International Journal of Research in Engineering, Science and Management
Volume 4, Issue 3, March 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Energy Efficient Framework for Cloud Computing

M. Vijay Ram[1*], V. Shanmugha Priya[2], K. S. Sughail Roome[3], B. Vinodhini[4], K. Sangeetha[5]
[1,2,3,4,5]*Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, India*

***Abstract*: The need of cloud computing services is increased widely, because of the growth of digital transformation and large elasticity of the cloud services, in the need of improving the efficiency of energy in data centers. In this paper, a kind of framework used to improve the energy consumption of data center are solved and implemented. The framework is based on these two, that is schedule algorithm and consolidation algorithm. It approaches depending only on one kind of approach as in the previous works. The framework rectifies the customer's request, in the need to their time and power needs before applying the schedule algorithm. It has an algorithm that undertaking the energy consumption when taking it to decisions. It also has another algorithm that determines the servers to be sleep or stop, from the loaded server's virtual machines to be migrate and the servers that will sent migrate virtual machines. The framework includes a jumping algorithm for transferring migrated virtual machines to new servers. Results of checking the experiment denoted the fabulous approach framework to the use the one approach only to put down the energy consumption in order of energy usage effectiveness, data center power secure, intermediate execution time and money saving.**

***Keywords*: Energy consumption reduction, Time saving, Storage saving.**

1. Introduction

Nowadays, most commonly IT-based businesses are cloud computing technologies. Cloud computing is a future technology and also cloud services, such as Apple, Amazon, and Microsoft, Google in the ways of improving more services for cloud services to keep their chances to be in industry to make more business on this and meet the increasing usage of customers. There are many different businesses based shifts to cloud-based puppets for IT systems. As a server by google, about 90% of cloud services are work through cloud computing methods in 2021.

However, International Corporation calculate the size of data used and proposed may reach up to 189 Zetta bytes by 2027.it needs more and more facilities and services to developed by cloud. These kind of facilities and services may cause many data centers and resources to be vanished in cloud that may result in more of electrical energy to be consumed.

Cloud computing systems resources are only for customers' work ships as virtual machines that are put down and complies in data centers. The data centers uses multiple physical servers and each and every server have its own resources.so each cloud have huge amount of resources that consume certain amounts of electrical energy. which cause high production of CO2 formation.

2. Literature Review

In [1], the authors suggested a hybrid steganography solution with the technique of LSB encoding and the DES algorithm. They encrypted the data using the DES encryption algorithm and then embedded the decrypted data using the LSB process. Since the LSB is insufficiently reliable, we may conclude that this device does not have better security.

In [2], an innovative approach for exchanging and safeguarding cloud data using multilayer steganography and cryptography is used. If the AES encryption algorithm encrypts data, the encrypted data is then inserted in a cover picture using the Hash-LSB algorithm.

In [3], An enhanced LSB-based image steganography technique has been applied by the authors of for RGB colour images that have better PSNR value than previously used LSB approaches.

In [4], the authors presented the cloud storage system with a cryptographic public verification of data integrity, where data integrity is verified by a third-party auditor. Nevertheless, the defective third-party auditor could not have adequate evidence.

In [5], the authors introduced a successful method of data encryption to manage data using cryptographic techniques in the cloud storage environment. Data is encrypted here and stored in the cloud afterwards.

In [6], A steganography technique was introduced by the authors of where they used diffusion-based image compression techniques and where stego-image accuracy depends on the number of important points.

In [7], a framework that enhances data storage protection in cloud computing by steganography is introduced. Using the steganography algorithm, they cover the data in an image to boost, then save the stego image in the cloud.

In [8], the authors suggested a multi-layer text encryption using cryptography of variable block size and steganography of images where authors used modified LSB along with raster scan technique for embedding.

In [9], The authors gave an opinion on the ability to obtain

*Corresponding author: ramv16449@gmail.com

data protection in cloud storage through cryptography.

In [10], When using some encryption algorithm, data is encrypted, and stored in the cloud server. It is stable, but it is not ideal for more sensitive data.

In [11], prior to the encryption method, the authors put forth an algorithm for concealing messages in encrypted photos using predetermined watermark embedding. The encryption /decryption here has a specific key and the processing of watermarks has a different key, so the message decryption is independent of extracting the image.

3. Proposed Architecture

1. The proposed system's architecture as shown in Fig.
2. In the following section, 1 and its working steps are defined.
3. The steps involved in this system are illustrated below:
   - *Encryption:*
     By using the Blowfish encryption protocol, the hidden message will be encrypted.
   - *Embedding:*
     In this stage, we would use the E-LSB embedding algorithm to hide the encrypted data in a cover image that would generate a stego-image as an output.
   - *Hashing:*
     Here the stego-image hash value will be determined later using the SHA-256 hashing algorithm to verify data integrity in the cloud storage.
   - *Retrieving:*
     We need to apply the recall algorithm to retrieve the data from the stego-image.
   - *Decryption:*
     The collected data will be decrypted by the Blowfish decryption algorithm to get a hidden code.

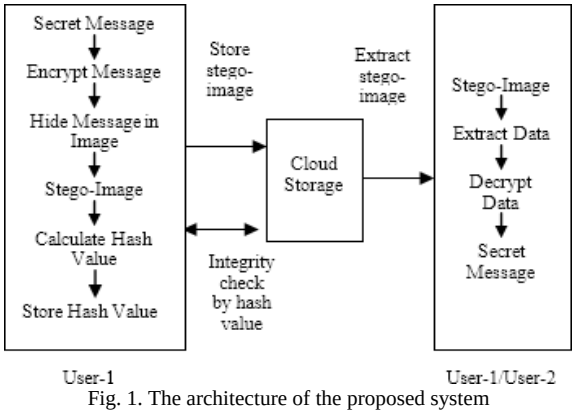

Fig. 1. The architecture of the proposed system

There are essentially three possibilities in the suggested scheme and those are listed below:

1. Safe cloud data storage: This requires two sections
2. Data security: The coding and the embedding algorithm must be used for encrypted data storage.
3. Data extraction: We need to implement the retrieval and decryption algorithm for safe data extraction.
4. Data integrity verification: The hash value of the stego-image has to be determined before it is stored in the cloud storage to check the integrity of the data so that we can quickly check the integrity later.
5. Safe data sharing in the cloud: It is important to supply the receiver with sufficient information to safely share the data so that the receiver can retrieve the data from the cloud storage by using the recovery and decryption algorithm.

4. Embedded least significant bits (E_LSB) Technique

Both RGB image pixels in the Embedded Least Significant Bits (E-LSB) phase are broken into 8-bit frames for the Red (R), Green (G), and Blue (B) planes, respectively. To apply this procedure, we first encrypt the message using the method of Blowfish encryption. Then the encrypted data will be embedded with the least important 3, 3, and 2-bit R, G and B frames, respectively, of a pixel of the image. We take an encrypted data character and transform it to 8-bit binary data (ASCII value), then cover the Rplane's 3 least significant binary data bits, the Gplane's next 3 significant bits, and the B plane's 2 most relevant bits, respectively.

We use the equation for determining the value of each LSB for the restored image pixel (1).

$$\mathbf{V} = \mathbf{P} \oplus \mathbf{M} \tag{1}$$

Here, V = nth pixel plane bit, P = kth pixel plane bit, and M = mth message bit, respectively.

We just need to know the value of P for extraction and we can get the encrypted hidden message again using equation (2),

$$M = V \oplus P \tag{2}$$

Suppose we have to cover in a pixel the encrypted binary message "10101101" whose value for the R, G, and B planes is "01101010", "11101011", and "10001001." We use P = 3rd bit (considering left to right) of each pixel plane for embedding for this case. Table 1 and Table 2 display this method.

Table 1
Binary 8-bits frames of a pixel of the cover image
(before embedding)

01101010	11101011	10001001

The encrypted message bits are: 10101101

Table 2
Binary 8-bits frame of a pixel of the stego-image
(after embedding)

01101010	11101010	10001010

In current techniques such as LSB, H-LSB, Modified LSB, the secret data can be easily retrieved by anybody. But we do not substitute LSB bits for real data in E-LSB, because it is not possible to retrieve the secret data from the stego-image without understanding the value of P. That's why it delivers greater protection than the approaches in use. And we need only the stego-image for the extraction process.

5. Conclusion

The binding of cryptography and steganography is used in the executed method. it encrypts the secure message, the Blow fish encryption algorithm is used for steganography, and LSB based steganography also used here .it provide more data security. In this method, compared to other methods, we have better values, which means that our method is more secure in terms of security. This method can reduce almost 15 KB message in a cover image of size 128×128 pixels, 256 KB in image of size 513×513 pixels, and 468 KB memory in image of size 850×650 pixels. Here we also used the SHA algorithm it calculates the hash value of the image by we can check the purity of the data when it is stored. In future to increase the data reducing capacity, video can be taken as media for usage. For reducing, different data such as 3:4:2 can be usable and randomly can be improved between techniques by switching between methods. It is also possible to approach to hide pixel variation.

References

[1] Kilgarriff, "Googleology Is Bad Science," Computational Linguistics, vol. 33, pp. 147-151, 2007.

[2] M. Sahami and T. Heilman, "A Web-Based Kernel Function for Measuring the Similarity of Short Text Snippets," Proc. 15th Int'l World Wide Web Conf., 2006.

[3] D. Bollegala, Y. Matsuo, and M. Ishizuka, "Disambiguating Personal Names on the Web Using Automatically Extracted Key Phrases," Proc. 17th European Conf. Artificial Intelligence, pp. 553- 557, 2006.

[4] H. Chen, M. Lin, and Y. Wei, "Novel Association Measures Using Web Search with Double Checking," Proc. 21st Int'l Conf. Computational Linguistics and 44th Ann. Meeting of the Assoc. for Computational Linguistics (COLING/ACL '06), pp. 1009-1016, 2006.

[5] M. Hearst, "Automatic Acquisition of Hyponyms from Large Text Corpora," Proc. 14th Conf. Computational Linguistics (COLING), pp. 539-545, 1992.

[6] M. Pasca, D. Lin, J. Bigham, A. Lifchits, and A. Jain, "Organizing and Searching the World Wide Web of Facts - Step One: The One- Million Fact Extraction Challenge," Proc. Nat'l Conf. Artificial Intelligence (AAAI '06), 2006.

[7] R. Rada, H. Mili, E. Bichnell, and M. Blettner, "Development and Application of a Metric on Semantic Nets," IEEE Trans. Systems, Man and Cybernetics, vol. 19, no. 1, pp. 17-30, Jan./Feb. 1989.

[8] P. Resnik, "Using Information Content to Evaluate Semantic Similarity in a Taxonomy," Proc. 14th Int'l Joint Conf. Aritificial Intelligence, 1995.

[9] D. Mclean, Y. Li, and Z.A. Bandar, "An Approach for Measuring Semantic Similarity between Words Using Multiple Information Sources," IEEE Trans. Knowledge and Data Eng., vol. 15, no. 4, pp. 871-882, July/Aug. 2003.

[10] G. Miller and W. Charles, "Contextual Correlates of Semantic Similarity," Language and Cognitive Processes, vol. 6, no. 1, pp. 1-28, 1998.