Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7698989

A STUDY ON USE OF DISTRIBUTED ALGORITHMS DURING DISTRIBUTING THE FILE AND PRACTICING STEGANOGRAPHY

Sarika Hemant Gadekar and Dr. Arpana Bharani
Department of Computer Science, Dr. A. P. J. Abdul Kalam University, Indore
Corresponding Author Email: sarikaghadge.sg28@gmail.com

Abstract:
Secure online information services are increasingly being provided using cloud computing. The ability to access data from any location is only one of the many benefits of cloud computing, which also includes not having to worry about backups or setting up disaster recovery and business continuity centres. However, cloud computing raises concerns regarding the appropriate management of such data and interactions by cloud service providers, end-user organisations, and governments. If you run a large organisation or are an individual who needs a wide range of network services at a low total cost, cloud computing is quickly becoming the most popular option. Data on individuals is often stored in the open Cloud, where it may be accessed by anybody. When compared to the adaptable services offered by cloud providers, this fundamental creates a wide range of problems.
Keywords: Distributed Algorithm, Distributing, Steganography

1. INTRODUCTION

Cloud computing proposes a new model for computing and the associated problems of its such as compute, storage, software program. Cloud computing has many buyers like average people, academia, and enterprises with purposes and motivations various to move more than to the cloud. If perhaps cloud computer users are actually academia, the security, as well as functionality of computing as well as the cloud service providers (CSPs), need to be effective. The majority of enterprises possess a lot of information and they search for a storage area of cloud setting to secure the information. Hence, protection plays a crucial role in protecting that very sensitive information. There are lots of CSPs that supply the security of information to the users.[1]

In the procedure of offering security for information, the CSPs create an inclination to tamper with or maybe misuse the very sensitive information without the previous information of the users. Thus, the users are pressured to conceal the originality of their information of theirs prior to storing directly in cloud storage. There are lots of standard present cryptographic strategies which assist the drivers to encrypt the information before saving directly into cloud storage. Each day the need for these cryptographic methods increases tremendously. The objective of encryption is making information unintelligible to unauthorised customers & incredibly tough to decipher when attacked. Encryption is able to offer good security for information to provide very sensitive details probably the highest amount of protection.[2]

1.1 Steganography

The Greek words steganos, meaning "connected" or "secret," and graphy, meaning "drawing" or "composition," are the basis for the modern term "steganography." Thus, steganography is

synonymous with secret writing. For steganography to be effective, it must first and foremost be able to hide information from the naked eye without raising suspicions about the authenticity of the information being sent. Interest in steganography has risen rapidly for two reasons: Companies involved in broadcasting and distribution have honed their skills in hiding embedded copyright imprints and sequence numbers in professionally produced films, audio chronicles, visual and written works, and audible items. In light of the different governments' efforts to limit the availability of encryption systems, individuals have begun to consider how their personal emails might be concealed in apparently benign communications that are then disseminated.[3]

The motivational force behind cryptography is the notion that anybody can make information secret by encoding it in a way that no one else can decipher it. It's quite unlikely that anybody, even the government, would be able to decipher a message encrypted using a strong cryptographic encryption. The first figure shows this steganographic paradigm.[4]

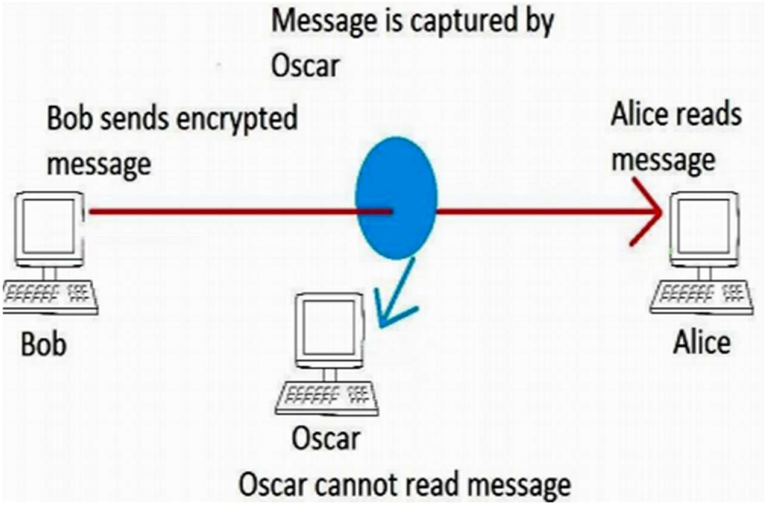

Figure 1.1: Conception of Steganography

1.2 Types of Steganography

There are several distinct varieties of steganography, each distinguished by the specific kind of cover file it employs.[5]

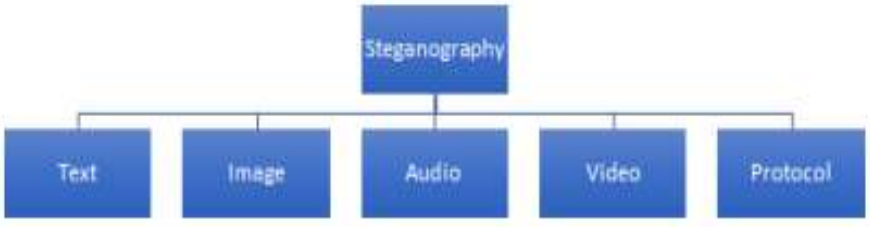

Figure 1.1: Type of Steganography

i. Text Steganography

When using text steganography, both the cover file and the concealed message would be written in a textual format. Like the Morse code used in radio transmission, the number of characters, white space, and capital letters are taken into account while deciding how to embed a message in a string of text for steganography.[6]

ii. Image Steganography

When a picture is used as the cover object, the technique known as steganography may be utilized to hide a secret message. In this steganography, graphical digital pictures are often employed as cover sources; the cover file enables the user to insert a large amount of data. The main benefit of picture steganography is that the cover image does not draw the attention of a potential intruder.

iii. Audio Steganography

Audio steganography is the art of concealing information in an audio stream such that it cannot be detected by the human ear. It's the study of inserting secret data into a host transmission, such as words or sounds. Function-wise, the host message and the stego message that results from steganography are almost interchangeable. Optical sound embedding is a more involved technique for transmitting secret information. There are a number of techniques for adding metadata to digital music.[7]

iv. Video Steganography

In multiple data concealing technology, video steganography is becoming a key study subject, which has become a promising approach. This is not just because of the growing need for secret message transmission to be encrypted, but also because video files contain a massive quantity of data that may be put to good use. Based on where the secret message is placed in the video, steganography may be classified as either intra-embedding, pre-embedding, or post-embedding. Intraembedding methods are grouped according to the phases of video encoding, such as intraprediction, motion vectors, interpolation of pixels, coefficients of transformation. Pre-embedding techniques are used to unprocessed video in order to transform it into different spatial formats or sub-domains. All the work of embedding and un-embedding video steganography is done on the compressed bit stream, which is the primary focus of post-embedding techniques.

1.3 Steganography Phases

Each Steganography method has its own unique set of steps that must be taken in order for the secret message exchange between sender and recipient to be successful.

Sender: To successfully convey the secret message, the sender must first embed it in the stego-medium and then use the chosen channel of communication.

Communication channel: The networked or otherwise disseminated cover image that conceals a concealed message in its encoding. To protect the concealed message from any unauthorised access, the embedding approach for man-in-the-middle assaults must be well developed.

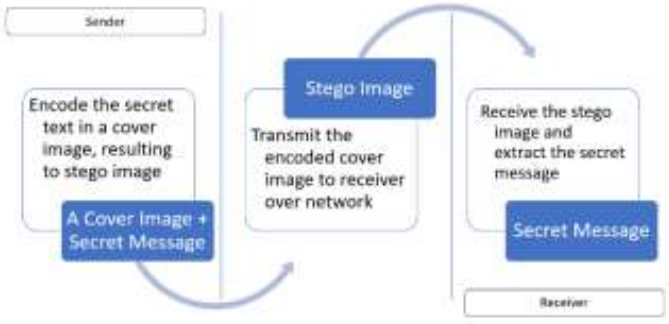

Figure 1.2: Phases of Steganography

Receiver: The last step of steganography involves retrieving and extracting the cover medium to determine whether the concealed message delivered through the channel was successfully decoded.[8]

1.4 Framework for Enhanced Security Algorithms in Cloud Computing

In this part, we proposed a plan to ensure the safety of information stored in the cloud. Addressing these common security concerns is the core focus of the framework. Indeed, cloud computing technologies are used in the suggested architecture.

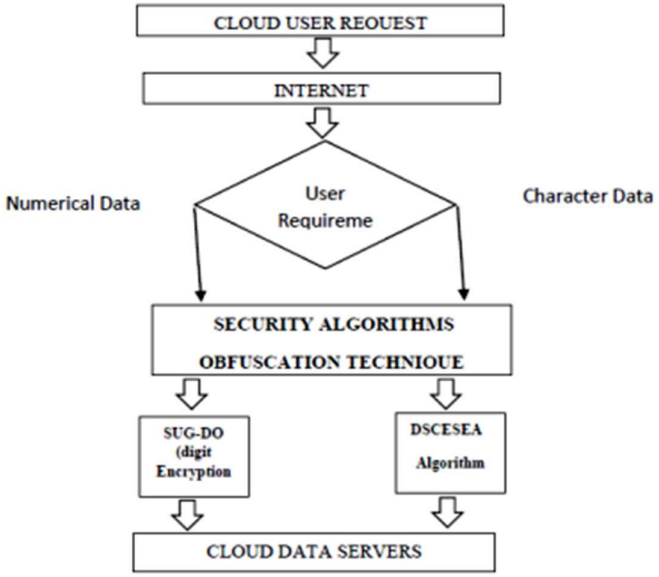

Figure 1.2: A Framework for Enhanced Data Security in Cloud

As can be seen in Figure 1, the most useful aspect of the framework is the user request, which provides the owners with a means for interacting with online services. Web-based property owners are making the request. Part 2 and the request from the owners are discussed in the first section, as is the availability of the services through the web. The request is sent to the security measures for a third party. The next step is to use the real security algorithm to provide the top protection available. Data security algorithms distribute information stored on a server based on the characteristics of the request. The motivation for this work comes from the need to assign information on various security measures. The following algorithm, SUG-DO, and DSCESEA, will be run based on user input.[9]

2. LITERATURE REVIEW

Handa, K. and Singh, U., (2015) The safety of their data storage facilities is a major worry for every business nowadays. Privacy of data and its security in whatever form is always the top concern for every organisation, regardless of whether it maintains its own infrastructure or uses cloud storage. Cloud computing services provide a vast number of data storage and other resources that may be allocated to different businesses in accordance with their specific needs. In this study, we take a look at four distinct methods recommended for safeguarding data and restoring it in the event of its deletion owing to, say, a cloud service outage. Seed-based approach, which is utilised for recovering data which is remotely stored at any geographical place in a cloud, is the first method to be investigated. If data is lost, the method may restore it. The second method discussed is the attribute based access control algorithm used to safeguard data, ensuring that information kept in the cloud remains private and secure.[10]

Zhu, Z., and Jiang, (2015) Numerous businesses rely on cloud computing to store massive amounts of data. Therefore, it may be necessary to safeguard the information, which may be in the form of text, audio, video, and many other media. Several techniques for protecting cloud-stored data have been developed keeping researchers' methods in mind. Extensive literature reviews have been carried out for this work, which is an attempt to highlight some of the essential algorithms for the security of statistics. With cloud computing, you may increase or decrease your storage capacity as needed without having to invest in any new physical infrastructure. A new storage layer stores information in a cloud records centre, a control layer guarantees the privacy and security of cloud storage, an application interface layer offers a platform for cloud application providers, and a fourth tier, the cloud access layer, grants users access to the cloud.[11]

Kajal, N., &Ikram, N. (2015) Even though there has been a lot of study and a lot of commercially available solutions aimed at authenticating users of digital voice-based systems, relatively few of them really work effectively in terms of usability and security in the audio domain. In addition, studies have revealed that speech biometrics perform poorly compared to other authentication strategies. We propose using audio steganography as a means of concealing authentication key material within sound, allowing for an additional authentication factor to be achieved within an audio channel to supplement other methods, thereby providing a multi factor authentication opportunity that retains the usability associated with voice channels. By developing a novel threat model for audio and voice-based systems, outlining a novel architectural model that makes use of audio steganography to mitigate threats in various authentication scenarios, and finally conducting experimental research into hiding authentication materials into an audible sound, this study provides a comprehensive overview of the difficulties and dangers that audio and voice-based systems face.[12]

Shaheen, M. (2015) Many people and businesses have benefited from cloud computing since it eliminates the need to invest in costly hardware, software, and ongoing support and maintenance. There are various security and trust issues that arise from Cloud Server's (CS) lack of reliability. Users may trust the integrity of their outsourced data to a third party, such a Third-Party Auditor, via a process called public auditing (TPA). One method of auditing that may confirm integrity using cryptographic techniques is called Provable Data Possession (PDP). Verification times are lengthened because many PDP techniques rely on bilinear pairing and homomorphic authenticators, both of which need complicated calculations. With the advent of new cryptographic methods, lightweight auditing systems have become an absolute need. One such newer, weaker primitive is Indistinguishability Obfuscation (IO), which, when combined with one-way functions, yields a wide variety of cryptographic structures. Cryptographic constructions were suggested by Sahai and Waters, who advocated for the use of IO. [13]

Saini, G., & Sharma, N. (2016) Information security is becoming an integral part of the ever-expanding communication and internet technologies of today, such as 5G, cloud computing, and blockchain. Any number of cyberattacks may be launched against data in transit if it is sent unencrypted. After experimenting with a variety of text sizes and the cover image in a variety of image formats, it was determined that the text size should be 15% smaller than the cover image. This is because the hybrid multi-stage data encryption architecture, which builds sequential and pseudo-random encoding/decoding algorithms with pre-stage text encryption,

found that the change in image size had no effect on the image's resolution or attributes. Additionally, the hybrid cryptography and steganography-pseudo-random encoding/decoding technique is more effective and less time-consuming than sequential encoding/decoding.[14]

3. METHODOLOGY

The methodology is the systematic, theoretical analysis of the methods applied to a field of study. It comprises the theoretical analysis of the body of methods and principles associated with a branch of knowledge. Typically, it encompasses concepts such as paradigm and theoretical model, phases. The term Research is related to seeking out information and knowledge on a particular topic or subject. In other words, research is the art of systematic investigation. Someone says that necessity is the mother of all inventions and the person engaged in this scientific investigation can be termed a researcher. Research is a pedagogic action the term should be used in a technical sense.

The main message will be sent out in two installments as follows:

- **At hosting site**

We'll save steganographically encrypted image, audio, and video files at the hosting service.

- **At Cloud**

Photos, music files, and videos may all have their corresponding references or even keys safely saved in the cloud. Since the other half of the decryption key for a file exists elsewhere, even if a person has the answer or guidance from the cloud, he still cannot access the encrypted file.

4. RESULT AND ANALYSIS

Performance analysis:

We've measured the time and effort required to decrypt files of varying sizes using symmetric encryption techniques (AES, DES, and Triple DES). The figure shows that AES is the preferred cipher when both key size and calculation cost are taken into account; because AES comes in a variety of key sizes, we let data owners decide which one is best for their needs. Similarly, the data is encrypted when the user downloads the file from the server, as described in the downloading phase. A decryption process on the Clint machine is performed if the user later decides they need access to their data in its original format. The decryption results and times for the various algorithms are shown in Figure 4.1.

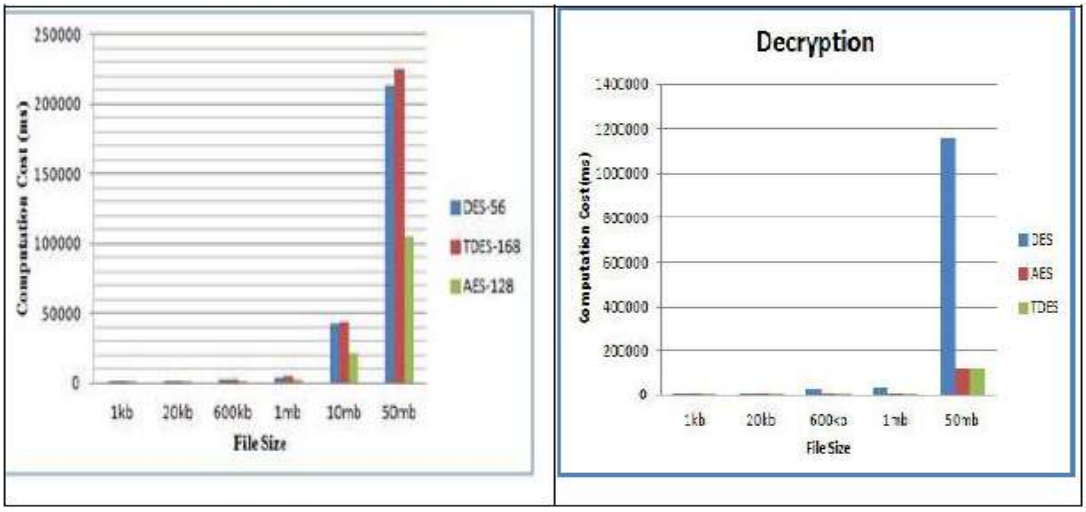

Figure 4.1: Encryption/Decryption Cost at Client side

The client (and the server) performs the cryptographic procedure of calculating a hash code (message digest) to check the integrity of the data. Cost of hash calculation at client, for various file sizes. In terms of speed, MD5 is our top pick, but if you're looking for something more secure, SHA-256 is a solid alternative.

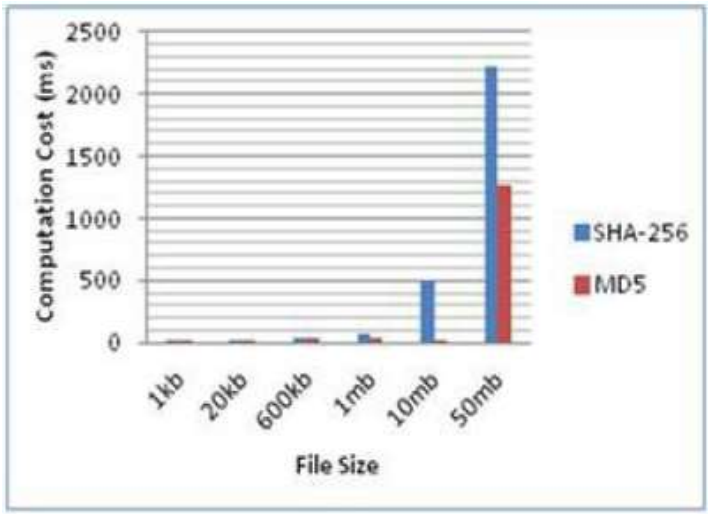

Figure 4.2: Hash code Computation Cost at user Side

It's not always the case that a user's data is very confidential. There may be times when a user only wishes to keep data on the server without any requirement for security. Consequently, in this scenario, the client may choose to not provide the file in an encrypted format; figure 4.3 below compares the computational cost and time savings that would result from either scenario. The diagram below depicts a complete cycle, beginning with a client sending a file (which may or may not be encrypted) to a server, which then sends the file back to the client. The DES encryption method is maintained in this implementation only in case a client decides to use an encryption.

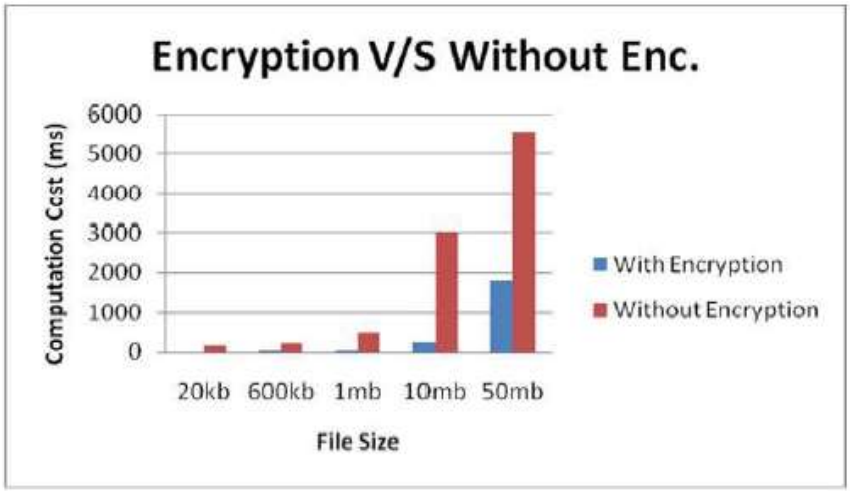

Figure 4.3: Encryption Cost comparison

Encryption is used for all data saved on the server. Since the user has no faith in the CSP, the latter is not provided with the symmetric encryption keys. The sole cryptographic operation performed by the CSP is the recalculation of the hash code. Hash is calculated by CSP and sent back to Client when they get a request. We can now confidently assert that the hash code size is consistent and extremely tiny, regardless of file size, resulting in significant savings in both communication costs and overhead. Obfuscation, like encryption, is something we advise doing on the server side, and although the proof of obfuscation may lengthen the process as a whole, it is still worth it in the end since it increases security. Download times with and without obfuscation are shown in figure4.4 below.

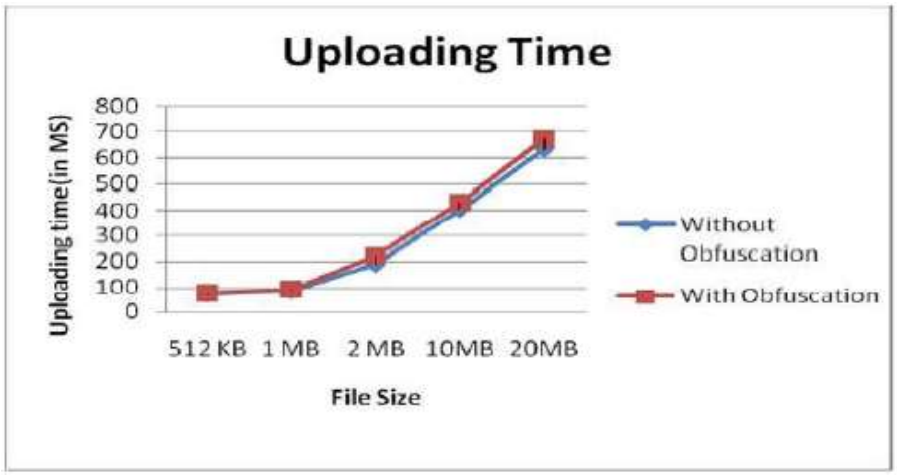

Figure 4.4: Obfuscation Cost comparison

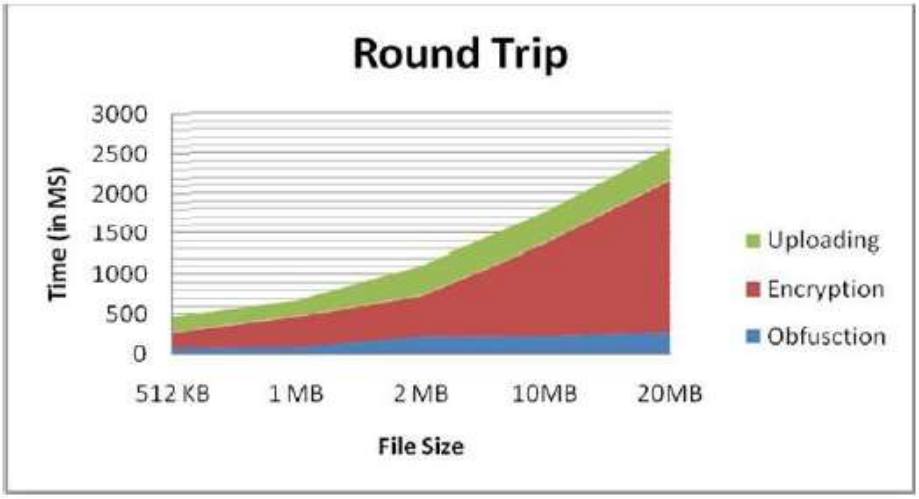

Figure 4.5: Round Trip cost

The total time spent on all the sub-processes that work together to complete the job is shown in figure4.5. Lots of researchers have laid forth the groundwork for both full and partial server-side encryption of database information. In order to ensure the safety of our idea, we use an obfuscation technique. Given the time savings compared to complete or partial encryption in the following chart, it seems clear that obfuscation is the way to go.

5. CONCLUSION

Despite cloud computing's many benefits, some customers are wary of adopting it because of concern for their data's safety, and the service provider may have concerns about unauthorized access as well. Therefore, we established a new framework by proposing a combination of encryption and obfuscation to address problems for both users and service providers. In this way, the user can be certain that his data will remain private while in transit over the network and before it is sent to the Cloud. To prevent data loss, we've designed a secure server that generates a unique hash for each file submitted by each user. To prevent unauthorised parties from gaining access to sensitive client data stored in the cloud, a robust obfuscation approach is recommended for cloud service providers.

REFERENCES

1. Hu, C., Liu, P., Yang, R., &Xu, Y. (2019). Public-Key Encryption With Keyword Search via Obfuscation. IEEE Access, 7, 37394- 37405, 2019
2. J. Surbiryala and C. Rong, (2018) "Data Recovery and Security in Cloud," 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), Zakynthos, Greece, , pp. 1-5.doi: 10.1109/ IISA.2018.8633640, 2018
3. Akshay, K. C., &Muniyal, B..(2018) Analysis of Data Hiding Methods in Image Steganography. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2023-2027).
4. Wu, W. C., & Yang, S. C. (2017). Enhancing image security and privacy in cloud system using steganography. In 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW) (pp. 321-322). IEEE.
5. Sharma, A., Sharma, N., & Kumar, A. (2017) A new algorithm to secure image steganographic file. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 570-573). IEEE.

6. Suneetha, D., & Kumar, R. K..(2017) A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography. Advances in Computational Sciences and Technology, 10(9), 2737-2744.
7. Ranjan, A., &Bhonsle, M. (2016) Advanced System to Protect and Shared Cloud Storage Data using Multilayer Steganography and Cryptography. International Journal of Engineering Research, 5(6), 434-438.
8. S. Arul Oli and Dr. L. Arockiam, (2016) "Enhanced Obfuscation Technique for Data Confidentiality in Public Cloud Storage", International Conference on Mechanical Engineering and Electrical Systems, Volume 40.
9. Suthar, K., & Patel, J. EncryScation (2015) A novel framework for cloud iaas, daas security using encryption and obfuscation techniques. In 2015 5th Nirma University International Conference on Engineering (NUiCONE) (pp. 1-5). IEEE, 2015
10. Handa, K. and Singh, U., (2015) Data security in cloud computing using encryption and steganography. International Journal of Computer Science and Mobile Computing, 4(5), pp.786-791.
11. Zhu, Z. and Jiang, (2015) A secure anti-collusion data sharing scheme for dynamic groups in the cloud. IEEE Transactions on parallel and distributed systems, 27(1), pp.40-50, R., 2015
12. Kajal, N., &Ikram, N. (2015) Security threats in cloud computing. In International Conference on Computing, Communication & Automation (pp. 691-694). IEEE.
13. Shaheen, M. (2015) Data Obfuscation for Privacy and Confidentiality in Cloud Computing. In 2015 IEEE International Conference on Software Quality, Reliability and Security-Companion (pp. 195-196). IEEE.
14. Saini, G., & Sharma, N. (2016) Triple security of data in cloud computing. International Journal of Computer Science and Information Technologies, 5(4), 5825-5827, 2014.