International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 4 No: 3 March 2019

Cloud Information Security using and Steganography Paired Encryption

[1]Emmanuel O.C Mkpojiogu, [2]Aliza Sarlan
[1]Department of Computer and Information Technology, Universiti Sains Malaysia, Penang, Malaysia
[2]Software Quality and Quality Assurance (SQ2E) Research Cluster, Universiti Teknologi Petronas, Perak, Malaysia

Abstract: In everyday life, security has become a wide necessity. The most obligatory security of all is data security. Data is opened to high potential risks in our system. We adopt various methods for various security reasons. Now we all depend on the security and storage cloud platform, but even it is vulnerable to different threats. The cloud data is not good-secured as it can be accessed by anyone who can reach our credentials, and cloud providers also have equal access to us. Thus, using encryption and steganography, we propose enhanced data security. Here the data is encrypted and hidden behind an image and subsequently uploaded to the cloud. The image could be downloaded whenever it felt necessary and the data can be decrypted to retrieve the original file. Our results provide improved data security and can be used smoothly anywhere.

Keywords: DWT Steganography, Cost- effective, Very flexible, private key, public key, RSA.

1. INTRODUCTION

In the Cloud computing will be the most important Internet services and computer infrastructure. Both applications and resources in the cloud computing environment are delivered to the Internet as services only on demand. Cloud computing is cost - effective, very flexible and provides either business or consumer IT services on the Internet with a delivery platform. In cloud computing there are two basic types of functions. They are storage of computers and data. The cloud models are Infrastructure as a Service (IAAS), which is used by virtualization technology to execute services by sharing hardware resources. Platform as a service (PAAS) offering software - like ecosystem execution of application servers. Software as a service (SAAS) that completes the entire application is on the internet. Cloud computing can be adopted by users and corporations. In order to make this adaptation, the security concerns of the user should first be corrected in order to make the cloud environment confident. The basic requirement for winning the requirement of the user is that the environment be trustworthy. In the cloud computing environment, data security in the traditional information systems is more complicated than data security. The security of cloud computing is one that is more important to address today. If security measures are not properly provided, then high risk will be associated with data operations and transmissions. Strongest security measures must be taken to address these challenges and implemented by identifying and solving security challenges.

Privacy will be used to Approval of tangible and intangible threats associated with its use of these securities. In the cloud computing environment, there are some of the major issues and the following are: Management of wealth, monitoring of wealth, and security of wealth. A framework for data security is being proposed for cloud computing networks.

Privacy will be used to verify tangible threats as well as intangible threats, data privacy, data protection, data availability, etc. were some data security issues. Data loss, data threats and malicious attacks from outsiders were the various security challenges. Cloud computing's most challenging issue is data sharing[1].

2. SYSTEM DESIGN

The work is mainly divided into three parts. The first part is the encryption of the file. The second part is to hide behind a picture the encrypted data. The third part is the cloud upload of the image. The image can be downloaded from the cloud platform whenever necessary and the data can be extracted and thus decrypted to obtain the original file.

A. Encryption

Encryption is the system for converting data or information (plaintext) into a different form, called cipher text, that

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 4 No: 3 March 2019

anyone other than the authorized person can easily understand. The process of converting cipher text back to plaintext is decryption. The primary purpose of encryption is to ensure the confidentiality of digital data stored on computer systems or transmitted via other computers on the network (internet). In the process of encryption and decryption, we generate a key to data encryption time and use the same or different key to decrypt data.

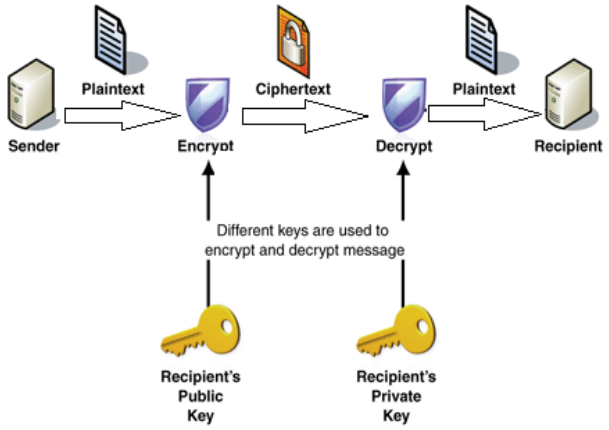

Figure 1. RSA encryption system model

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

B. Steganography

Steganography is communication that uses the technique of cloaked writing to hide any existing message or data. Since ancient times, steganography has been used in several forms for secret communication. It is deployed for secure data transmission over the digital channel in this technological era in which the information is hidden in some media.

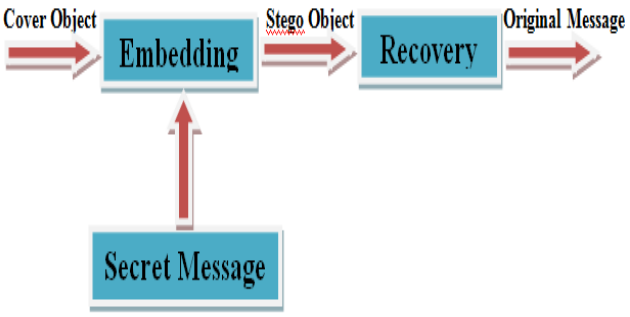

Figure 2. Steganography model

Steganography plays a major role in this system. We use steganography from DWT. The secret message with the cover image is given as the input and to form the stego object it is embedded together. In order to acquire the original image, this can be retrieved by extraction process and also returns the message. It does the hiding data role.

C. Cloud Platform

Cloud is the environment where files and documents are stored. It is basically a storage where all of our vital information is stored and when system failure occurs it acts as backup. However, the data inside the cloud is never safe, there are various cloud service suppliers. Our information should be confidential and should not be easily disclosed.

3. IMPLEMENTATION

We used two RSA encryption techniques and DWT steganography in this paper. These techniques provide increased data security. Each technique has algorithms of its own.

A. RSA Encryption

There are three steps in the RSA algorithm: key generation, encryption and decryption.

Significant generation

- Using primality tests, two large distinct prime numbers p and q are selected at random. This makes it harder to result.
- Evaluate the n module as $n = pq$ and find $\varphi(n)$
- And now we find d as such for the private key exponent that $d = e - 1 \bmod \varphi(n)$.

Encryption

Both A and B agree on a reversible protocol time scheme. A sends its public key (n, e) to B but keeps a secret about the private key. If B now wants to send a message M to A, B uses the padding scheme B to convert the message M to an integer m and then calculates the cipher text C as C = Me mod n B and transmits C to A.

Decryption

As M = Cd mod n, A recovers the integer M from C. Given m, by reversing the padding scheme, A recovers the original message M[2].

B. DWT Steganography

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 recovery systems. For example, the 2D DWT is computationally intensive in the JPEG2000 standard compared to other functions.

We're using the discrete two - dimensional wavelet transformation here.

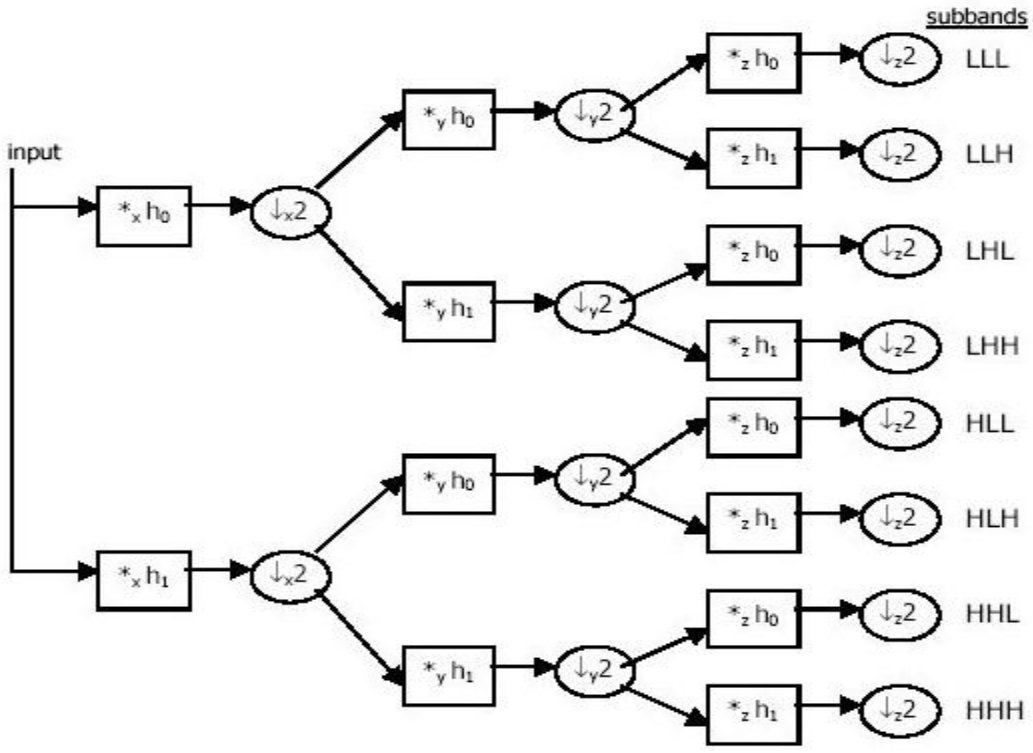

Figure 3. DWT steganography model

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 4 No: 3 March 2019

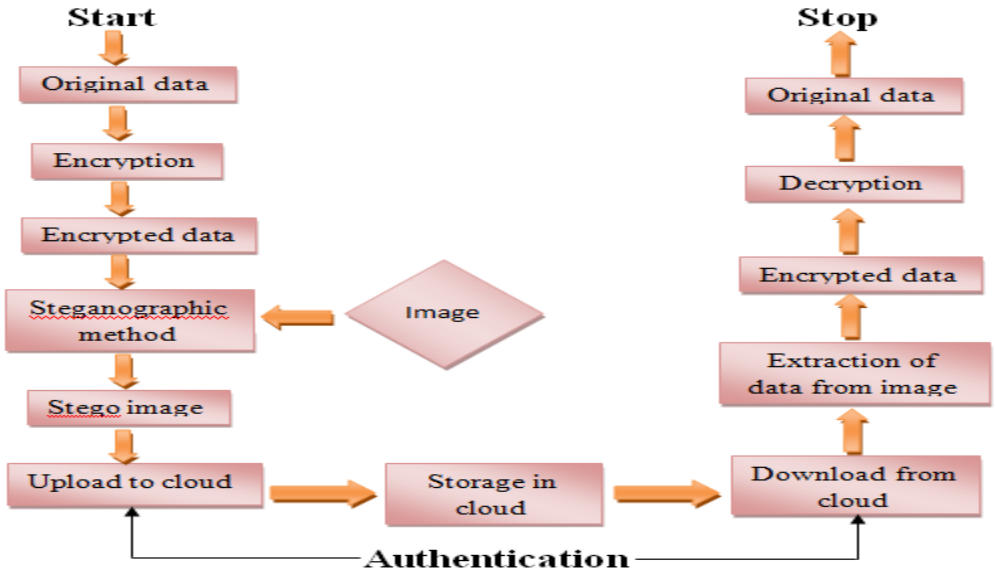

Figure 4. Flowchart of the system

These techniques must be used to ensure data security. The original data is taken from the system. This data is encrypted using RSA encryption, then an image is selected where this encrypted data is hidden and a stego object is obtained. This stego object is subsequently uploaded to the sever of the cloud. The image is downloaded from the cloud whenever you feel the need for the file and data is extracted from the image that gets the original image. Therefore, the data is decrypted to get back the original file for which RSA is again being used to decrypt.

The data will be encrypted in the form of ASCII codes. Every character in the file is converted on encryption to ASCII codes. The combination of prime numbers should be given again on decryption. If invalid key combination is given, it leads to error and provides security from now on.

4. RESULTS AND DISCUSSION

This project led to a noble venture being developed to ensure cloud computing security. The ' CLOUD DATA SECURITY ' ensures data security. Encryption and steganography are the main techniques used in which we evaluate and verify data. This ensures data security mechanisms at multiple levels. Certifying data fortification over cloud computing. This project paved an opportunity to develop a society - friendly application.

Figure 5. Comparison between input image and stego-object

This figure shows the comparison between the input image and the stego object, where it hides the encrypted data.

5. CONCLUSION

The area of IT modems is entirely based on online service or web services. Our project addresses security issues and how they can be prevented in cloud computing systems. We use cryptography and steganography together here to secure data. RSA is a safer algorithm than any other algorithm. To provide more data security, we integrate the RSA algorithm with other algorithms. We get encrypted image in the Steganography process, which by human eye looks exactly the same as the original image. If we analyze the binary image codes then we will see the differences. Otherwise, the original image cannot be identified. In this paper, the approach we use will help make cloud computing a strong data security system.

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.

