IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

# A Survey of Data Hiding methods for data security in Cloud

**A Mallareddy[1*], R Sridevi[2], Ch G V N Prasad [3]**

[1]Department of IT, CVR College of Engineering and Research Scholar, JNTUH Hyderabad, Telangana, India
[2]Department of CSE, JNTUH College of Engineering, Hyderabad, Telangana, India
[3]Department of CSE, Sri Indu College of Engg & Tech., Hyderabad, Telangana, India

[*]*Corresponding Author: mallareddyadudhodla@gmail.com, Tel.: +91-98489-62142*

DOI: https://doi.org/10.26438/ijcse/v7i5.690694 | Available online at: www.ijcseonline.org

Accepted: 24/May/2019, Published: 31/May/2019

***Abstract*—** In recent years cloud computing has achieved great development as it provides economic and convenient services. Cloud data services are an interesting and the latest way for storing enterprise data as more companies and users are uploading their data to cloud. The problem of data privacy and security needs to be addressed efficiently to fully utilize the power of cloud data services. Data security is a crucial aspect in cloud data storage and transmission. The use of data hiding methods for the security in data transmission and data storage would be very effective in securing cloud data. In this paper, we present a survey of data encryption methods, steganography methods and hybrid methods, that have been extensively applied in this context. However, majority of these methods suffer the overloads involved with encryption techniques and also have heavy computational time. A new method that specifically addresses security of cloud without the usage of encryption process is essential for reducing the overheads of encryption techniques, thereby improving the overall performance. At this juncture, data hiding techniques are considered to be more suitable and potential substitute over the encryption-based cloud data storage security techniques existing in the literature. We propose to build such data hiding techniques as future work.

***Keywords*—** Data Hiding, Cloud data security, Encryption Techniques, Data aggregation.

## I. INTRODUCTION

Cloud data services are an interesting and the latest way for storing enterprise data. Amazon Relational Database Service (RDS) and Microsoft SQL Azure are the popular platforms wherein enterprises are outsourcing their data storage. The hardware and software underlying data storage are shared among users in cloud data services. The cloud data services allow enterprises to deploy their data quickly without making the large investment on their proprietary hardware and software, hence reducing the total cost of ownership. Moreover, the data services on cloud can be elastic, meaning that an enterprise can dynamically increase or decrease the resources allocated to its data according to its business requirements.

With the rapid development of cloud technologies, more and more data are generated and transmitted in various fields, that may include sensitive information which should be secured. The communication media used for transmission of data does not provide data security mechanisms which increases the risk of data misuse. Even though cloud data services appear as an attractive paradigm of data management, their power cannot be fully utilized until the problem of data privacy and security is addressed efficiently. Hackers and security researchers [] have shown that the virtualization capabilities of cloud can be exploited to create new and more robust forms of malware that are hard to detect and can evade the traditional security techniques. Several solutions to address the security and privacy in cloud computing can be proposed as monitoring cloud server services, protection of data privacy, determination of the accuracy of the information, inaccessibility by third parties, protection against unwanted changes and deletions, prevention of malicious content and ensuring uninterrupted access to information [1].

Data security aims to prevent access to user data by third parties for whatever purpose and is of great importance for all users involved.This paper emphasizes utilization of data hiding techniques for security of users data. Data hiding techniques are popular for increasing the security in various fields of their application as they are designed to protect data against malicious users and a variety of attacks. Data hiding techniques can be divided into three main categories: steganography, watermarking and cryptology. Steganography does data hiding in a multimedia tool (images, videos, etc.) to prevent it from being recognized by malicious users. Watermarking is widely used for unauthorized copying and copyright issues in general, and the hidden data is expected to be robust against attacks. Cryptology involves usage of encryption algorithm for data hiding. The data will thus become meaningless to unauthorized users. However, there is risk of data manipulation by malicious users. There has been extensive

 

research benefiting equally from both these techniques for achieving data security in cloud and hence various hybrid methods have been proposed in the literature.

This paper presents a survey of such researches, especially the techniques of steganography, cryptography and hybrid methods that combine encryption methods with steganography for data hiding in cloud. The paper is organized as follows : Section II discusses the various data hiding techniques based on encryption methods applied for cloud data security. Various methods of steganography applied for cloud data security are compared in Section III. Many hybrid methods using cryptography and steganography are proposed in the literature. These methods are discussed in Section IV. Future Scope is summarized in Section V. We conclude in Section VI.

## II. ENCRYPTION METHODS

Muhammad Usman et.al[] propose an improved compression and encryption technique for transferring mobile video data to cloud server by using modified AES and RSA schemes. The proposed scheme is a combination of Private key (PRK), Public Key (PUK) and Secret Key (SK). The modified AES-256 is applied at the user side and RSA is applied at the server side. The cloud generates a pair of PRK and PUK. The PRK remains at the cloud's side while the PUK is sent to the user for encryption purpose. In general, this scheme has three major phases, i.e., HEVC ( High Efficiency Video Coding) for video encoding, video and secret data encryption, half decryption and full decryption with the secret data extraction. User who is uploading the data, first encodes the video, encrypts the secret data using SK, adjusts the encrypted data into encoded video, and then encrypts the video using PUK to generate an encrypted HEVC Encoded Video Stream (HEVS). Next, the owner uploads the encrypted HEVS over the public cloud, where the cloud sources decrypt the video using the PRK, a technique known as half decryption. The cloud sources are ignorant of the data hidden in the video stream. When the receiver downloads the video, he decrypts it using SK, extracts the required data and then either keeps or discards the video stream. The authors claim that the average computational time taken for encryption in their proposed strategy is less when compared to computational times involved in DES, AES-128, AES-192, AES-256.

Singla & Singh[] deals with the methods of providing security using data encryption and ensuring that an unauthorized intruder cannot access user file or data in the cloud. Data is encrypted by a symmetric block cipher cryptography algorithm called "Rijndael" before being stored in a cloud environment. Neha and Ganesan[] have proposed a strategy that ensures secured transmission of data from the user to cloud server. They use Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism for connection establishment. The proposed encryption mechanism uses the combination of linear and elliptical cryptography methods. They claim that usage of ECC reduces the computational cost compared to the linear algorithms.

Kaur and Bhardwaj[2] propose a hybrid technique which combines multiple encryption algorithms such as RSA, 3DES, and random number generator for more flexibility and enhanced security in cloud data. This method suffers heavy computational time due to the multiple algorithms involved. Manivannan and Sujarani[4] have proposed a lightweight mechanism for database encryption known as transposition, substitution, folding, and shifting (TSFS) algorithm. The algorithm encrypts only the sensitive data in the database which in turn results in efficient query execution reducing user response time. Even though TSFS is designed as a symmetric encryption technique, the authors use three keys for encryption and decryption. The 3 keys used are expanded into 12 sub keys by using a key expansion technique. This method suffers from computational overhead as number of keys are increased.

Huang and Tso [7] proposed a commutative encryption algorithm based on the ElGamal encryption which can be applied in data hiding, database integration and some cryptography applications. A commutative encryption enables a plaintext to be encrypted more than once using different users public keys without decryption of the first cipher text before applying further encryption/re-encryption processes. Moreover, the resultant ciphertext can be decrypted by the designated decrypters without considering the order of public keys used in the encryption/re-encryption processes. The authors modify the ElGamal encryption to suit commutative encryption. The method proposed is supported by theoretical proof and hence has no experimental analysis of the computational time taken.

## III. STEGANOGRAPHY METHODS

Sarkar and Chatterjee[0] have proposed an architecture for securely storing the client's data at cloud server as an image. Their architecture utilizes three Cloud Service Providers: CSP-1, CSP-2 and CSP-3, each of which have their specific roles in representing the user data as image using steganography. Based on the size of the data file and image file sizes stored at CSP-1, CSP-3 requests CSP-1 for suitable image files. Then CSP-3 requests CSP-2 to provide suitable algorithm to transform the file data into the pixels of the image provided by CSP-1. The proposed scheme is able to handle only a limited number of security threats in a fairly small environment and needs performance evaluation for real time environment.

Handa et.al[5] proposed an extended approach for LSB Steganography. The user selects the data to be uploaded and

 

this selected data gets encrypted using a strong algorithm such as AES. This encrypted data is then uploaded to the cloud server. On receiving the encrypted data, a hiding algorithm is applied such that it randomly selects the bits positions from images where data is to be stored. The bit position is either $0^{th}$ , $1^{st}$ or $2^{nd}$ position. This hiding algorithm is used to save the files or data behind the images. This process is called steganography using images.

Suneetha and Kiran Kumar[15] proposed a modified Least Significant Bit (LSB) - image based Steganography approach for secure storage of information at Cloud Service Provider side. Unlike LSB steganography where only LSB is considered for storage and retrieval of data, both pixels LSB and MSB are used for storage and retrieval. Based on one of the possible values of LSB and MSB (i.e. 00, 01, 10, 11 ) bitwise or, xor operators are used for this process. This approach is tested using the metrics Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

## IV. HYBRID METHODS

Garg and Kaur[12] claimed that encryption alone cannot guarantee secure storage of data in cloud. They proposed a hybrid approach of encryption and steganography techniques. The data in the cloud is encrypted using AES algorithm in the first stage. Then least significant bit steganography is applied on the result encrypted data within a image. This image is then loaded and encrypted within a cover image.

Kini et.al[9] propounded an efficient data hiding technique and image encryption in which the data and the image can be retrieved independently. The data owner encrypts the original uncompressed image which is further passed on to a data-hider who may compress the least significant bits of the encrypted image using a data-hiding key. This creates a sparse space to accommodate additional data. The receiver can extract additional data using data hiding key without having information about the original image content. Also, using the decryption key the receiver can extract data to obtain an image similar to the original one, but cannot extract the additional data. A receiver having both the data hiding key and the encryptions key can extract the additional data and the original image without any loss. The authors use FJRC-4 algorithm to create the pseudo random sequence using the 128-bit encryption key.

Rao[3] proposed a hybrid technique for data confidentiality and integrity that uses key sharing and authentication techniques. The connectivity between the user and the cloud service provider is made more secure by utilizing key sharing and authentication processes. RSA public key algorithm is used for secure distribution of the keys between the user and cloud service providers. Mohamed et.al.[] proposed a three-layered data security technique in which the first layer is used for authenticity of the cloud user either by one factor or by two factor authentication. The second layer then encrypts the user data for ensuring data privacy, whereas the third layer does fast recovery of data through a decryption process.

Surbhi[] proposed a hybrid technique that utilizes encryption algorithm and steganography for data hiding in cloud. Firstly, the sensitive data is encrypted using Advanced Encryption Standard(AES) algorithm. Further in steganography, cover media is processed to form monogram puzzle inside the symmetric shapes. The selection of monogram puzzle and symmetric shape is done on the fly based on output of random number generator. Lastly, the encrypted information is hidden inside the monogram puzzle by using 2-bit LSB technique.

## V. FUTURE SCOPE OF RESEARCH

A group of user nodes, working for the same application, need a secured storage facility for aggregate data in the cloud.The data produced by each user node must be known only to itself to ensure data privacy. This in turn means that this private data must be invisible to the aggregator in the cloud server which makes the problem more challenging. However, data aggregation and data privacy protection contradict each other since to achieve data aggregation, any aggregator must view each data item they process in plaintext. As discussed earlier end-to-end data encryption, a well-known security method, as well as popular methods of steganography has been extensively applied in this context.
A new method that specifically addresses such contradiction without the usage of encryption process is required to reduce the overheads of encryption techniques, thereby improving the overall performance. Our future work focuses on building efficient data-hiding techniques for ensuring data privacy and also needs to aggregate the private data, when group of user nodes are working for the same application. Such a scheme is aimed at achieving the following:

1. Data privacy: The user data collected by the user node must only be known to itself.
2. Accuracy: The user node data must have accurate aggregation results.
3. Dynamic: The proposed scheme must be adaptable to dynamic addition and deletion of user nodes

 

since the number of user nodes participating in the node is dynamic.

## VI. CONCLUSION

The presented survey discussed various research proposals for data hiding in cloud which are based on Encryption techniques, Steganograohy and hybrid methods. We compare these methods and summarize their merits and demerits in Table 1 based on their capability in achieving the following parameters -

- Data Privacy.
- Secure Communication.
- Algorithms used.
- Computational Time.

As shown in Table. 1, most of the proposed works rely on the standard encryption techniques and steganography algorithms. These algorithms have an overload of key distribution and secret key sharing. Also, the computational time taken for hiding the private data is considerably high due to the computations of the algorithms used. Hence these algorithms are not applicable to applications that require data hiding techniques with a faster computational time.

**Table 1: Comparison of various methods for data hiding in cloud**

| Proposed Method | Data Privacy | Secure Communication | Algorithms Used | Computational Time | Time complexity |
|---|---|---|---|---|---|
| Muhammad Usman et.al[11] 2017 | Yes | Yes | AES and RSA | High | $O(N) + O(N^3)$ |
| Singla and Singh[13] 2013 | Yes | Yes | Rijndael | High | $O(N^3)$ |
| Neha and Ganesan[16] 2014 | Yes | Yes | Diffie Hellman Key Exchange and Elliptical curve cryptography | High | $O(N) + O(N^4)$ |
| Kaur and Bhardwaj[2] 2012 | Yes | Yes | RSA, 3DES | High | $O(N^3) + O(N)$ |
| Manivannan and Sujarani [4] 2010 | Yes | Yes | TSFS | High | ------ |
| Huang and Tso [] 2012 | Yes | Yes | Asymmetric encryption techniques | High / Medium | $O(N)$ or $O(N^3)$ or $O(N^4)$ |
| Sarkar and Chatterjee[] 2014 | Yes | No | Steganography based on random bits | Medium | Based on the Image Size |
| Handa et.al [] 2015 | Yes | No | AES and Steganography based on LSB | Medium | $O(N)$ |
| Suneetha and Kiran Kumar[] 2017 | Yes | No | Steganography based on LSB and MSB | Medium | $O(N)$ |
| Garg and Kaur[] 2016 | Yes | Yes | AES and Steganography | Medium | $O(N)$ |
| Kini et.al[9] 2016 | Yes | Yes | FJRC-4 algorithm and Encryption algorithm | Medium | $O(N)$ |
| Rao[3] 2012 | Yes | Yes | RSA and other Encryption algorithms | High | $O(N^3)$ |
| Mohamed et.al[6] 2012 | Yes | Yes | Encryption algorithms | High / Medium | $O(N)$ or $O(N^3)$ or $O(N^4)$ |
| Surbhi[14] 2018 | Yes | Yes | AES and Steganography based on LSB | Medium | $O(N)$ |

## REFERENCES


[1] Avizienis A, Laprie J C, Randell B and Landwehr C 2004 "*Basic concepts and taxonomy of dependable and secure computing"*. IEEE Trans. Depend. Secure Comput. 1(1): 11-33

[2] A. Kaur and M. Bhardwaj, *"Hybrid encryption for cloud database security"*, International Journal of Engineering Science & Advanced Technology, vol. 2, pp. 737 -741, 2012.

[3] A. Rao, "*Centralized database security in cloud"*, International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, pp. 544-549, 2012.


 

[4] D. Manivannan and R. Sujarani, "*Light weight and secure database encryption using tsfs algorithm"*, in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT '10), pp. 17, IEEE, 2010.

[5] Handa, Karun, and Uma Singh. "*Data security in cloud computing using encryption and steganography*." International Journal of Computer Science and Mobile Computing vol. 4, pp. 786-791, 2015.

[6] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "*Enhanced data security model for cloud computing"*, in Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12), pp. CC-12CC-17, IEEE, 2012.

[7] K. Huang and R. Tso, "*A commutative encryption scheme based on ElGamal encryption"*, in Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC 12), pp. 156-159, IEEE, August 2012.

[8] Kevin Skapinetz, "*Virtualisation as a Blackhat Tool*," in Network Security, Elsevier., 2007, pp. 4-7.

[9] Kini, K., M. Mithani, R. Naik, D. Raut, et M. Kumbar. "*Securing cloud data using crypto-stegno based technique"*. Journal of Insect Behavior 5, 178-180, 2016

[10] MR KA Sarkar TR Chatterjee.. "*Enhancing Data Storage Security in Cloud Computing Through Steganography"*. ACEEE Int. J. on Network Security, Vol. 5, No. 1.2014.

[11] Muhammad Usman, Mian Ahmad Jan, Xiangjian He, "*Cryptography-based secure data storage and sharing using HEVC and public clouds"*, Information Sciences, Volume 387, 2017, Pages 90-102, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2016.08.059.

[12] N. Garg, and K. Kaur, *"Hybrid information security model for cloud storage systems using hybrid data security scheme"*, International Research Journal of Engineering and Technology, Vol. 3, Issue 4, pp.2194-2196, 2016.

[13] Singla, S. et J. Singh . *"Implementing cloud data security by encryption using rijndael algorithm"*. Global Journal of Computer Science and Technology Cloud and Distributed 13,19-22.2013

[14] Singla, Surbhi. *"Data Embedding Technique for Image Steganography in Cloud Computing"*. Diss. 2018.

[15] Suneetha, D., and R. Kiran Kumar. *"A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography"*. Advances in Computational Sciences and Technology,Vol. 10: 2737-2744, 2017

[16] Tirthani, Neha, and R. Ganesan. *"Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography"* IACR Cryptology ePrint Archive 2014 (2014): 49.

## AUTHORS PROFILE

**A. Mallareddy**, M.Tech (Ph.D) is working as Associate Professor in Department of Information Technology at CVR College of Engineering, Hyderabad, and also pursuing Ph.D in Computer Science and Engineering from JNTUH Hyderabad. His research interests focus on Data Structures, Cloud Security, Cryptography and Network Security.

**Dr. R. Sridevi** is a Professor and heading Computer Science and Engineering Department at JNTUH College of Engineering Hyderabad, Jawaharlal Technological University Hyderabad. She received her Ph.D in 2010. Her research interests include Data Structures, Steganography, Steganalysis, Network security and Cryptography, Computer Networks and Cloud Security. She has published more than twenty research papers in reputed journals and eight international and national conferences.

**Dr. Ch G V N Prasad** , M.Tech,,Ph.D (Experience-- 20 years ; 12 years IT industry ( 8 years in National Informatics Centre, Govt. of India, as Scientist and Software Analyst in AT&T in US ) and 18 years Teaching as Professor and HOD of CSE dept). He is currently working as Professor in Department of Computer Science & Engineering in Sri Indu College of Engg & Tech. Hyderabad. His research interests include Network security and Cryptography, Data mining, Cloud Security. He has published more than Fifteen research papers in reputed journals, international and national conferences.

 