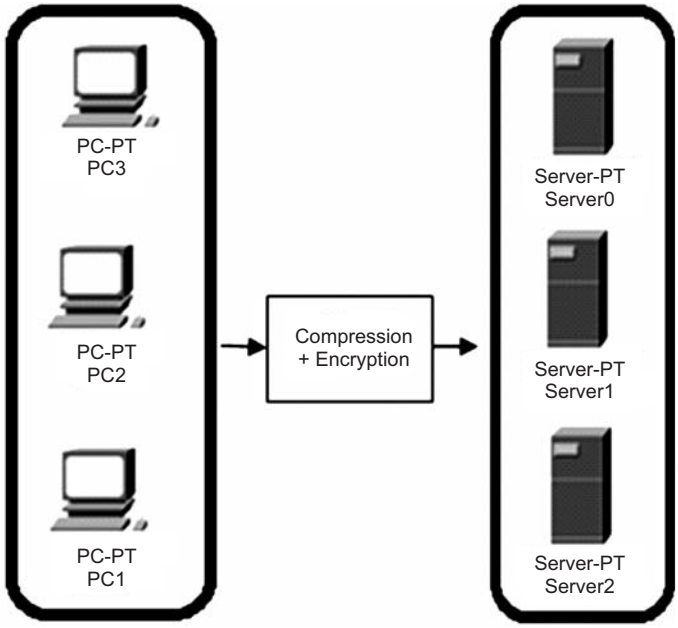

Figure 1: Secure data communication in cloud

The communication between cloud clients and cloud server is ensuring a secure way by using cryptographic algorithms in general at most of the applications. Here to addressing this issue with the help of compression[2].

2. RELATED WORK

Internet services are generally consumed by the clients or users through web browsers and will be carried out with the help of numerous supporting protocols. It works almost to act as the intermediate communication between the users and cloud service providers. There are no specific functionalities or modifications on the data sharing or store mechanisms. In order to related this work, in this section indicates some of the compression algorithm and cryptographic algorithms involving in a secure cloud data transactions.

2.1. Huffman Compressor

Huffman coding, compression and decompression is a short program that needs very little memory. But it doesn't compress particularly well when compared to commonly use other compression techniques programs. The efficiency of Huffman coding also depends heavily on having a good estimate of the true probability of the value of each input symbol.

2.1.1. Improvements

Here to surpass the compression ratio of these programs, we need to start adding enhancements to the modelling code. That is Arithmetic coding produces slight gains over Huffman coding. So after constructing the Huffman code, once again apply the arithmetic coding in Huffman code, might be we can get the better result.

2.2. Arithmetic Compressor

This algorithm wills results in both faster updates as well as better compression. This scheme works well for incrementally encoding a message. There isenough accuracy retained during the double precision integer calculations to ensure that the message is accurately encoded. In order to use arithmetic coding to compress data, a model for the data is needed. The model needs to be able to do two things to effectively compress data:

1. The model needs to accurately predict the frequency/probability of symbols in the input data stream.
2. The symbol probabilities generated by the model need to deviate from a uniform distribution.

The process of encoding and decoding a stream of symbols using arithmetic coding is not too complicated. But at first glance, it seems completely impractical. Most computers support floating point numbers of up to 80 bits or so [4][5].

Table 1
Huffman coding VsArithmetic coding

Compression Techniques	*Size of Input files (bytes)*	*Size of Compressed file*	*Compression Ratio*	*Compression Time (Comp + Expan.time)*
Huffman Coding	589312	340021	42.30%	0.08 + 0.09%
Arithmetic Coding	589312	327837	44.37%	0.09 + 0.08%

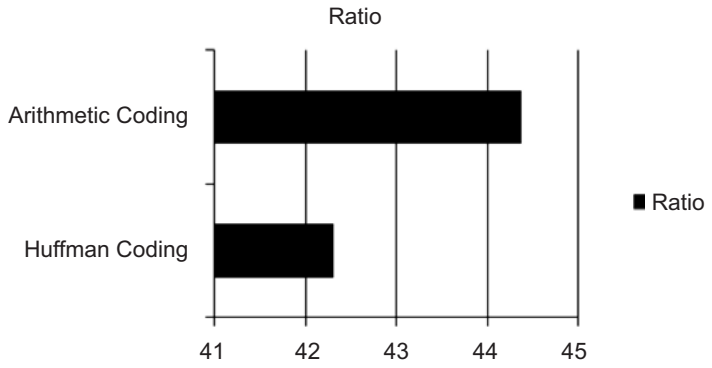

Figure 2: Comparison between the compression algorithms

In order to ensure the cloud data communication over the communication channel is achieved with the help to mixing both Arithmetic compressions on the cloud data storage and encryption algorithm for cloud data share /access. For this reason, now the data (especially to concentrate more on the multimedia information content) is available in the combination of crypto-compressed format of content in its home place.

2.3. MIT group algorithm

In general it specifies the power of numerical equivalent values is consider for encryption and decryption in order to protect the data from unauthorized access. Especially it is based on numeric theory and makes some what complicated extensions to the intruders attempt regarding try to get original information [6][7][8].

3. PROPOSED WORK

The core concept behind the proposed work is obviously illustrated in the figure 3 and 4. The original data or information from the owner outlet is compressed by using the arithmetic coding and applies the encryption algorithm RSA (Rivest, Shamir, Aldimer) on it before to store the cloud server. In the sender node, the data get the modifications such as Original Text (PT), Compressed Text (CT) and Cipher text (CiT) as well as the receiving node, cipher text, decompressed text (DCT) and the original Text.

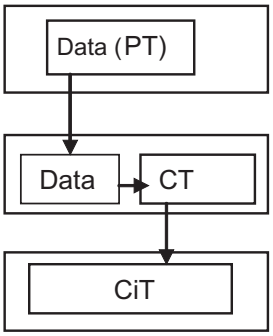

Figure 3: Data transaction in Sender node

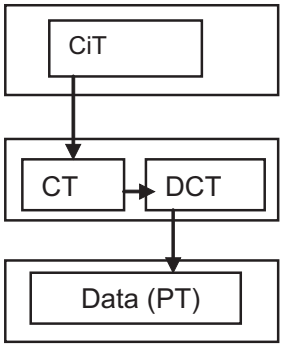

Figure 4: Data transaction at Receiving Node

The following figure 5 shows the detailed explanation about the cloud data transaction under the cloud between the cloud service provider and the client. The data resides in the cloud storage sections are in the combined formation of compression and the encryption in order to secure the data communication over the channel.

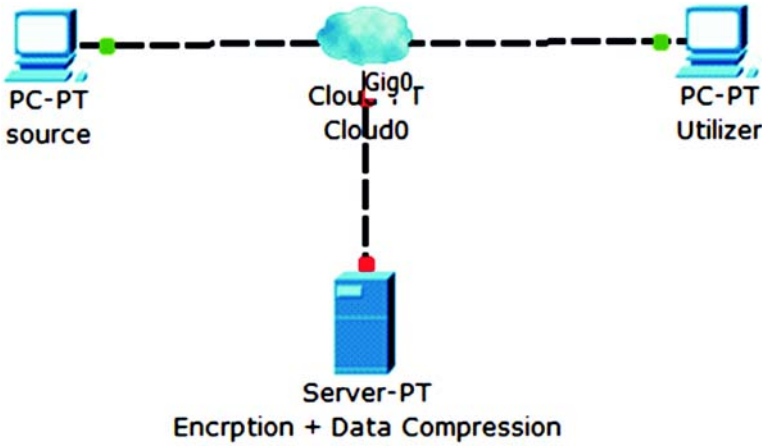

Figure 5: Secure data transmission under cloud

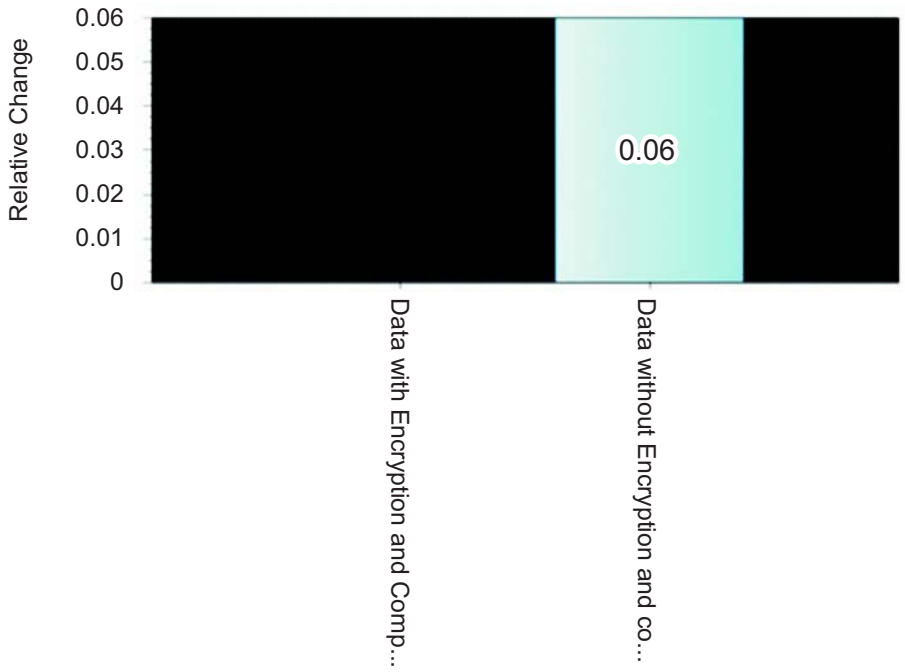

Figure 6: Cloud data security comparison

Receiver Components		
	Data with Encryption and Compression	0.5
Number of Ordinary	0	
Complexity Score	1	
Highest Centrality Variables		
	Data with Encryption and Compression	0.5

Figure 7: Statisticalanalyses for cloud data security

From the figure 6 and 7 depicts the scenario for the cloud security compression and statistical analysis. The data under the cloud transactions in the form with encryption and compression is almost around the "null" value and the risk factor for without encryption and compression is almost around 0.06%.

4. CONCLUSION

The objective of the work is to conduct a secure cloud data transmission over the communication channel. In order to achieve the goal, the work proposes the concept of mixing the compression techniques as well as the crypto system in the multimedia data resided in the cloud data storage section. The previous work for the research article depicts the framework for the cloud storage management and in the extensive effort for that one come to conclusion with the secure data transmission achievement by this modern approach.

REFERENCES

[1] An approach for secure data transmission in Private cloud,AnuragPorwal, RohitMaheshwari, B.L.Pal, GauravKakhani , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012

[2] Information Hiding: A New Approach in Text Steganography , L. Y. POR, B. Delina , Faculty of Computer Science and Information Technology, University of Malaya, 50603, Kuala Lumpur, MALAYSIA porlip@um.edu.my, delinabeh@yahoo.com .

[3] Image Information hiding –An Survey , D. Saravanan, A. Ronald Doni& A. AbishaAjithSathyabama University, Chennai, Tamilnadu, INDIA

[4] Information hiding codes and their applications to images and audio by mehmetkivanc¸ mihc¸ akb.s., Bilkent University, 1996 M.S., University of Illinois at Urbana-Champaign, 1999

[5] Information Hiding Techniques: A Tutorial Review , Sabu M Thampi ,Assistant Professor Department of Computer Science & Engineering ,LBS College of Engineering, Kasaragod Kerala- 671542, S.Indiasmtlbs@yahoo.co.in

[6] IEEE Journal on Selected Areas in Communications.Special Issue on Copyright and Privacy Protection, vol. 16, no. 4, May 1998.

[7] Proceedings of the IEEE. Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, July 1999.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding - a survey,” Proceedings of the IEEE. Special Issue on Protection of Multimedia Content, vol. 87, no. 7, pp. 1062-1078, July 1999.