A SURVEY: AN APPROACH TO SECURELY SHARE INFORMATIONIN CLOUD USING STEGANOGRAPHY TECHNIQUE

[1]Trupti Patel, [2] juikhamar
[1] M. Tech Student, [2]Assistant Professor,
[1] Department of Computer Engineering, MEC, Basna. India.
[2] Department of Computer Engineering, MEC, Basna. India.
[1]truptipatel8253@gmail.com,[2]juiakhamar@gmail.com

Abstract - In recent years, cloud computing services have become a must in our daily lives. Cloud computing is a hub of various server and many database to store data. cloud computing provide many services to user which is reliable ,efficient and low cost. As it is internet based technology security becomes a big issue to the cloud data. Due to storing data on cloud there is an issue of data security, integrity and confidentiality. The main problem is that existing systems and/or programs usually have some unknown issues and can be attacked by some unauthorized persons in some unexpected ways. To solve the problem, at least partially, we have proposed a new steganography protocol for improving information security in cloud storage services. Initial analysis shows that the new protocol is very secure. This paper formulates the protocol in a more formal way, so that based on the formulation, we can find possible weak points more easily, and make the protocol more practically useful.

Index Terms - Cloud computing,Confidentiality , Integrity,Security,Steganography

I. INTRODUCTION

Cloud computing service (CCS) [5] is becoming one of the most important factors in our daily lives. With CCS, we can use a large number of applications via portable computing devices (PCDs) or personal computers. Cloud storage service (CSS) is a special form of CCS. With CSS, we can store various data in the CSS servers for free via public networks, and access the data anywhere and anytime. Due to storing data on cloud there is an issue of data security and confidentiality. To provide security to the user's data one can encrypt the file and send it to cloud. Also integrity is another major challenge in outsourcing data to the cloud. To protect the system as well as the data, CSS systems must employ some well-known security methods. However, the security of existing systems is far from enough. The main problem is that existing systems, programs, and even security methods, may have some unknown issues and can be attacked by some unauthorized persons in some unexpected ways. One method for improving security is to use steganography which tries to conceal the existence of secret data. In this paper, we study the possibility of using the proposed technology to improving the security of CSS systems.
The rest of the paper is organized as follows. Section 2 illustrates Survey on various securityproposals on storage correctness approaches available with their pros and cons. Section 3contains overall comparison among all these approaches followed by conclusion in Section 4.Last section contains the list of references used.

II. LITERATURE SURVEY

Authors of [5] proposed a new steganography technology based on image morphing. In the proposed technology, an image is synthesized via image morphing, and is then used as the encryption key, the stego-key, as well as the cover data. Thus, it is a very important information, and should be protected very strictly. There are at least two factors that effect the security of the synthesized image. The first one is the security of the transmission channel, and the second one is the authentication between the client C and the cover image generating server Sc. As for user authentication between C and Sc, Author using conventional one-factor (password only)

authentication now. However, this can be easily broken by third party. In this case, the third party may obtain the synthesized images, and can obtain any information from the public storage server.

Authors of [6] proposed a new steganography technology base Author use LSB Technique.The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. We emphasize strongly on image Steganography providing a strong focus on the LSB techniques in image Steganography. This paper explains the LSB embedding technique and presents the evaluation results for 2,4,6 Least significant bits for a .png file and a .bmp file.

Authors of [7] use mutual authentication where the user and cloud server can authenticate one another. The protocol is designed in such a way that it uses steganography as an additional encryption scheme. The scheme achieves authentication using secret sharing. Secret sharing allows a part of the secret to be kept in both sides which when combined becomes the complete secret. The proposed protocol can resist many popular attacks such as replay attack, man in the middle attack, and denial of service attack.

Authors of [12] proposes a new Protocol Steganography with encryption.This paper deals with data security issues related to cloud computing so that data centres can provide a good environment to keep data. This scheme revolves around the problem of data security and with the help of encryption at client side and steganography at server side provides a highly secure model that will not only solve the issue of data safety but also simple in its implementation and hence usage. As per now the above mentioned scheme has been implemented using java. In future, the technique of image compression would be added to improve storage.

Authors of [8] introduce a mechanism to provide secure data. Authors combine three algorithm DSA(Digital signature Algorithm),DES(Data Encryption Standard) and Steganography to provide maximum security in cloud computing. By implementing these three algorithm it provide authenticity, security and data integrity to tha data. Author find that the Time complexity is high because it is a one by one process but in future this time complexity could be reduced.

III. COMPARISON OF VARIOUS RESEARCH SCHEMES

The table below shows a short comparison about the various schemes proposed by a researcherby taking different parameters. The table gives the description about the basic technique usedwith the benefits that researcher gets as well as the limitations found in schemes.

CriteriaGroup →	**Encryption/Steganography oriented measures**						**Others**	
Individual Criteria → Providers ↓	**Encryption**	**cryptography**	**Authentication**	**steganography**	**integrity**	**Hash based tech. used ?**	**Flexible security options**	**Algo/Flowchart shown ?**
[4]	X	X	X	√	√	X	X	√
[5]	√	X	√	√	X	X	X	√
[6]	X	√	X	√	X	√	X	X
[7]	√	X	√	√	X	X	X	√
[8]	X	X	√	√	√	X	X	√
[12]	√	X	X	√	√	X	X	√

Table-1: Comparative Study

IV. CONCLUSIONS

This proposed System presented a model for secret sharing data over Cloud environment securely. The proposed method introduces a new way of secret sharing and has potential of hiding a large message. Owner can share the data with only important user. The user can ask for sharing of files to the owner anytime and from anywhere. We use hashing scheme which is used to check integrity of data this helps user to ensure that no modification is done in data and this system provides higher speed with more accuracy.

V. REFERENCES

[1] Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satapathy , “Cloud Computing: Security Issues and Research Challenges”. (IJCSITS) Vol. 1, No. 2, December 2011.

[2] AncaApostu, FlorinaPuican, GeaninaUlaru, George Suciu, GyorgyTodoran, “Study On Advantages And Disadvantages Of Cloud Computing” ISBN 2013.

[3] Mehdi Hussain and MureedHussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[4] Mohammed Salem Atoum, Subariah Ibrahim, GhazaliSulong and MazdakZamani, “A New Method for Audio Steganography Using Message Integrity”, Journal of Convergence Information Technology (JCIT) Volume8, Number14, September 2013.

[5] Murakami, Qiangfu Zhao, RyotaHanyu, “A new Steganography Protocol for Improving Security” IEEE 2014.

[6] Deshpande Neeta, KamalapurSnehal, “Implementation of LSB Steganography and its Evaluation for Various Bits” computer Science Dept, India. IEEE 2014.

[7] Nimmy k., M.Sethumadhavan, “Novel Mutual Authentication Protocol for cloud using secret sharing and Steganography” IEEE 2014.

[8]GarimaSaini, Naveen Sharma, "Triple Security of Data in Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014.
[9] MrinalkantiSarkar,TrijitChatterjee, "Enhancing Data Storage Security in Cloud computingThrough Steganography",ACEEE.Int.J.on.Network Security,Vol.5,No.1,January2014.
[10] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, "Comparison of different techniques for Steganography in images",International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 2, February 2014.
[11] Vaishali, AnkurGoyal, "An Implementation of 4 Bit Image Steganography for Data Security in Clouds",Volume 4, Issue 11, November 2014,www.ijarcsse.com.
[12] Karun Handa, Uma Singh,"Data Security in Cloud Computing using Encryption and Steganography"IJCSMC, Vol. 4, Issue. 5, May 2015.
[13] DomenicoBloisi and Luca Iocchi, IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY, http://www.dis.uniroma1.it /~bloisi/steganography/isc.pdf.