Enhanced Cloud Data Security using Combined Encryption and Steganography

Acqueela G Palathingal [1], Anmy George [2], Blessy Ann Thomas [3], Ann Rija Paul[4]

[1,2,3] B.Tech Student, Dept. of Computer Science Engineering, Sahrdaya College of Engineering & Technology, Kerala, India
[4] Assistant Professor, Dept. of Computer Science Engineering, Sahrdaya College of Engineering & Technology, Kerala, India

---

Abstract - *Security has become a wide necessity in day-to-day life. Data security is the most obliged security of all. The data in our system is opened to high potential risks. Due to various security reasons we adopt diverse methods. Now we all are depending on cloud platform for security and storage but even it is vulnerable to various threats. The data inside cloud is not well-secured as it can be accessed by anyone who can attain our credentials and also the cloud providers has equal access that as of us. So we propose an enhanced security to the data using encryption and steganography. Here the data will be encrypted and hidden behind an image and hence uploaded to the cloud. Whenever felt necessary the image could be downloaded and the data can be decrypted to obtain back the original file. Our results provide augmented security to the data and can be used anywhere without qualms.*

Key Words: Cloud computing, Cryptography, RSA, Encryption, Decryption, DWT Steganography.

1. INTRODUCTION

The Cloud computing will be most important in Internet of Services and computer infrastructure. Both applications and resources are delivered to the Internet as services only on demand in the cloud computing environment. Cloud Computing is cost- effective, very flexible, and it provide delivery platform to either business or consumer IT services over the Internet. There are two basic types of functions in Cloud computing. They are computing and data storage. The Cloud models are Infrastructure as a service (IAAS) which is for executing services by sharing the resources of hardware, by using the technology of virtualization. Platform as a service (PAAS) which offers a execution environment in software like an application server. Software as a service (SAAS) which completes all the application is on the internet. Cloud computing can be adopted by users and enterprise. To make this adaptation, the user's security concerns should be rectified first to make cloud environment trustworthy. The basic requirement to win the user's requirement is that the trustworthy environment. In cloud computing environment, Data security is more complicated than data security in the traditional information systems. Cloud Computing security is one that is more important to be addressed nowadays. If security measures are not provided properly, then Data operations and transmissions will be at high risk. To handle these challenges, strongest security measures are to be made and it has to be implemented by identifying security challenge and its solution.

To recognize the tangible and intangible threats related to its use these securities, privacy will be used. There are some of the major issues in the cloud computing environment and it as follows: resource management, resource monitoring and resource security. A data security framework for cloud computing networks is proposed.

The privacy will be used to study about the tangible threats and also the intangible threats, Some of the issues in data security were privacy of data, protecting the data, availability of data, etc. The various challenges in the security were loss of data, data threats and malicious attacks from outsiders. The most challenging issue in cloud computing is data sharing [1].

2. SYSTEM DESIGN

The work is dividing into mainly 3 parts. The first part is to encrypt the file. The second part is to hide the encrypted data behind an image. The third part is uploading the image to the cloud. Whenever necessary the image can be downloaded from the cloud platform and then the data can be extracted and hence decrypted to get the original file.

2.1 Encryption

Encryption is the process to converting data or information (plaintext) into another form, called cipher text, which cannot be easily understood by anyone except authorized person. Decryption is the process to converting cipher text back into plaintext. The main purpose of encryption is to secure the confidentiality of digital data stored on computer systems or transmitted via other computer on network (internet). In process of encryption and decryption we generate a key to time of data encryption and use same or different key to decrypt the data.

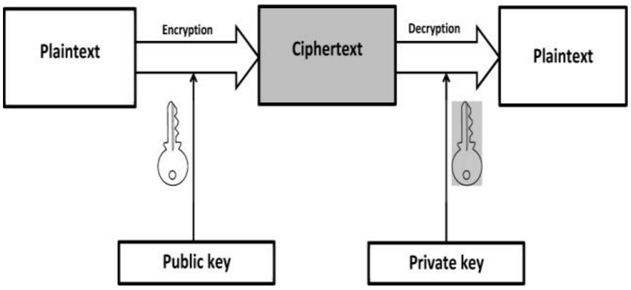


Fig -1: RSA encryption system model

In this system RSA (Rivest-Shamir-Adleman) is used for encryption process. Files are taken from the system and are encrypted using this technique. Thos is a public key cryptography where mainly 2 keys are used i.e., one for encryption and the other for decryption. On the encryption side we use to encrypt using the public key whereas in the decryption face we use the private key.

2.2 Steganography

Steganography is communication that uses the technique of cloaked writing that aims at hiding the existence of any message or data. Steganography has been in use for secret communication since ancient times in multiple forms. In this technological era it is deployed for secured transfer of data over digital channel in which the information is hidden in some media. The information can be hidden in image, text, audio or video and are called image steganography, text steganography, audio or video steganography respectively.

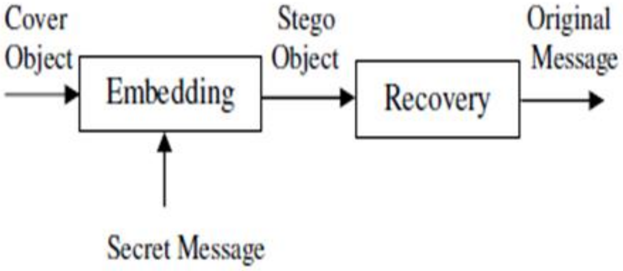


Fig – 2: Steganography model

In this system steganography plays an important role. We are using DWT Steganography. The secret message with the cover image is given as the input and it is embedded together to form the stego object. This can be retrieved by extraction process to acquire the original image and also gives back the message. It does the role of hiding data.

2.3 Cloud Platform

Cloud is the environment where are opting for saving the files and documents. It is basically a storage where all our vital information is kept and acts as a backup in case of system failure. There are diverse cloud service providers nevertheless the data inside cloud is never safe. It is necessary that our information must be confidential and should not be disclosed easily.

3. IMPLEMENTATION

In this paper, we have used two techniques RSA encryption and DWT steganography. These techniques give enhanced security for the data. Each technique has its own algorithms.

3.1 RSA Encryption

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key Generation

1. Two large distinct prime numbers p and q are chosen at random using primality tests. This makes factoring harder.
2. Evaluate the modulus n as n = pq and then find φ(n)
3. Now we choose our public key (say 'e') such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$ as the public key exponent.
4. And now for the private key exponent, we find d such that $d = e - 1 \bmod \varphi(n)$.
5. Thus we have: The public key consisting of the modulus n and the public (or encryption) exponent e. And the private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

Encryption

1. Both A and B agree upon a padding scheme (reversible protocol).
2. A sends his/her public key (n, e) to B but keeps the private key d a secret.
3. If B now wants to send a message M to A, B converts the message M into an integer m using the padding scheme B the computes the cipher text C as $C = M^e \bmod n$ B then transmits C to A.

Decryption

1. A recovers the integer M from C as $M=C^d \bmod n$.
2. Given m, A recovers the original message M by reversing the padding scheme [2].

3.2. DWT Steganography

The proposed architecture deals with the separable 2-D DWT, whose mathematical formulas are defined as follows [3]:

$$x_{\mathrm{LL}}^{J}(n_1,n_2) = \sum_{i_1=0}^{K-1}\sum_{i_2=0}^{K-1} g(i_1)\cdot g(i_2)\cdot x_{\mathrm{LL}}^{J-1}(2n_1-i_1)(2n_2-i_2) \quad (1)$$

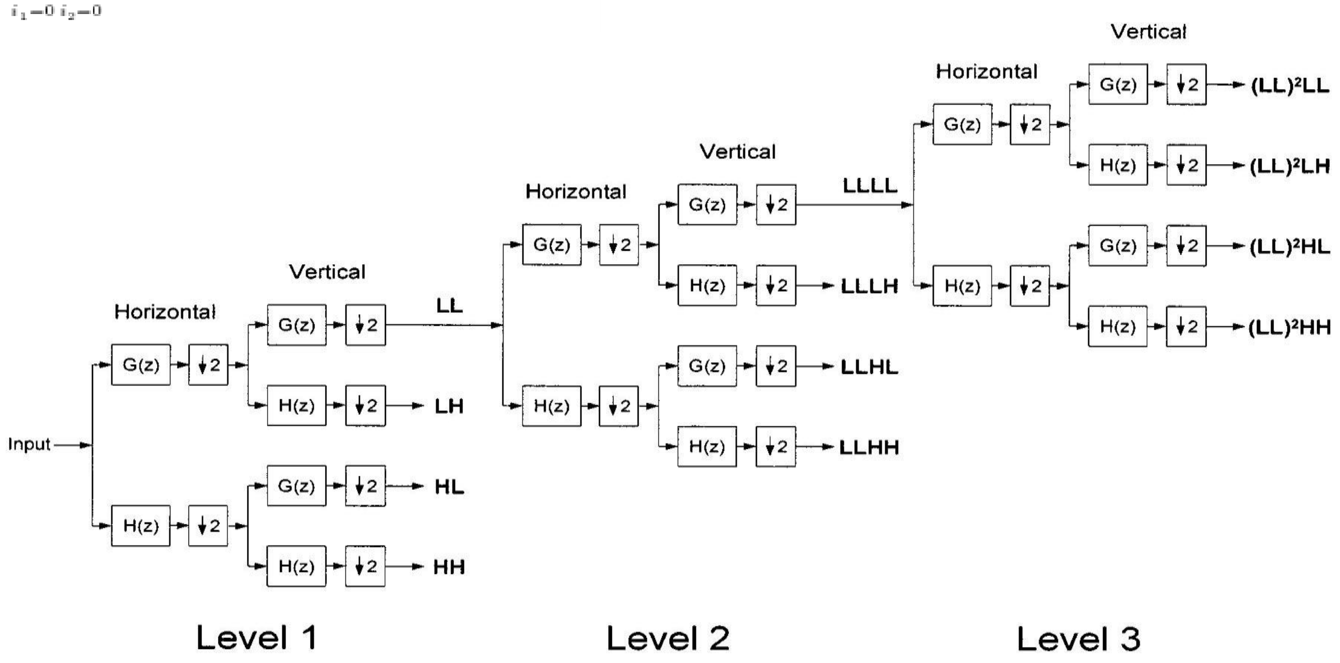
$$x_{\mathrm{LH}}^{J}(n_1,n_2) = \sum_{i_1=0}^{K-1}\sum_{i_2=0}^{K-1} g(i_1)\cdot h(i_2)\cdot x_{\mathrm{LL}}^{J-1}(2n_1-i_1)(2n_2-i_2) \quad (2)$$

$$x_{\mathrm{HL}}^{J}(n_1,n_2) = \sum_{i_1=0}^{K-1}\sum_{i_2=0}^{K-1} h(i_1)\cdot g(i_2)\cdot x_{\mathrm{LL}}^{J-1}(2n_1-i_1)(2n_2-i_2) \quad (3)$$

$$x_{\mathrm{HH}}^{J}(n_1,n_2) = \sum_{i_1=0}^{K-1}\sum_{i_2=0}^{K-1} h(i_1)\cdot h(i_2)\cdot x_{\mathrm{LL}}^{J-1}(2n_1-i_1)(2n_2-i_2) \quad (4)$$

The two dimensional Discrete Wavelet Transform (DWT) is an important function in many multimedia applications, such as JPEG2000 and MPEG-4 standards, digital watermarking, and content-based multimedia information retrieval systems. The 2D DWT is computationally intensive than other functions, for instance, in the JPEG2000 standard.

Here we are using the two dimensional discrete wavelet transform.



Fig–3: DWT steganography model

Where,

J	2-D DWT level;
K	filter length;
$g(n)$	impulse responses of the low-pass filter $G(z)$;
$h(n)$	impulse responses of the high-pass filter $H(z)$;
$x_{\mathrm{LL}}^{0}(n_1,n_2)$	input image.

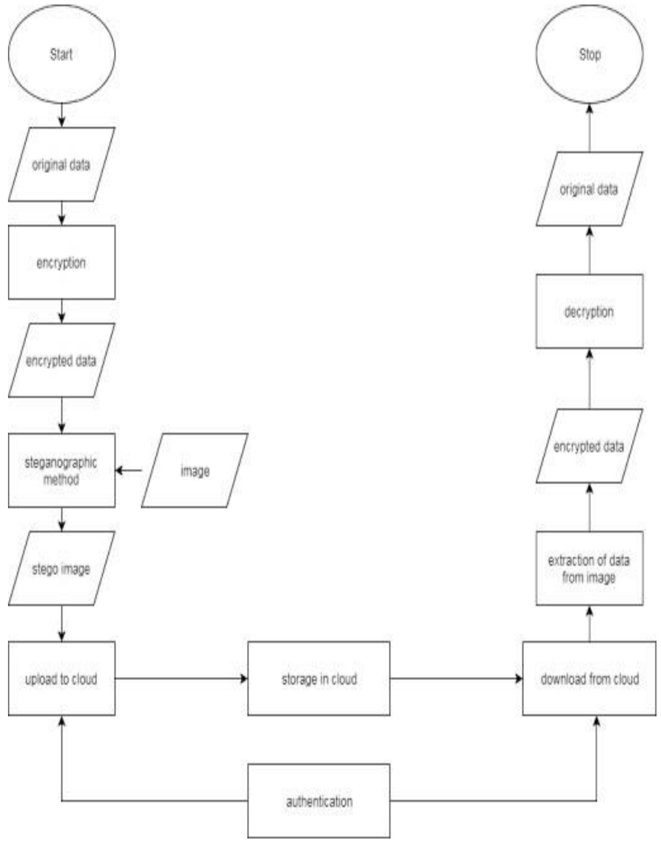


Fig – 4: Flowchart of the system

To make sure of the data security we must use these techniques. The original data is taken from the system. This data is encrypted using RSA encryption then an image is selected where this encrypted data will be hidden and hence obtaining a stego object. This stego object is later uploaded to the cloud sever. Whenever you feel necessity for the file, the image is downloaded from the cloud and data is extracted from the image obtaining the original image. The data is hence decrypted to obtain the original file back for which again RSA is used for decryption process.

The encrypted data will be in the form of ASCII codes. Each character in the file is converted to ASCII codes on encryption. On decryption, again the combination of prime numbers should be given. If invalid combination of keys is given then it leads to error and henceforth it provides security.

4. RESULTS AND DISCUSSION

This project resulted in development of a noble venture to ensure security in cloud computing. The 'CLOUD DATA SECURITY' enables to make sure the security of data. The main techniques used are encryption and steganography in which we evaluate and verify data. This ensures multilevel security mechanisms of the data. Thus certifying fortification of data over cloud computing. This project paved an opportunity to develop an application which is of use to the society.

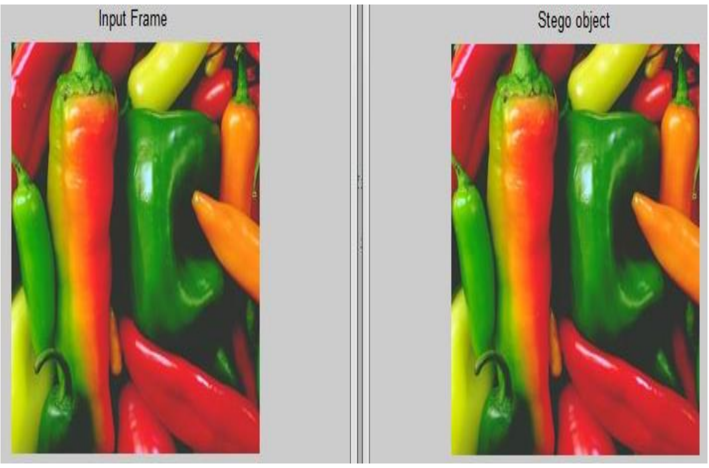


Fig – 5: Comparison between input image and stego-object

This figure shows the comparison of the input image and the stego object, where the encrypted data is hidden into.

5. CONCLUSION

Modem area of information technology is fully based on online service or web services. Our project deal with security problems in cloud computing systems and how they can be prevented, here we use cryptography and Steganography method together to secure data. RSA algorithm is more secure than other algorithm. We integrate RSA algorithm with other algorithm to provide more security to data. In Steganography process we get encrypted image, which looks exactly the same to original image by human eye. If we analysis the image binary codes then the differences would be seen. Otherwise we are unable to identify the original image. The approach we have use in this paper, will help to make a strong structure for security of data in cloud computing field.

REFERENCES

[1] Dr. K.B.Priya Iyer , Manisha R , Subhashree R ,Vedhavalli K "ANALYSIS OF DATA SECURITY IN CLOUD COMPUTING" International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics,2016 IEEE

[2] Nentawe Y. Goshwe Arham Chopra ,"Data Encryption and Decryption Using RSA Algorithm in a Network Environment".

[3] Po-Cheng Wu and Liang-Gee Chen "An Efficient Architecture for Two-Dimensional Discrete Wavelet Transform" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 11, NO. 4, APRIL 2001.