http://dx.doi.org/10.21172/ijiet.104.05

Security for Cloud Computing using Steganography

Er. Daljit Kaur[1]
[1]*Computer Faculty, B.M. Govt. Sen. Sec. School, Raikot, Ludhiana, Punjab, India*

Abstract- Cloud Computing is a flexible, rate-effective and legitimate platform for all the industries and IT enabled customers offerings the services on the net. The secure data storage on cloud environments is the primary requirement of such applications, where data are being transferred between the servers and their users. Steganography is the system of hiding, encapsulating or understanding the hidden information with the help of digital media. To ensure security of data in cloud computing, this paper presents a new text steganography approach for hiding secret English text file in a cover English text file. The proposed approach improved data security.
Keywords: Cloud Computing, Steganography, Security, information hiding.

I. INTRODUCTION

1.1 Cloud Computing

The importance of Cloud Computing is increasing daily and it's getting a high concentration in industries as good as various other scientific communities. Cloud Computing allows flexible, on demand community access to a shared pool of configured computing resources (storage, server, utility, community and services) that can be quickly provisioned and released with minimal management effort. Cloud computing Appears as a computational paradigm as good as a distribution structure and its predominant purpose is to furnish cozy, rapid, effortless information storage and web computing service, with all computing resources visualized as services and delivered over the web[1][2][3][4].

Cloud computing researchers have divided cloud computing in three layers. First-Infrastructure as a Service (IaaS), inthis technique the hardware resources such as hard disk, memory, networking resources etc. are provided on rent and are charged as per the usage. Second-Platform as a Service (PaaS), which not only provide all the facilities as in IaaS but also provides operating system facilities, their updates etc. Third-Software as a Service (SaaS), which is the most flexible and easiest to use. It has all the features of IaaS and PaaS and it provides the freedom to choose software applications from a bundle of already available resources. SaaS includes some processes that enable the service providers to provide application that can be rented on the internet [5].

1.2. Steganography

Steganography is derived from the Greek word which means covered writing and essentially means "to hide in the palin sight". As defined by Cachin[6] steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been use in for hundreds of years, but with the increasing use of files in digital media new techniques for information hiding have become required.

Steganography and encryption are both used to ensure data confidentially. The main difference between them is that with encryption anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret.

II. RELATED WORK

Steganography and cloud computing are standard areas of research, many concrete and amazing research milestones are finished in these fields. A few of works are as follows:

Sugumaran et al.[7] developed a symmetric layer that was inserted for encrypting the secure data using symmetric algorithm using a block based symmetric cryptography. The major focus was on data security.

Padmapriya et al.[8] developed the classical substitution cipher same key used for encryption and decryption for data security and privacy using the technique of Inverse Caesar Cipher. Security was applied on cloud customer and cloud provider in this model.

Sarkar et al.[9] provides a very solid technique for maintaining the integrity of data. The data being sent to server is saved behind the images. The proposed model makes use of steganography using images for protecting the integrity of data.

Garima et al.[10] provides security of data in cloud computing by combining three algorithms, first apply DSA(Digital Signature Algorithm) for authentication of data. Then apply AES (Advanced Encryption Standard) algorithm for encryption of data and Steganography to hide data within audio file for providing maximum security to the data.
Karun et al. [11] provides hiding algorithm that is used to save the files or data behind the images. The user selects the data to be uploaded and encrypted it using a strong algorithm such as AES algorithm. The encrypted data is then uploaded to server. On receiving data, one which came from user side a hiding algorithm is applied which randomly selects the bits positions from images where data is to be stored.
Awadh et al.[12] presents a new text steganography approach for hiding secret English text file in a cover English text file.

III. PROPOSED STEGANOGRAPHY IN CLOUD COMPUTING

3.1. Proposed Algorithm for Embedding

Input: A secret text file (Fs), cover text file (Fc)
Output: A matrix of locations (Mol)
Step 1: Select secret text file (Fs) and cover text file (Fc) to be uploaded.

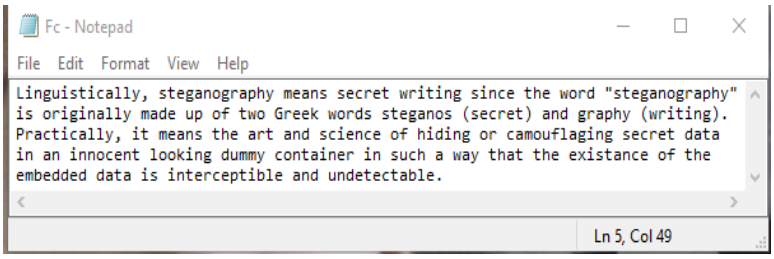

Figure 1. Cover text file (Fc.txt)

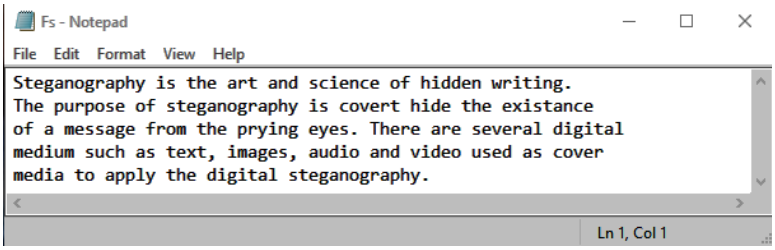

Figure 2. Secret text file (Fs.txt)

Step 2: Compute number of characters in secret text file (Fs) and cover text file (Fc).
Number of characters in secret text file (Fs)=279
Number of characters in cover text file (Fc)=318
Step 3: Check if number of characters in cover text file (Fc) is greater than number of characters in secret text file (Fs), then continue to Step 4. Otherwise End.
Step 4: Convert secret text file (Fs) into ASCII format then into binary format.

1	83	1	1	0	1	0	0	1	1
2	116	2	1	1	1	0	1	0	0
3	101	3	1	1	0	0	1	0	1
4	103	4	1	1	0	0	1	1	1
5	97	5	1	1	0	0	0	0	1
6	110	6	1	1	0	1	1	1	0
7	111	7	1	1	0	1	1	1	1
8	103	8	1	1	0	0	1	1	1
9	114	9	1	1	1	0	0	1	0
10	97	10	1	1	0	0	0	0	1

Figure 3. ASCII and binary format of Secret text file (Fs.txt)

Step 5: For all rows i= 1 to rows_of_Fs repeat steps 5 to 7
Step 6: For all columns j=1 to 7
Step 7: If Fs[i][j] is equal to 0 then
Save random even number between 1 and 10 in matrix of locations (Mol).
Otherwise, if Fs[i][j] is equal to 1 then
Save random odd number between 1 and 10 in matrix of locations (Mol).

1	3	2	5	4	6	3	5
2	5	3	7	2	7	4	6
3	9	5	4	6	9	4	3
4	7	7	6	4	7	5	5
5	5	9	4	8	4	6	7
6	7	5	2	7	5	7	4
7	3	5	4	5	3	9	7
8	3	7	8	4	7	5	9
9	5	3	7	6	4	5	2
10	5	9	2	2	6	4	3

Figure 4. Matrix of locations(Mol)

Step 8: Display message “Secret data file has been embedded successfully”.
Step 9: Upload cover text file and matrix of locations(Mol) to the security channels (SaaS).
Step 10: End.

3.2. Proposed Algorithm for Extracting
Input: Cover text file(Fc), matrix of locations(Mol)
Output: Secret text file (Fs)
Step 1: Read cover text file (Fc) and matrix of locations (Mol).
Step 2: For all rows i= 1 to length_of_Mol repeat steps 3 and 4
Step 3: For all columns j=1 to 7
Step 4: If Mol[i][j] is an odd number then
Save 0 in extract_matrix.
Otherwise, if Mol[i][j] is an even number then
Save 1 in extract_matrix.
Step 5: Convert extract_matrix from binary to ASCII format.
Step 6: Convert ASCII format into character format.
Step 7: Display secret text file (Fs).
Step 8: End.

IV. CONCLUSIONS.

Cloud Computing is considered a new paradigm in the Information Technology. It is necessary to secure the data stored by user on the cloud. This study proposed a new method to secure data storage on cloud computing by hiding one file into another file. There are several advantages for this method. Users can hide data without producing any distortion in the cover file. It can improve the security of stored data in cloud computing.

V. REFERENCES

[1] Gartner Inc Gartner identifies the top 10 strategic technologies for 2011. Online available: http://www.gartner.com/it/page.jsd?id=1454221
[2] Zhao, Gansen, et al. “Cloud computing: A statistics aspect of users”, IEEE International Conference on Cloud Computing, Springer Berlin Heidelberg, 2009.
[3] Zhang, Shuai, et al. “Cloud computing research and development trend”, Future Networks, 2010. ICFN’10 , IEEE Second International conference, 2010.

[4] S. Mathew, and T.Anuradha, "Security for cloud computing using steganography", International Journal of Computer Enggineering and Applications, Vol. XI, No. VI, pp.1-7, 2017.
[5] S. U. Khurana , A.N. Verma , " Comaparisons of cloud computing service models: SaaS, PaaS, IaaS", IJECT, Vol. IV, No. Spl-III, 2013.
[6] C. Cachin, " An information- theoretic model for Steganography", Proceedings of 2nd Workshop on Information hiding, MIT Laboratory for computer science, 1998.
[7] Sagumaran, M. B. B. Murugan, D. Kamalraj, "an architecture for data security in cloud computing", World Congress on Computing and Communication technologies (WCCCT), 2014.
[8] P. Kumar, and Padmapriya, "Data puncturing in OFDM channel: A multicarrier stego", Information Technology Journal 13.12, 2014.
[9] M. R. K. A. Sarkar, T. R. Chatterjee, "Enhancing data stroage security in cloud computing through Steganography", ACEEE International Journal on Network Security, Vol. V, No. I, 2014.
[10] S. A. Garima, and S. H. Naveen, "Triple security of data in cloud computing ", International Journal of computer Science and Mobile Computing, Vol. V, No. IV, 2014, pp.5825-5827.
[11] H. A. Karun, SI Uma, "Data security in cloud computing using encryption and steganography", International Journal of Computer Science and Mobile Computing, Vol. IV, No. V, pp.786-791, 2015.
[12] W. A. Awadh, A. S. Hashim, "Using steganography for secure data storage in cloud computing", International research Journal of Engineering and Technology, Vol. IV, No. IV, pp.3668-3672, 2017.