International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on Smart Cities (ICSC-2019)
Volume-05, Special Issue_March_2019.

Fortifying Cloud through Steganography

Payal Garg[1], Lalita Cahudhary[2], Hradesh Kumar[3]

[1] *GL Bajaj Institute of Engineering and Technology,*
[2] *I.T.S Engineering College*
[3] *I.T.S Engineering College*

***Abstract.** The rising trends of computer technology in collaboration with Internet services has boosted the aeon of cloud computing. But with everything positive comes something negative. As cloud computing is an asset for the IT industry as well as for the individual users, but it is also a liability as it leads to various security issues. Till date many cryptographic techniques are being used to secure the data at rest. The strongest cryptographic algorithms which are being used are AES (Advanced Encryption Standard), DES (Data Encryption standard) for symmetric encryption, ECC (Elliptic Curve Cryptography) and RSA for asymmetric encryption. For ensuring data security of the stored data, we have proposed to secure the data with stereography instead of regular cryptographic techniques from unauthorized access. This scheme is expected to work perfectly for storing the data at cloud and successfully retrieving the data.*

***Keywords:** Cloud computing, Stenography, Security*

1 Introduction

Cloud computing can be defined as the technology which enables the user to remotely access the data, store the data and manipulate the data as well. [2] It gives the liberty to the user to use the infrastructure and the services without the service provider's interaction. In cloud computing it is not necessary that the person who is using cloud must own his own cloud. The user has to pay only for the services which he avail. The prime goal of cloud is to let their customers use the cloud services and infrastructure instead of their resources to reduce the resource budget.

A cloud has various traits. The chief trait of it is: it's capability to store huge amount of data at the cloud storage centers. The cloud service provider provides the storage as per the user's need and charge him accordingly. But many of the IT industries are still not able to adopt cloud computing as they question about the security and privacy control issues of the cloud. The security issues of the cloud are always controversial as per the outlook of many IT industries.

From the point of view of security of the data which is the paramount facet of cloud computing, there are innumerable threats which cannot be overlooked. Firstly, the long-established cryptographic techniques cannot be appropriate for security of the data at the cloud because the user will lose control over the data. Thus we need a system which insures security without explicit exposure of the whole data. Secondly, the data at cloud is operated dynamically. Various operations such as insertion, deletion, modification, recovery and so on are performed. Hence advanced methodology must be adopted which does not compromise in data quality and assure security too. In addition to all the foregoing, the data at the storage centers is accessed simultaneously in a cooperated and distributed manner. The data of each individual user is remotely stored at different physical locations. Thus, it becomes important to follow the distributed protocols for correct storage and achieving robust system for cloud computing.

For a better and much enhanced security system, we have proposed to hide the user's data in images. Instead of using the conventional or regular cryptographic techniques we will use prominent technique which is stenography. Stenography can be defined as the technique in which we hide the data in the images by using appropriate algorithm. Steganography is the exalt technique in comparison to existing cryptographic techniques. This proposed system almost guarantees coherent storage of data at cloud. [1]

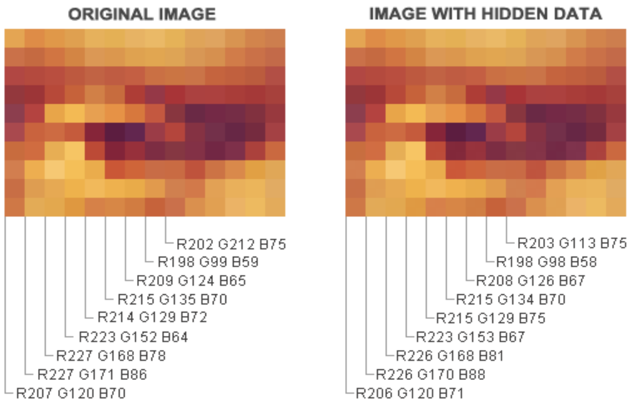

Figure 1: Difference between images and pixels before and after Steganography.
(Source: http://www.easysector.com/secretlayer)

As stated by our survey, this methodology is not incepted so far. This combination of technologies can enhance security quality. And it can also act as add on to the security approaches.

2 Framework of the cloud

The architecture of the cloud is described by mainly two models: service delivery model and deployment model. The service delivery models of the cloud are Infrastructure as a Service (IAAS), Platform as a Service (PAAS) and Software as a Service (SAAS)

- IaaS: This model provides the cloud user a virtual interface which enables the cloud user to use all cloud resources such as network, server, storage etc. The user is charged on the basis of resources used, storage done, CPU utilization, consumed network bandwidth and so on. This charge is known as usage charge. Example: Amazon S3, Amazon EC2, Layered tech and etc.
- PaaS: This model provides either runtime environment or application deployment framework to the users who are generally developers. They developers can directly develop the application/program, testing can also be done and deployment can also be done. This service model is useful for developers, application deployer, testers and so on. Example: IBM smart cloud, Google app engine, Microsoft Azure, salesforce.com, jelastic.com etc.
- SaaS: In this service model the cloud user directly access the software over the network. He can use the software anywhere and anytime. This model dedicated to the end users. The person using this service model does not need to have much knowledge about cloud because these software works as a general web applications. Example: Gmail, YouTube etc.

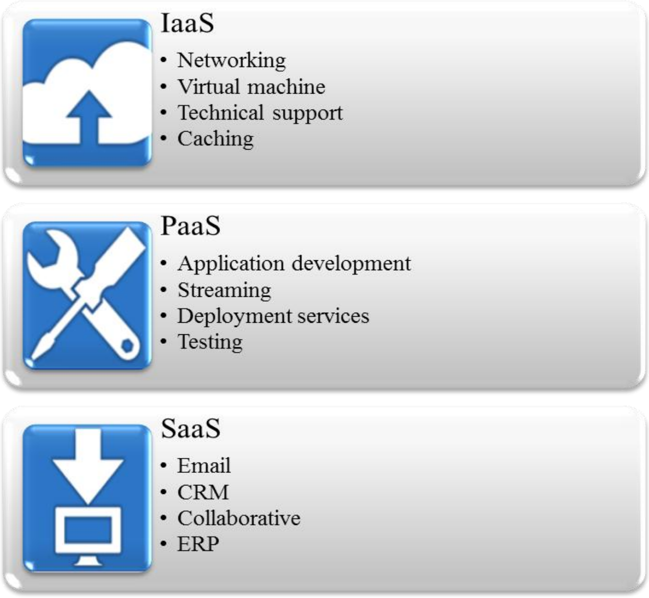

Figure 2: Service delivery models of cloud and their Applications.

The deployment model can be categorized into four major categories are private cloud, public cloud, hybrid cloud and community cloud.

- Private cloud: When an organization owns his/her own cloud then such a cloud is known as private cloud. The organization holds all the rights of the cloud.
- Public cloud: When a cloud is publically accessible and all the users are charged as per they avail the services then such a cloud is known as public cloud. The third party vendor of the cloud holds all the rights of the cloud. The vendor is the policy maker for the cloud.
- Hybrid cloud: A hybrid cloud comprises of public cloud as well as private cloud. In other words, we can say that a hybrid cloud is the combination of both. All the rights of the cloud are reserved by the vendor.
- Community cloud: When several organizations use a common cloud and hold equal rights, such a cloud is known as community cloud. [5]

After the foregoing discussion, it is very much clear that due to different deployment models it becomes more typical to provide security at foremost level. Also it is very much important to achieve foremost level of security because it is the significant reason for abandonment of cloud computing even by trending IT industry. The well-known security issues, active attacks and passive attacks possess threats to the user’s data. These threats are required to be tackled in an efficient manner with appropriate technique.

3 Problem Statement

The major issues with stored data of the cloud are loss of control over the data and unauthorized user access simultaneously. The regular cryptographic techniques offer two processes serially i.e. encryption and decryption respectively. Each encryption and decryption algorithm possesses a key which is known as encryption key or decryption key respectively. If any user with malicious intent gets any of them, then the original data can be fetched. Thus the cryptography technique fails. To overcome this problem we have approached to hide the data in images. As there will be no key to encrypt or decrypt the data, so this issue of malicious intend will fail.

a. *System Design*

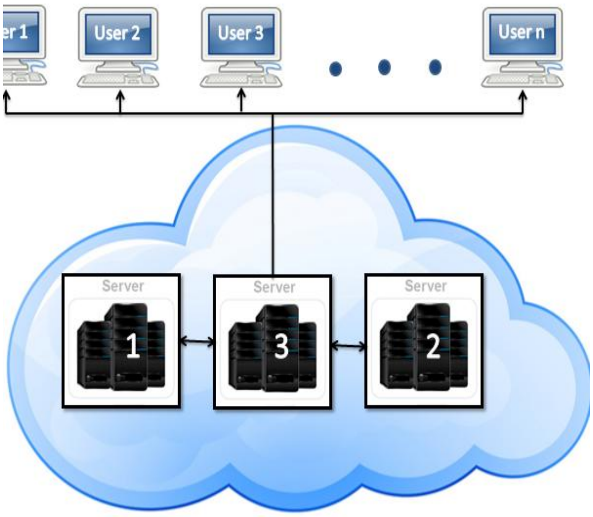

Figure 3: Architecture of the proposed system.

In our proposed system, the architecture mainly comprises of three servers and 'n' number of users. There are three servers namely Server 1, Server 2 and Server 3. Server 1 is responsible for handling the databases. Server 2 is responsible for algorithms. And Server 3 performs all the computation and processing. The 'n' user depicts the various users of the cloud. They can either be individual users or organizations. The major concept is that the users store their data on cloud on which stenography is performed to secure the data.

b. *Prerequisites for the System*

For the evolution of the above system, the major pre-requisites are an image databases, file database, efficient searching and sorting algorithms. In advance we need to maintain an image database in which we store gray scale images of various sizes in which we will later on hide the data. A separate file database is to be maintained to keep track of all the images in which the data is stored. Searching and sorting algorithms will be used to select the image of appropriate size according to the data to be hidden.

c. *System Working*

The figure below depicts the working of the system.

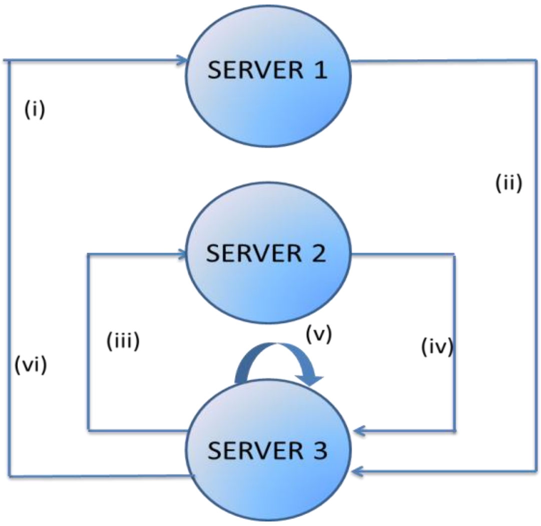

Figure 4: Flow diagram of System Functioning.

After receiving the data from the user, the above depicted process needs to be followed. The systematic process of the system is described below sequentially:

Server-3 requests an image from the image database from Server-1.
Server-3 accepts the image sent from the image database.
Server-3 requests the algorithm for hiding the data into the image from Server-2.
Accepting the algorithm from Server-2 and perform further processing.
Processing the image i.e. hiding data into the image by Server-3 itself.
Storing processed image to another database at Server-1.

d. *Design Goal*

It is the weakness of the human sight system that it cannot detect the minute variation in every pixel of gray scale images. By taking this as advantage to our system we proposed this system in which we hide the data of the files in the gray scale images. By doing so we have achieved the following:

Correctness: The data which is stored in the images can be hidden in the images and when they are retrieved back they will be in correct form.

Availability: *The user who has the authority of that data can readily retrieve data anytime from anywhere.*
Protection: *Only the authorized user can access the data by successfully retrieving it. The person with malicious intend will not be able to identify the concept.*

4 Security Analysis

a. *Server 1*

At Server-1, we have maintained the databases which store all the grayscale images. Even if the person with malicious intend identify the correct images; he will not be able to identify the correct data format. Thus he will not be able to retrieve the correct format of the information.

b. *Server 2*

At Server-2, we maintain the codes of various algorithms for searching and data hiding. The person this only access to these cannot be able to successfully retrieve the data because algorithms alone do not solve the purpose till he is not aware of the exact images.

c. Server 3

This server is connected to Server-1 and Server-2. This server is responsible for all the operations, computations and processing. As only computations are taking place at this server so any interruption cannot be able to retrieve the information. All the images will be removed from this server after the process.

5 Literature Survey

Stenography and cloud computing, both are prominent fields of oneself for the researchers. Stenography acts as an advantage over regular cryptographic techniques. Thus using them in collaboration will result in positive results. Some of the constructive and outstanding efforts are:

- G. Shaik Abdullah and B. Muthulakshmi [7] have applied stenography with simultaneous implementation of with cryptography and referred it as twin stenography. This model is robust enough to conduct distinguishable challenges. In this model each owner of the data first registers in the service provider cloud. They have to conform Thumb finger print and Aadhaar Card Number. Both the details are stored in Security as a service cloud. The key provider as a service cloud provides the key to the owner of the data to access the data later on. Separate cloud servers are maintained for storing the information as well as creating key for the data owner. The user needs to pass the authorization security check, only then he can access the data using the private security key.
- *Another research work "Triple Security of Data in Cloud Computing" was implemented by Garima Saini and Naveen Sharma. [10] Their work proposed to implement three algorithms, that is: AES (Advanced Encryption Standard), DSA (Digital Signature Algorithm) and steganography in collaboration with each other to the cloud network. Firstly they applied DSA for the data authentication. Secondly, they used AES algorithm for encryption of data. Lastly, by using steganography to hide the data in the audio files they developed a durable model. This model provides three layer authentications to the system. But the time complexity of the system was quite high, which is expected to be reduced in future work.*

6 Conclusion

After the foregoing discussion above, we conclude that we have studied the basic framework, service delivery models, deployment models, functioning of the cloud and security issues of the cloud thoroughly. In addition to this we have also compared that how stenography can dominate the tradition cryptographic techniques. On the basis of which we proposed this system in which we have applied the concept of stenography on the data at rest at cloud servers to secure the data which was previously confined to distributed systems only.

Some of the milestones which have been set up till now related to this work are mentioned in the literature survey. The models were successful enough to meet their mentioned goals. But they hold some of the drawbacks which could be eliminated using the proposed system. This system is different from existing approaches as it only deals with data at rest and not with dynamic data. But this stratagem is applied on compact system. But adopting such methodologies will leads to customer contentment. This can attract more IT industries to embrace cloud computing at significant level.

In this paper, we are only confined to gray scale images in a compact system. After observing more stenography simulations on RBG image we hope to develop a system in which stenography can be performed on the RBG images. This can help in providing a more robust system. Stenography on RBG images will be a better approach. It will be an extension to our proposed system.

7 Acknowledgement

This polite gesture is to show my gratitude to my mentors for helping me. I am exceedingly grateful to Ms. Lalita Chaudhary (Assistant Professor at I.T.S.Engineering College, Greater Noida.) for her cardinal time and knowledge. She has guided me throughout my research work as well as she helped me with thorough study of the concepts. heading and should not be assigned a number.

8 References

[1] Latika and Yogita Gulati, "A review of Steganography and Research and Development", IJARCSSE, volume 5, Issue 4, ISSN: 2277128X.

[2] Kui Ren, Con Wang, Qian Wang, and Wenjng Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International workshop on Quality of service, USA, pp1-9, 2009, IBSN: 978-42443875-4.

[3] Tahir Ali and Amit Doegar, "A novel approach of LSB based Steganography Using Parity Checker", IJARCSSE, ISSN: 2277128X.

[4] Shyam Nandan Kumar, "Cryptography during Data Sharing and Accessing over Cloud", *International Transaction of Electrical and Computer Engineers System* 3.1 (2015): 12-18.

[5] Suruchee V. Nandgaonkar and Prof. A.B. Raut, "A Comprehensive study on Cloud Computing", IJCSMS, ISSN: 2320-088X.

[6] Rosziati Ibrahim & Teoh Suk Kaun, "Steganography Algorithm to Hide Secret Messages inside an Image", Computer technology and application 2 (2011) 102-108.

[7] G. Shaik Abdullah and B. Muthulakshmi, "A Novel Proofless Public Key Encoding Scheme for Secure Information Sharing in Cloud using Twin Image Steganography", IDOSI, ISSN: 1990-9233(2015).

[8] Dr. M.Umamaheshwari, Prof.S.Suivasubramaniam & S. Pandiarajan, "Analysis of Different Steganographic Algorithm for Secured Data Hiding", IJCSNS, Vol.10 No. 8.

[9] V. Spoorthy, M. Mamatha & B. Santosh Kumar, "A Survey on Data Storage and Security in Cloud Computing", IJCSMC,ISSN:2320-088X

[10] Garima Saini and Naveen Sharma, "Triple Security of Data in Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 825-5827, ISSN: 0975-9646

[11] Simi Gupta, Kamal Kumar Sharma & Surjeet Dalal, "Multi Objective Parameters for Real Time Scheduling in Cloud Computing", IJRAEM, ISSN:2348- 6627

[12] T. Swathi, K. Srikanth & S. Raghunath Reddy, "Virtualisation in cloud", IJCSMC, ISSN:2320-088X

[13] Kelvin Hamlen, Murat Kantarciouglu, Latifur Khan & Bhavani Thuraisingham, "Security Issues in Cloud Computing", IJISP 4(2):39-51.

[14] B. Arun & S. K. Prashanth, "Cloud computing Security using Secret Sharing Algorithm", IJR, ISSN: 2250-1991.

[15] M. Vijayapriya, "Security Algorithm in Cloud Computing", IJCSET.