International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 09 | Sep -2016 www.irjet.net p-ISSN: 2395-0072

A Novel Technique to Secure Cloud Data using Steganography

Ganavi M[1], Suma N Dilliwala[2]

[1]*Assistant Professor, Department of CS&E, Jawaharlal Nehru National College of Engineering, Shivamogga, Karnataka, India*

[2]*M.Tech Student, Department of CS&E, Jawaharlal Nehru National College of Engineering, Shivamogga, Karnataka, India*

Abstract - *Cloud computing offers the on demand computational infrastructure to the users which has the potential to decrease the huge cost to build IT based services. It can provide ubiquitous, convenient data storage facility. It is a significant issue as the whole data stored to a set of interconnected resource pools which are situated over different location of the world. Stored data can be accessed through virtual machines by unauthorized users. There are different types of security and privacy challenges that are required to analyze and take care. To ensure privacy and security of data in cloud computing, here proposed a new data hiding technique called Steganographic Approach using Huffman Coding (SAHC) which ensures data security in cloud computing during data-at-rest. Objective is to prevent data access by unauthorized users from cloud storage. The main idea is to develop a steganographic technique to secure cloud data.*

Key Words: **SAHC, CSP, EC2, S3**

1.INTRODUCTION

Cloud computing is recognized like a model or replica of most recent innovation above the web or network which fulfill on interest administrations, for example, network, software, storage, resources. Despite the fact that readily available numerous services can be given to the customer by the cloud yet information accumulate in single fundamental features that the cloud administration supplier gives to the customers. In any case, various customers are not set up to realize distributed computing model as a result of the nonappearance or absence of legitimate means proper security framework in security of data. There are such an assortment of distributed computing dealers, for instance, Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Services (S3).

Steganography is the claim to fame of hiding information inside safe spread transporters covered message is undetectable. St-ego implies secured or secret-and "graphy" connotes "make" and in this manner, steganography gets the opportunity to be "secured or puzzle making". The major concern regarding security of data in cloud computing is that, as data are available in remote servers in raw format. So, it can be easily accessible and can be manipulate by unauthorized users. The main aim is to ensure data security in cloud storage such that it can't be detectable by any malicious users. Therefore the main idea is to develop a steganographic technique to secure cloud data. The proposed method achieves the cloud data storage security like data loss, data breaches, account hijacking, malicious insiders etc. by hiding the data in images instead of data storage in files, This is done by using three different Cloud Service Providers (CSP) to increase data security.

The main objectives of this proposed work are, to improve the security of data set away in cloud by utilizing Huffman coding, to give high embeddings efficiency, to give cloud security to data in cloud while embeddings and extraction of
secret data, to avoid redundant stockpiling of same data in the cloud along these lines improving storage space and cost of the cloud.

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section 2. Experimental results are presented in section 3. Concluding remarks are given in section 4.

2. PROPOSED ALGORITHM

To design the system set of requirements must be met by the
system. Implementation is the process of converting the system design into a practical approach. This chapter provides an insight on the design and implementation of the proposed "Ensuring Data Storage Security in Cloud computing using Steganography" system using flow charts and algorithms of the proposed system.

A. System architecture

In this engineering, there are distinctive elements which can
be recognized as appeared in fig 1.

User: Users are the one who have to to utilize cloud establishment.

- **Cloud Service Provider-1(CSP-1):** In the form picture data are secured here.
- **Cloud Service Provider-2(CSP-2):** Here both unscrambling and encryption frameworks are secured. This tool will hide data or information into the pictures and recoup those hidden information or data from those pictures.

- **Cloud Service Provider 3(CSP-3):** CSP-3 will interface with CSP-2 and CSP-2. By the clients or customer all the figuring's will be taken at this juncture.

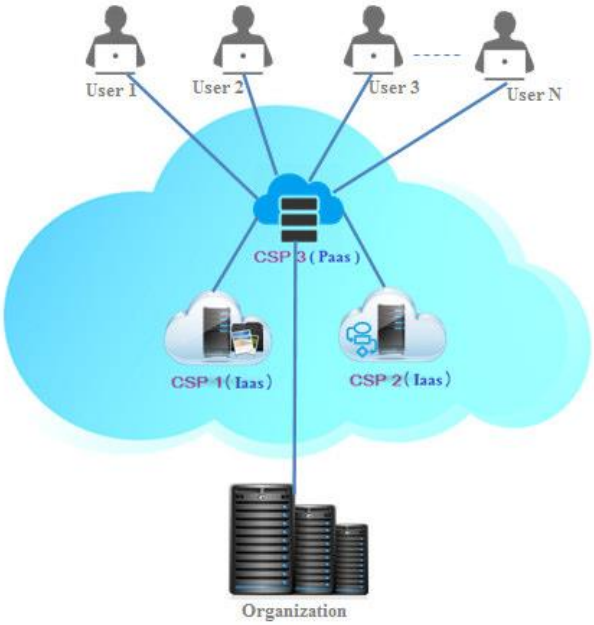

Fig 1. System architecture for cloud

B. Security Model

The data record is not securing physically. As opposed to securing data into a record, data is securing in a couple pictures. This thought is acknowledged as steganography which makes that disguise one part of message/data in such amanner that no one apart from the proposed recipient and sender relates the nearness with the message/data. Through uncertain quality this one is the new perspective of security. Case in point detach the entire record into 3 segments and each segment is secured into the looking at pictures fig 2. Depending upon the dgree of picture and data archive the division of record is done.

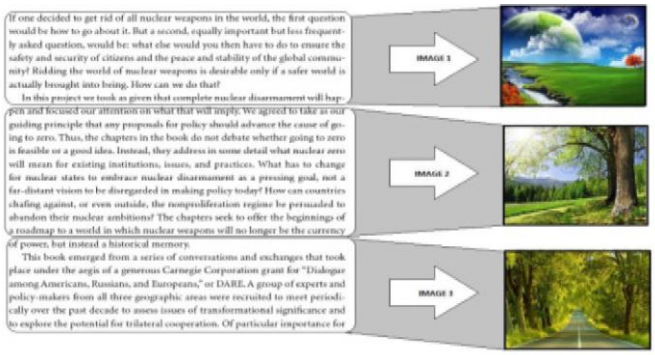

Fig 2. Hiding data into Images

C. Computation Model

In fig 3 and fig 4 the computation model is represented. In CSP-3 the evaluations or computations done by the users willtake place. To store the user data or information, the subsequent steps will take place:

1. For CSP-1, CSP-3 will ask for set of images.
2. By sending the required set of images to CSP-3 from CSP-1, CSP-3 will receives an acknowledge from CSP- 1.
3. For CSP-2, CSP-3 will ask for the data hiding algorithm which is stored in CSP-2.
4. After receiving a request from CSP-3, CSP-2 will launch data hiding algorithm to CSP-3.
5. For hiding the real/actual data steganographic technique will applied from CSP-3 and in the form images data will be saved.
6. At this moment to CSP-1 the images will be sent.

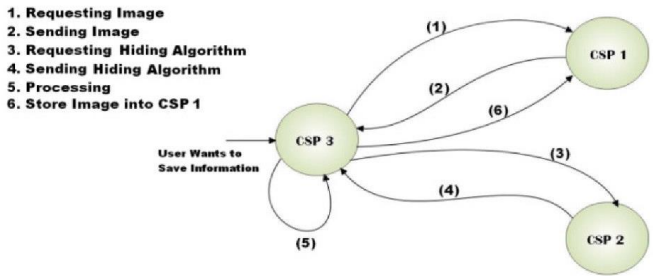

Fig 3. Computational model for to storing data

The subsequent procedure will be made at whatever time the user want to get back the data.

1. For CSP-1, CSP-3 asks for the set of images which contains the message or data.
2. CSP-1 sends set of images to CSP-3 along with acknowledgment.
3. For CSP-2, CSP-3 will ask for the data hiding algorithm which is stored in CSP-2.
4. After receiving a request from CSP-3, CSP-2 will launch data hiding algorithm to CSP-3.
5. At this moment, on images the retrieval algorithm will applied by CSP-3 and in a separate file the retrieved data will be stored.

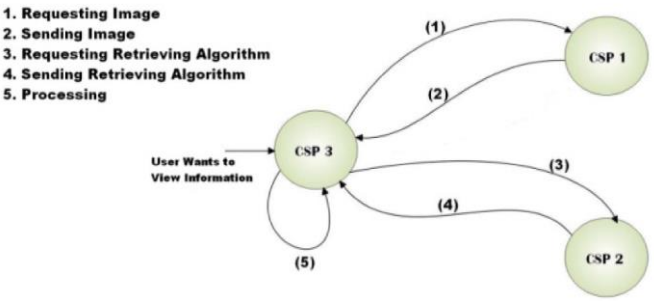

Fig 4. Computational model to retrieve data

To the user this file will be displayed. When the user want to logout from the system this temporary file will be removed.

3. EXPERIMENT AND RESULTS

In this section, the aftereffects of the task are portrayed with
the assistance of depictions. The task is completed utilizing
three cloud administration suppliers, spread picture and emit information. Different performances of the undertaking have been assessed.

Primary form is the primary UI of the undertaking and connections to a structure resemble enrollment structure, (cloud administration supplier) CSP1, CSP2 and CSP3 frames. This is appeared in fig 5.

Fig 5. Main form

Registration form is the enrollment structure for the new clients for entering the data like ID, secret key, versatile number, city, state, nation. By giving all these data client will
be enrolled. This is appeared in fig 6.

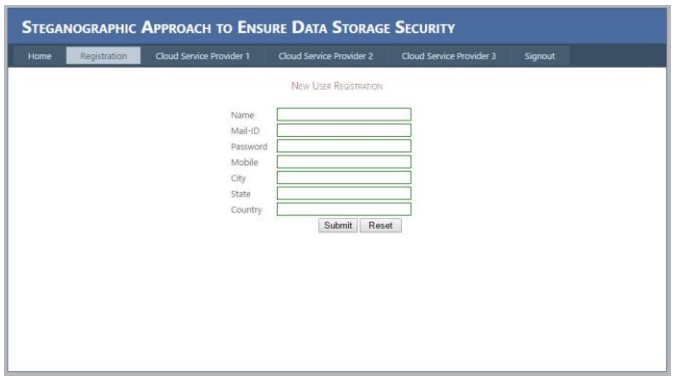

Fig 6. Registration form

Cloud Service Provider 1
To go into any of the CSP, need to login by giving ID and secret key. This CSP1 keeps up a portion of the structures like picture database, view pictures, steganographed pictures and extraction. This is appeared in fig 7.

Fig 7. Login form

Selecting Cover Image
This structure demonstrates that, a picture can be chosen from the picture database keeping in mind the end goal to shroud the information. In the wake of selecting a picture, it can be seen in the CSP1 as appeared in fig 8.

Fig 8 selecting image

The steganography procedure is done in cloud administration supplier 3. The stego picture is put away in CSP1, select catch is utilized to concentrate document from the picture. By giving secret key we can see the substance covered up in the image.If copy information happens it won't acknowledge with a specific end goal to decrease repetition. This is appeared in the fig 4.6, 4.7, 4.8 and 4.9.

Fig 9 Uploading data

CSP2 Form
Enterinto CSP2 by giving Id and secret key. In CSP2 the pressure and extraction calculation are put. CSP3 will prepare the steganography by taking picture from the CSP1 and coding from the CSP2 and procedure the steganography and handled stego picture is again put away in CSP1. This is appeared in fig 4.10 and 4.11.

Fig 10. Login page for CSP-2

CSP3 Form

By utilizing ID and secret key go into CSP3, This is the structure were we can transfer the information by picking the document. Subsequent to concealing information into picture, secret word is given for security reason. By giving secret key steganography procedure will finish. With a specific end goal to concentrate we require that watchword which is done in CSP1. Login page of CSP-3 looks similar to CSP-2.

Table 1 speaks to the spread picture used that is Hydranges.jpg and Jellyfish.jpg which are 256x256 and 125x125 in estimation independently. The estimation of PSNR (Peak- Signal-to-Noise-Ratio) and MSE (Mean Square Error) for changing word incorporate is depicted the going with table. Test results saw from the above table depicts that as the amount of words masked inside the spread picture extends, PSNR regard decreases and MSE regard increases.

*Table 1. PSNR and MSE values for image of 256*256*

Cover image Hydrenges			
Sl. No.	**No. of Words in secrete file**	**PSNR (dB)**	**MSE**
1	1	50.81	0.54
2	5	50.62	0.56
3	10	50.33	0.60
4	15	50.14	0.63
5	20	50.06	0.65

The above table 1 portrays that PSNR esteem expanding relies on upon the quantity of words disguising in the picture. For the above table hydrenges.jpg picture is utilized which is 256*256. The pixel of the picture matters for the estimation of PSNR and MSE.

*Table 2. PSNR and MSE values for image of 125*125*

Cover image Jellyfish			
Sl. No.	**No. of Words in secrete file**	**PSNR(dB)**	**MSE**
1	1	50.63	0.56
2	5	50.55	0.57
3	10	50.37	0.60
4	15	50.15	0.63
5	20	50.03	0.65

The above table 2 depicts that PSNR value increasing depends on the number of words concealing in the image. For the above table jellyfish.jpg image is used which is 125*125. The pixel of the image matters for the value of PSNR and MSE.

4. CONCLUSION

The focal reason for this anticipate that is will exhibit the security challenges that are occurring in cloud information stockpiling and present another joined encoding and information concealing strategy to avoid unapproved information access in cloud information stockpiling. Steganographic way to deal with oversee guarantee information stockpiling security in passed on figuring utilizing Huffman Coding (SAHC) is an able steganographic system for upgrading security of cloud information when it is still. Essentially store the information into pictures which is secured in the cloud information stockpiling. Unapproved clients can't right the essential substance of the information as a consequence of HVS. Through unequivocal security
examination it is displayed that this framework gives high security of information when it is on rest in the server residence of any CSP.

Steganography however is still a genuinely new thought, there are steady headways in the PC field, proposing progressions in the field of steganography also. It is likely that there will soon be more effective and more propelled strategies for Steganalysis. In future different change strategies can be utilized to shroud the emit information safely in the cloud. The proposed procedure can be improved to implant.

REFERENCES

[1] Con Wang, Qian Wang, Kui Ren, and Wenjng Lou, "Guaranteeing Data Storage Security in Cloud Computing",17th International workshop on Quality of administration, USA, pp1-9, 2009.

[2] B.P Rimal, Choi Eunmi,I.Lumb, "A Taxonomy andSurveyof Cloud Computing Sytem",

JointConference on INC, IMS and IDC, pp.44-51,Seoul,Aug, 2009.

[3] H Shacham and B. Waters, "Smaller Proofs of Retrievability", Proc. of AsiacryptDec. 2008.

[4] K. D. Nooks, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage", Cryptology ePrint Archive, 2008.

[5] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files", Proc. of CCS '07, pp. 584– 597, 2007.

[6] Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing ", Journal of Network and Computer Application, vol. 34, issue 4, pp 1113- 1122, Academic Press td London, UK, July 2011.

[7] M. A. Shah, M. Pastry specialist, J. C. Head honcho, and R. Swaminathan, "Examining to Keep Online Storage Services Honest", Proc. eleventh USENIX Workshop on Hot Topics in Operating Systems, pp. 1–6, 2007.

[8] T. J. Schwarz and E. L. Mill operator, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage", Proc. of International Conference on Distributed Computing Systems, pp. 12–12, 2006.

[9] G. Ateniese, R. Smolders, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Tune, "Provable Data Possession at Untrusted Stores", Proc. Bureau Committee on Security, pp. 598–609, 2007.

[10] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, Scalable and Efficient Provable Data Possession", Proc. of Secure Comm, pp. 1–10, 2008.

[11] R. Curtmola, O. Khan, R. Smolders, and G. Ateniese, "MRPDP: Multiple-Replica Provable Data Possession", Proc.ofInternational Conference on Distributed Computing Systems, pp. 411–420, 2008.

[12] D.Nirmal Dev, K.Sakthivel, "Triple Encryption Method on Password for Secured Cloud Data Storage in Mobile" Proceedings of Second International Conference on Advanced Computing and Communication Technologies, IEEE Conference Publications, pp 309 – 313, 2010.

[13] M. F. Tolba, M. A. Ghonemy, I. A. Taha, A. S. Khalifa, "Utilizing Integer Wavelet Transforms as a part of Colored Image-Stegnography", International Journal on Intelligent Cooperative Information Systems, Volume 4, pp. 75-85.2012.

[14] Xie, Qing.,Xie, Jianquan., Xiao, Yunhua. "A High Capacity Information Hiding Algorithm in Color Image", Proceedings of second International Conference on EBusiness and Information System Security, IEEE Conference Publications, pp 1-4, 2011.

[15] M. Satyanarayan "A Cloudlet Architecture" Proceedings of fourteenth International Conference on Computer and Information Technology, IEEE Conference Publications, pp 286 – 291, 2010.