ADD ON SECURITY WITH STEGANOGRAPHY IN CLOUD

K.MONICA[1], T.RAMARAO[2] ,CH.ASHOK[3]
Assistant Professor[1], Assistant Professor[2,] Assistant Professor[3]
Department of CSE,
Godavari Institute of Engineering & Technology, Rajahmundry, India

Abstract: Cloud computing is considered as the emerging and ever green technology in the field of computers.With the introduction and usage of cloud computing many institutions and organizations started transactions of data over cloud.As now a days information is being safeguarded as wealth,there is a minut doubt in the mind of both customers and organizations that whether their data or information in safe or not? Though it provided many services to the customers it cannot erase the doubt which arose in their minds.For that many technics and algorithms are used to clear the doubt but it would be better enough to provide additional security to the already secured data.This can be achieved by steganography which is an art of hiding crucial data in any image or multimedia.So this paper gives an overview of the security measures provided by steganography to the data which is being safeguarded in cloud.This is done by using to texts namely Data and cover text.

Keywords: Cloud computing, Steganography, Data security, matrix of location, English text or data, Cover text.

1. INTRODUCTION:

1.1 Cloud Computing:

With the introduction of Cloud computing in computer technology people and organizations of all size started relying mostly on the services provided by cloud with a click without the pain of standing in longer queues and in many of the daily routines. It started providing services like updation of softwares in institutions with pay per usage strategy which reduced the overhead of regular updation of versions. Even schools are depending on cloud by downloading information and uploading vital information.

Cloud developers or experts categorized the services into three types namely

- Infrastructure As A Service (IaaS)
- Platform As A Service (PaaS)
- Software As A Service (SaaS)

Fig 1. Structure of Services of Cloud

Infrastructure as a Service is a technique the hardware resources such as hard disc, memory, network services are provided on demand (rent) and are charged as per usage.

The second technique is ***Platform as a service*** where it not only provides ***IaaS*** but also provides facilities of an operating system and their updates there by making the overall work easy. Generally the schools and colleges use this type of techniques for updating of labs softwares.The third and the last technique is Software as a Service(SaaS) where in it provides all the facilities included in both 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 [6]. Figure1 shows the structure of cloud computing layers.

Most researches classify the deployment approaches of cloud computing into four main categories which are; ***Public, Private, community, and Hybrid*** [8] [9]. Public cloud is 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 [9][11]. 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 [11]. Figure 2 presented the approaches of cloud computing deployments.

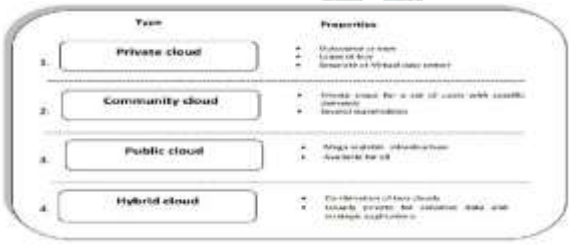

Fig.2. Deployment approaches in cloud

1.2 Security Issues of Cloud Computing:

Assume that while uploading details like bank accounts and some vital information, if the user forgets the secret key of the locker in a bank and if the assistant comes running towards him with a lock will that person trust that bank again? That scenario immediately blows his mind off isnt it? The same is with cloud the user may store data and may forgets the password sometimes but it should be mandatory that he should get back to access his account without any problem and at the same time the cloud should provide security from itself too. There are several security threats include:

- 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.
- 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 [14]. 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 [15]. 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 [16]. 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" [17]. 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 [18]. 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 [19]. This is the actual problem that every individual is dealing with now-a-days he should get easy access as well as his data must be secured and maintained confidentially. This is done with the help of steganography.

2 Literature Survey

1. *Using Steganography for Secure Data Storage in Cloud Computing*

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 , it can improve the security of proposed method by encryption a matrix of location and can be applied to any language.

2. *Enhancing Data Storage Security in Cloud Computing through Steganography [20]*

*I*n this paper the author provides 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.

3. *Triple Security of Data in Cloud Computing [21]:*

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.. PROPOSED ALGORITHM

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.

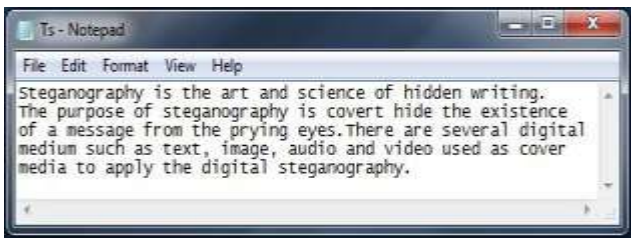

Fig-3: Secret text file (Ts.txt)

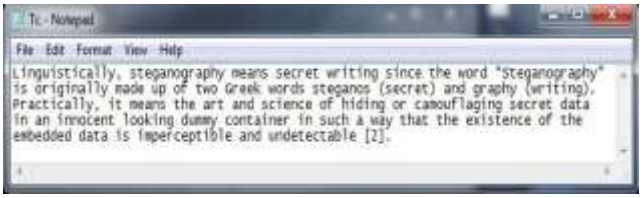

Fig-4: Cover text file (Tc.txt)

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	1	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

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.

5. REFERENCES

[1] Wid A. Awadh, Ali S. Hashim "Using steganography for secure data storage in cloud" International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 04 | Apr -2017

[2]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.

[3] 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.

[4] 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.

[5] 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.

[6]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)

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

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

[9]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.

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

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

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

[13]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.

[14] AL Saber & WI Awadh. (2012). A New Text Steganography Method by Using Non-Printing Unicode Characters and Unicode System characteristics in English/Arabic documents.
[15]MA Wojciech & SZ Krzysztof (2011). Is cloud computing steganography-proof. IEEE.

[16] 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.

[17] 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.

[18]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.

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

[20]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.

[21]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.

[22]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.