Hybrid information security model for cloud storage systems using hybrid data security scheme

Nancy Garg[1], **Kamalinder Kaur**[2]

[1] *Student,Dept.of Computer Science and Engineering,CEC college,Punjab,India*
[2]*Assistant Professor, Dept.of Computer Science and Engineering & CEC college,Punjab,India*

---***---

Abstract - *The secure data storage on cloud environments is the primary requirement of such applications, where data are being transferred or transmitted between the servers and their users. The data security is quite important because they belongs the users. With an internet based development and use of computer technology several trends are opening up in the era of cloud computing .Moving data into the cloud offers much ease to users since they don't have to care about the complexities of managing hardware directly. Steganography is the practice of hiding a content of a file ,a message, image, or video within other file, message, image, or video. Generally, the hidden messages appear to be part of other: shopping lists, articles images. When steganography is combined with encryption it provides security .In this paper two approaches which include stegnography along with encryption is presented for security of data storage on cloud.*

***Key Words*: Cover Image, LSB , CIBE , Encryption, Steganography.**

1.INTRODUCTION

The primary requirement of such applications is the secure data storage on cloud environment where data are being transferred or transmitted between the servers and their users. The data security is quite important because they belongs the users. With an internet based development and use of computer technology several trends are opening up in the era of cloud computing.

Moving data into the cloud offers much ease to users since they don't have to care about the complexities of managing hardware directly. The discoverer of Cloud Computing vendors, Amazon a Storage Service (S3) and Amazon Elastic Cloud Compute (EC2) both are well known examples .These internet-based online services do provide huge amounts of storage space and customized computing resources, computing platform shift, however, is reducing the responsibility of local machines for maintaining data at the same time. As a result, for the availability and integrity of their own data users are at the mercy of their cloud service providers.

Cloud Computing naturally raises new challenging security threats for many reasons. First, traditional cryptographic basics for protection of data security can not be directly adhered due to the loss control of data by users under Cloud Computing. Therefore, verifying the storage of correct data in the cloud must be performed without clear knowledge of the whole data. Considering different data for every user stored in the cloud and the demand of continuous data security assurity , the problem of verifying correctness o f data storage in cloud becomes more challenging. Secondly, this type of Computing is not a data warehouse by third party. The stored data in the cloud may be frequently updated by the users, which include deletion ,insertion, appending ,modifying, reordering, etc. To ensure correctness of storage for updation of dynamic data is of much importance.. Last but not the least, the evolution of Cloud Computing is done by data centers running simultaneously ,with cooperation and in distributed manner.

Since users are focusing on single server scenario and most of them do not consider data operations performed dynamically ,the techniques, which can be useful to ensure the correctness of storage without having users possessing data, cannot address all the cloud data storage security threats . So researchers have proposed distributed protocols for ensuring storage correctness across different servers as an complementary approach. Steganography is the practice of hiding a content of a file ,a message, image, or video within other file, message, image, or video. The word steganography is a combination of Greek words steganos, means "covered" and 'graphie' means "writing".

In the Steganographia, a study on cryptography and steganography, Johannes Trithemius recorded first use of the term was in 1499 which is concealed as a magic book . The messages which is hidden appear to be part of other: images, articles, shopping lists, or some other cover text. For example, the message i.e hidden may be in form of invisible ink between the visible lines of a letter which is private.

Some steganography implementations in the forms of security through obscurity that lack a shared secret, whereas key-dependent steganography schemes implements Kerckhoffs's principle.
The benefit of steganography over cryptography alone is that the original secret message does not attract attention to itself as an object of close examination. Thus, whereas cryptography is the practice of securing only the message contents, steganography is concerned with concealing the fact of sending a secret message , as well as protecting the contents of the message. When steganography is combined with encryption it provides high level for security.Encryption deals with converting the plain text into cipher text .Steganography deals with hiding the data under cover image .When both encryption and steganography is used it provides much security by encrypting the data and hiding it under cover image and transmitted.

2. LITERATURE SURVEY

Creighton T.R. Hager , "In Personal Digital Assistants Energy and Performance and Efficiency of Block Ciphers". On various kinds of data comparative analysis has been performed by the author of various encryption algorithms. This research has proved that blowfish performs all other encryption algorithms. The best and fast encryption algorithm than others is the Blowfish .

Gary C.Kessler, **"An Overview of Cryptography".** It is an old paper based on cryptography by Gary C. Kessler, and since then till date it was continuously updated . It was last updated in 2014. The author suggested again the great source for the cryptography algorithms. Before putting it in the use it is very important to understand the structure of the encryption algorithm.

Navita Aggarwal "Simultaneously performed Compression, Steganography and Encryption, and simultaneously and an efficient Pixel-shuffling Based Approach on images". The authors conducted the research, where it have applied encryption , compression, and steganography on the digital image data. Encryption algorithm Pixel shuffling based symmetric, compression algorithm as DCT , for Image steganography WinRAR are used to achieve the proposed model in the paper.

Verma O.P., Agarwal R., Dafouti D. "Performed Data encryption algorithms Analysis ", In this research , it have presented main characteristics that differentiate and identify one encryption algorithm from other is its ability to protect the data against attacks. This paper provides a comparison based on performance between most common encryption algorithms : Blowfish,AES ,DES, 3DES,. The comparison was done by running several encryption settings to evaluate the algorithm's encryption / decryption speed by processing different sizes of data blocks. Simulation has been conducted using C# language.

Abdouli A.S., "Experiment on hard problems along their cryptography application ", On security of several cryptosystems rests on different hard problems the authors have proposed an algorithm. Many cryptographic schemes are based on the number of theoretic problems such as factoring and discrete logarithms.. It is desired to investigate that have exponential complexity of both the ordinary and quantum new classes candidates of hard problems computers, for example, error correcting codes, lattice problems, and subset - product. In this paper, authors will focus on the hard problems and their implementation to cryptography.

Gunjan chugh. 'Technique of Image steganography , This paper presents, overview Steganography is described. In what way Steganography is different from cryptography is also discussed. In the stegnography, message is hidden under cover source where as in the cryptography message is encrypted but visible during the transmission. Iimage steganography different techniques with their r pros and cons such as Least Significant Bit (LSB), Making and Filtering, Parity Checker Method, discussed.
Jasleen Kaur and Deepankar Verma," Steganography technique" The different techniques data hiding and security are used to implement steganography using LSB,ISB, MLSB. LSB is the most widely used technique for steganography.

Rashi Singh and Gaurav Chawla," Image Steganography Review" The Paper provides the Steganography review, its history and working of Image Steganography along with various techniques of insertion used in Image Steganography, like Distortion Technique Masking and Filtering. Spatial Domain Methods,Transform Domain Technique. It also covers software of steganography and various applications such as copyright protection, secret communication, digital watermarking.
Mamta Juneja and Parvinder S. Sandhu ,"A Steganography Technique based on LSB for RGB Color Images" In this paper for steganography least significant bit(LSB) technique provides security .Also helps to hide in the location of pixel the encrypted data that is adjacent and random in locations in edges . The edges are detected by it in the cover image,then message bits are embedded in randomly selected edge area pixels with the least significant byte. It ensures that the attackers will not have any knowledge that message bits are hidden in the image.

PREVIOUS SYSTEM

The secure data storage on cloud environments is the primary requirement of such applications, where important because they belongs the users. These data, if hacked, can be used to defame a person's social data. Many times users have to share and send confidential information with others .Such confidential data can be hacked if not secured. Thus to protect the secret information encryption method can be used. Here we are proposing data encryption which will ensure the security. This algorithm will be used with the technique of steganography which helps in adding an extra layer of security of the data storage.

PROPOSED MODEL

In this paper, we proposed a hybrid data security model for the storage and communications on cloud, which is done by combining various techniques together for data security . Steganography and Encryption techniques are used. Stored data on cloud is first encrypted using AES algorithm and then the steganography is applied on encrypted data which is merged with cover image using least significant bit(LSB) method .In this method in image pixels of LSB data is hidden .If the LSB of the pixels are changed then it create not much difference in the image and thus the stego image seems same as the original image. The image is loaded ,then it is encrypted and hidden in the cover image .For cover image we get area using color illumination based estimation(CIBE).Then the encrypted image and cover image is merged using LSB. Then the data that is encrypted will become unreadable data.

3. CONCLUSIONS

In this paper we used the hybrid approach for security of data storage on cloud .Due to increasing development of internet technology it is necessary to secure the data stored by user on the cloud and maintain their confidentiality. For this we have encrypted the loaded image and cover image is used to hide it so that eavesdroppers are unable get the original content .Robustness of the data is increased. Spatial domain technique Least Significant Bit (LSB) substitution is commonly used. In this technique the secret message bits are used to replace the least significant bit of each pixel.

REFERENCES

[1] Hager, Creighton TR, Scott F. Midkiff, Jung-Min Park, and Thomas L. Martin. "Performance and energy efficiency of block ciphers in personal digital assistants in *Pervasive Computing and Communications, 2005. Per Com 2005. Third IEEE International Conference on*, pp. 127-136. IEEE, 2005.

[2] Kessler, Gary C. "An overview of cryptography." (2003).

[3] Agarwal, Navita, and Himanshu Sharma. "An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography. " *International Journal of Computer Science and Mobile Computing (IJCSMC)* 2, no. 5 (2013): 376-385.

[4] Verma, O. P., Ritu Agarwal, Dhiraj Dafouti, and Shobha Tyagi."Peformance analysis of data encryption algorithms."In *Electronics Computer Technology (ICECT) , 2011 3rd International Conference on*, vol. 5, pp. 399-403. IEEE, 2011.

[5] Abdouli, Ameera Salem, Joonsang Baek, and Chan Yeob Yeun. "Survey on computationally hard problems and their applications to cryptography." In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, pp. 46-52. IEEE, 2011.

[6] Gunjan chugh. 'Technique of Image steganography Jasleen Kaur and Deepankar Verma,"steganography technique "(May 2014) .

[7] Rashi Singh and Gaurav Chawla ," A Review on Image Steganography" (May 2014)

[8] Mamta Juneja and Parvinder S. Sandhu ,"An Improved LSB Based Steganography Technique for RGB Color Images".