Using Steganography for Secure Data Storage in Cloud Computing

Wid A. Awadh[1], Ali S. Hashim[2]

[1] *College of Computer Science and Information Technology, Iraq*

[2] *College of Computer Science and Information Technology, Iraq*

---***---

Abstract - *Cloud computing is one of the popular method of accessing shared and dynamically configurable resources via the computer network on demand. The secure data storage on cloud environments is the primary requirement of such applications, where data are being transferred or transmitted between the servers and their users. One of the most effective techniques for secure communicating is steganography in cloud. The steganography refers to the method of writing hidden messages in a manner that no one other person but sender and receiver would be able to securely understand and communicate the information hidden in the means of communications. To ensure security of data in cloud computing, this paper presents a new text steganography approach for hide loaded secret English text file in a cover English text file. The proposed approach improved data security, data hiding capacity, and time.*

Key Words*:* Cloud computing, Steganography, A matrix of location, Data security.

1. INTRODUCTION

1.1 Cloud Computing

Cloud computing is considered as a new paradigm in the Information Technology (IT) that has originated in 2007 [1]. It is a result of innovations in Internet technologies, hardware technologies, systems management, and distributed computing [2]. It is a dynamic technology platform that addresses a wide range of needs by providing cyber-infrastructure to maintain and extend information storage capabilities. In addition, cloud computing provides access to software and hardware without large capital investment and provides easier access to applications and services that can be realized with minimal service provider interaction [3]. This has enabled cloud computing to develop as a technological innovation that can handle large amounts of information that are transferred and stored via electronic applications [4].

Cloud computing researchers have divided cloud computing into three layers. First: Infrastructure as a Service (IaaS), in this 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 provides all the facilities as in (IaaS) but also provides operating system facilities, their updates, etc. hence make the overall work quite easy. 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 moreover 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. Many companies are using and providing these services this include for example Google Apps [5]. Figure1 shows the structure of cloud computing layers.

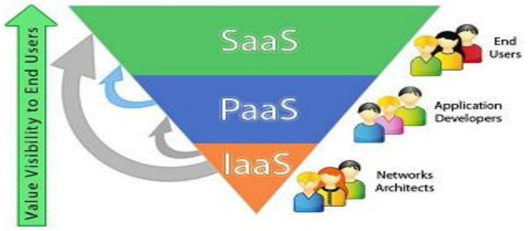
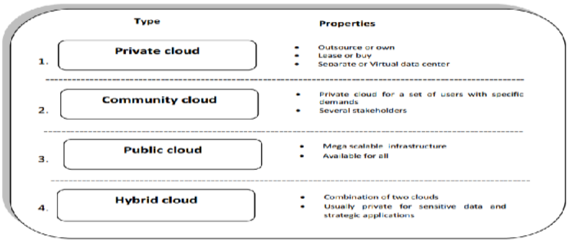


Fig-1: Structure of cloud computing-services [6]

Most researches classify the deployment approaches of cloud computing into four main categories which are; Public, Private, community, and Hybrid [7] [8]. Public cloud are cheap and accessible but less secure than private. Whereas, the hybrid mixed between the affordability and the high security. Whereas, community cloud is an integration between some organization to use the cloud technology [8] [9] [10]. Each deployment model has its benefits and drawbacks. The decision of choosing a proper cloud computing deployment model should consider technological as well as organizational factors [10]. Figure 2 presented the approaches of cloud computing deployments.



	Type	Properties
1.	Private cloud	• Outsource or own • Lease or buy • Separate or Virtual data center
2.	Community cloud	• Private cloud for a set of users with specific demands • Several stakeholders
3.	Public cloud	• Mega scalable infrastructure • Available for all
4.	Hybrid cloud	• Combination of two clouds • Usually private for sensitive data and strategic applications

Fig- 2: Approaches in cloud deployment [11]

1.2 Security of Cloud Computing

Cloud computing naturally raises new challenging security threats for many reasons [12]:

1- Traditional encryption basics for protection of data security cannot be directly adhered because the control of data is lost by users under Cloud Computing. Considering different data per user stored in the cloud and the demand of continuous data security certainly, the problem of data storage validation in cloud becomes more challenging.
2- Data stored in the cloud may be frequently updated by the users, which include deletion, insertion, appending, modifying, reordering, etc. To ensure authenticity of storage for updating of dynamic data is of much importance.
3- The evolution of Cloud Computing is done through data centre's running simultaneously, with collaboration and in distributed manner.

1.3 Steganography in Cloud Computing

Computer application in real life is increasing every day. Therefore, the need to data security is becoming more and more essential part of message or data transfer. So, information security became a part of our daily life. Among the different techniques, hidden exchange of information is a concerns in the area of information security. Various methods like cryptography, steganography, coding and so on have been used for this purpose. However, in recent years, steganography has attracted more attention [13].

Steganography techniques can be used to provide an excellent tool for data exfiltration, to enable network attacks or hidden communication among secret parties. The aim of these techniques is to hide secret data (steganograms) in the innocent looking carrier e.g. in normal transmissions of users [14].

The word "steganography" is of Greek origin and means "concealed writing" from the Greek words "steganos" meaning "covered or protected", and "graphein" meaning "to write". Steganography works have been carried out on different medium such as images, video clips, text and sounds [15]. There are three important parameters in the design of the methods of steganography: perceptual transparency, robustness and hiding capacity. These requirements are known as "the magic triangle" [16].

The best carrier for steganograms must have two features: it should be popular i.e. usage such carrier should not be considered as an anomaly itself and modification of the carrier related to inserting the steganogram should not be "visible" to third party not aware of the steganographic procedure [17]. And how to find a carrier that would fill abovementioned requirements? In the Internet today we are witnessing an expansion of various, advanced Internet services from which more and more are migrating to abovementioned cloud computing services. The major cloud service providers are significantly investing in their infrastructure and in acquiring customers, big players list include: Google (Gmail, GoogleDoc), Microsoft (Azure), Amazon (Amazon Web Services), Cisco (WebEx). These services sometimes use complex protocols and infrastructures to achieve their goals. Thus, they are good candidates for secret data carriers [18].

2. RELATED WORK

1. Enhancing Data Storage Security in Cloud Computing through Steganography [19]:

   Here the authors provide a very solid technique of maintaining the integrity of data. In this model, the data being sent to server is saved behind the images. Thus, the unauthorized access cannot perceive the data as it is hidden. The proposed model makes use of steganography using images for protecting the integrity of data which is a very good approach however, the security of data during transmission is not handled at all. Hence, even though it's a very unique approach but could have been much better if integrity and confidentiality of data can be handled while uploading to cloud server.

2. Triple Security of Data in Cloud Computing [20]:

   In this paper the authors provide security of data in cloud computing by combining three algorithms, first: apply DSA (Digital signature algorithm) for verification and authentication of data. Then apply AES (Advanced Encryption Standard) algorithm for encryption of data and Steganography to hide data within audio file for provide maximum security to the data. This model satisfies both authenticity, security but the time complexity is high because it is a one by one process.

3. Data Security in Cloud Computing using Encryption and Steganography[21]:

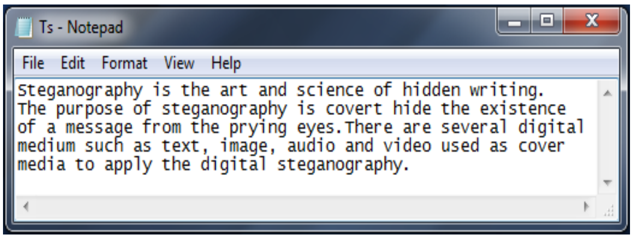
   In this paper authors provide hiding algorithm is used to save the files or data behind the images. In this algorithm the user selects the data to be uploaded and encrypted it using a strong algorithm such as AES algorithm. The encrypted data is then uploaded to server. On receiving data, one which came from user side a hiding algorithm is applied which randomly selects the bits positions from images where data is to be stored.

3. PROPOSED STEGANOGRAPHY IN CLOUD COMPUTING

3.1 Proposed Algorithm for Embedding :-

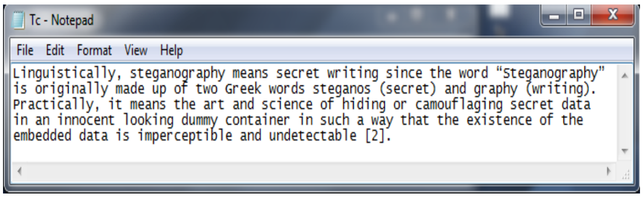
Input: A secret text file (Ts), cover text file (Tc).
Output: A matrix of location (Lom).

Step1: Select the secret text file (Ts) and the cover text file (Tc) to be uploaded.



```
Steganography is the art and science of hidden writing.
The purpose of steganography is covert hide the existence
of a message from the prying eyes.There are several digital
medium such as text, image, audio and video used as cover
media to apply the digital steganography.
```

Fig-3: Secret text file (Ts.txt)



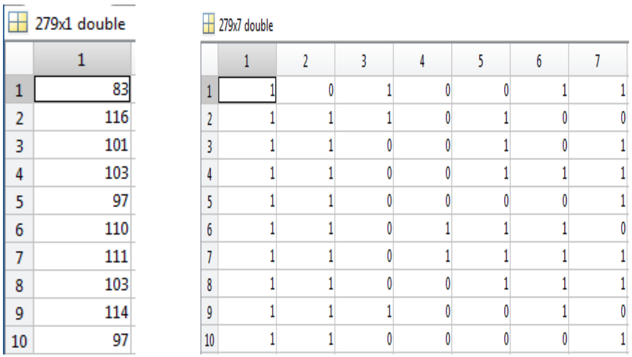
```
Linguistically, steganography means secret writing since the word “Steganography”
is originally made up of two Greek words steganos (secret) and graphy (writing).
Practically, it means the art and science of hiding or camouflaging secret data
in an innocent looking dummy container in such a way that the existence of the
embedded data is imperceptible and undetectable [2].
```

Fig-4: Cover text file (Tc.txt)

Step2: Compute the number of characters in the secret text file (Ts) and the cover text file (Tc).

Number of characters in secret text file (Ts) =279
Number of characters in cover text file (Tc) =318

Step3: Check if the number of characters in the cover text file (Tc) greater than the number of characters in the secret text file(Ts), if condition is true continue to step 4, otherwise, go to step11.
Step4: Conversion of the secret text file (Ts) and the cover text file (Tc) into ASCII value and then into binary format.



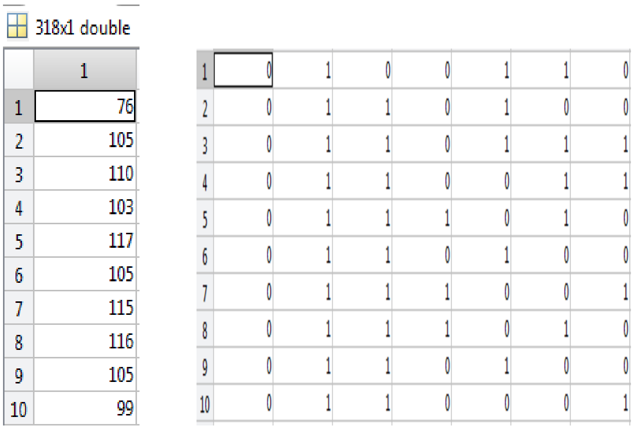
279x1 double

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

279x7 double

	1	2	3	4	5	6	7
1	1	0	1	0	0	1	1
2	1	1	1	0	1	0	0
3	1	1	0	0	1	0	1
4	1	1	0	0	1	1	1
5	1	1	0	0	0	0	1
6	1	1	0	1	1	1	0
7	1	1	0	1	1	1	1
8	1	1	0	0	1	1	1
9	1	1	1	0	0	1	0
10	1	1	0	0	0	0	1

Fig-5: ASCII and Binary format of the secret text file (Ts)



318x1 double

	1
1	76
2	105
3	110
4	103
5	117
6	105
7	115
8	116
9	105
10	99

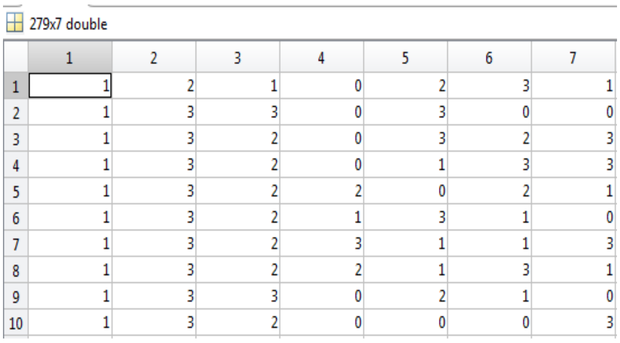
1	0	1	0	0	1	1	0
2	0	1	1	0	1	0	0
3	0	1	1	0	1	1	1
4	0	1	1	0	0	1	1
5	0	1	1	1	0	1	0
6	0	1	1	0	1	0	0
7	0	1	1	1	0	0	1
8	0	1	1	1	0	1	0
9	0	1	1	0	1	0	0
10	0	1	1	0	0	0	1

Fig-6: ASCII and Binary format of the cover text file (Tc)

Step5: For all i=1 to 7 repeat steps 5 to 9
Step6: For j=1 to rows_of_cover_text_file
Step7: Matching the bits of the cover text file (Tc) with the bits of the secret text file (Ts) is performed.

- If bit of cover text file (Tc) =0 and bit of secret text file (Ts) =0 then save the number of zero in matrix of locations (Lom).
- If bit of cover text file (Tc) =0 and bit of secret text file (Ts) =1 then save the number of one in matrix of locations (Lom).
- If bit of cover text file (Tc) =1 and bit of secret text file (Ts) =0 then save the number of tow in matrix of locations (Lom).
- If bit of cover text file (Tc) =1 and bit of secret text file (Ts) =1 then save the number of three in matrix of locations (Lom) of dimensionality n rows and 7 column.

//n is the number of the characters in secret text file (Ts).
// resulting is the locations of matrix (Lom). Save the dimensions a matrix of location (Lom) in variable m x n.



279x7 double

	1	2	3	4	5	6	7
1	1	2	1	0	2	3	1
2	1	3	3	0	3	0	0
3	1	3	2	0	3	2	3
4	1	3	2	0	1	3	3
5	1	3	2	2	0	2	1
6	1	3	2	1	3	1	0
7	1	3	2	3	1	1	3
8	1	3	2	2	1	3	1
9	1	3	3	0	2	1	0
10	1	3	2	0	0	0	3

Fig-7: The matrix of locations (Lom)

Step8: Increase the value of location and count variable by 1.
// Count variable is used to check whether complete data has been hidden or not.

Step9: If count variable is equal to the number of the characters in secret text file. Then message displays "Secret data file has been embedded successfully" and then uploaded to server, go to step 11.
Step10: Else message displays "Text has not been embedded, Size of the cover text file is small".
Step11: Upload the cover text file and a matrix of location to the security channel (SaaS), End.

3.2 Proposed Algorithm for Extracting :-

Input: Cover text file (Tc), a matrix of location (Lom).
Output: Secret text file (Ts).

Step 1: Read the cover text file (Tc), and a matrix of location (Lom).
Step 2: Conversion of cover text file (TC) into ASCII and then into binary format.
Step 3: Calculate the length of a matrix of location (Lom).
Step4: For all i=1 to 7 repeat steps 5 to 6
Step5: For j=1 to length of a matrix of location (Lom).
Step 6: Match the values of matrix of locations (L0S) and the matrix of cover text.

- If bit of cover text file (Tc) =0 and bit of matrix of locations (Lom)=0 then save the number of zero in extract_matrix (Eom).
- If bit of cover text file (Tc) =0 and bit of matrix of locations (Lom)=1 then save the number of one in extract_matrix (Eom).
- If bit of cover text file (Tc) =1 and bit of matrix of locations (Lom)=2 then save the number of zero in extract_matrix (Eom).
- If bit of cover text file (Tc) =1 and bit of matrix of locations (Lom)=3 then save the number of one in extract_matrix (Eom).

//extract_matrix (Eom) containing secret text has been created in binary format
Step 7: Increase the value of location and count variable by 1.
Step 8: Conversion of the extract_matrix (Eom) from binary to ASCII format.
Step 9: Conversion of ASCII format to character format.
Step 10: Display the secret text (Ts).
Step11: End.

4. CONCLUSIONS

Due to increasing development of internet technology; it is necessary to secure the data stored by user on the cloud and maintain their confidentiality. So, this study proposed a new approach to secure data storage on cloud computing by hide secret English text file in cover English text file by generating a matrix of location. There are several advantages for this method. Firstly, proposed approach improves the data hiding capacity. Secondly, users can hide more amount of data without producing any distortion in the cover text file that means changes reflected are almost negligible. On the other hand, can improve the security of proposed method by encryption a matrix of location and can be applied to any language.

REFERENCES

[1] US Nasir & MH Niazi, (2011). "Cloud computing adoption assessment model (CAAM)". Proceedings of the 12th International Conference on Product Focused Software Development and Process Improvement (pp. 34-37). ACM.

[2] RA Buyya, CH Yeo, SR Venugopal, IV Brandic & JA Broberg. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), 599-616.

[3] BE Yuan, CH Yang, & BA Hwang (2012). "Key consideration factors of adopting cloud computing for science". In Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 597-600). IEEE Computer Society.

[4] FR Leymann & et al. (2011). Moving applications to the cloud: an approach based on application model enrichment. International Journal of Cooperative Information Systems, 20(03), 307-356.

[5] SU Khurana & AN Verma. (2013). Comparison of Cloud Computing Service Models: SaaS, PaaS, Iaas, IJECT Vol. 4, Issue Spl-3. ISSN: 2230-7109 (Online) | ISSN: 2230-9543(Print).

[6] RE Boksebeld. (2010). The Impact of Cloud Computing on Enterprise Architecture and Project Success. Apeldoorn: Hogeschool Utrecht Faculty Science and Engineering.

[7] PE Mell & TI Grance. (2011). The NIST Definition of Cloud Computing, Recommendation of the National Institute of Standards and Technology.

[8] JI WO Lian, DA C.Yen, & YE TI Wang (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. International Journal of Information Management, 34(1), 28-36.

[9] B Gustafsson & A Orrgren. (2012). Cloud Computing: the adoption of cloud computing for small and medium enterprises. Jonkoping international business school. Jonkoping University.

[10] QI Zhang, LU Cheng & RA Boutaba (2010). Cloud Computing: state-of-the- art and research challenges. Journal of internet services and application. 7-18.

[11] Nilsvold. (2012). Cloud basics–Deployment models. Retrieved April 26, 2015, from:http://blog.visma.com/singletesting/2012/03/12/cloud-basics-deployment-models.

[12] NA Garg & KA Kaur. (2016). Hybrid information security model for cloud storage systems using hybrid data security scheme. International Research Journal of Engineering and Technology (IRJET). Vol, 03 Issue: 04.

[13] AL Saber & WI Awadh. (2012). A New Text Steganography Method by Using Non-Printing Unicode Characters and Unicode System Characteristics in English/Arabic documents. J.Thi-Qar Sci. Vol.3 (3). ISSN 1991-8690.

[14] MA Wojciech & SZ Krzysztof (2011). Is cloud computing steganography-proof. IEEE.

[15] UD Kamred (2014). A Steganography Technique for Hiding Information in Image. International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS). ISSN (Print): 2279-0047 ISSN (Online): 2279-0055.

[16] AR Malik, GE Sikka, & HA K. Verma (2016). A high capacity text steganography scheme based on LZW compression and color coding. Engineering Science and Technology,an International Journal.

[17] Vaishali & AN Goyal. (2014). An Implementation of 4 Bit Image Steganography for Data Security in Clouds. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 11.

[18] TA Ahamad & AB Aljumah. (2014). Cloud Computing and Steganography Attack Threat Relation. MAGNT Research Report (ISSN. 1444-8939). Vol.2 (4), 72-75.

[19] MR KA Sarkar & TR Chatterjee. (2014). Enhancing Data Storage Security in Cloud Computing Through Steganography. ACEEE Int. J. on Network Security, Vol. 5, No. 1.

[20] SA Garima & SH Naveen. (2014). Triple Security of Data in Cloud Computing. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4), 5825-5827.

[21] HA Karun & SI Uma. (2015). Data Security in Cloud Computing using Encryption and Steganography. International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, 786-791.