Increasing Security for Cloud Computing By Steganography in Image Edges

Hassan Hadi Saleh
College of Physical education and sport sciences, University of Diyala, Iraq.

Articleinfo
Received
22/2/2016
Accepted
22/6/2016

Keywords:
Cloud Computing,
Data Storage,
Security,
Steganography,
Edges of image.

ABSTRACT

The security of data storage in “cloud” is big challenge because the data keep within resources that may be accessed by particular machines. The managing of these data and services may not be high reliable. Therefore, the security of data is highly challenging. To increase the security of data in data center of cloud, we have introduced good method to ensure data security in “cloud computing” by methods of data hiding using color images which is called steganography. The fundamental objective of this paper is to prevent "Data Access” by unauthorized or opponent users. This scheme stores data at data centers within edges of color images and retrieves data from it when it is wanted.

الخلاصة

يعطي هذا البحث نظرة معلوماتية عن اهمية زيادة أمن المعلومات المتواجدة في مراكز خزن البيانات في السحابة الحاسوبية كونها معرضة الى السرقة ، التعديل ، الاستخدام الغير مخول . زيادة الامنية من خلال بناء نظام برمجي يقوم بإخفاء المعلومات الحساسة في حدود صور ملونة بشكل عشوائي قبل ارسالها الى مركز خزن البيانات في السحابة الحاسوبية وبالإمكان استرجاعها فقط من قبل الشخص. ان الهدف الاساسي للنظام هو منع الخصم من الوصول الى البيانات المخزونة في مراكز حفظ البيانات في السحابة الحاسوبية.

INTRODUCTION

Cloud Computing is a very known and still a very important model for enabling convenient, on demand network access to a shared pool of configurable computing resources [1, 2]. Big issue in cloud computing is a security; when our data is present in any server, there is a biggest chance of our data to be attacked [3]. Data must be secure during all processing stages including: *storing*, *processing*, and *uploading* [4].

Clients can store large amount of data in cloud data storage centers; but many users are not implement cloud computing, because the weakness in protection of data [5]. Secure data transformations on Internet has been a dream since the emergence of the Internet [6]. The good method to make secret data secured in "cloud" is to hide data in an image, audio, or video by Steganography techniques.

In this paper, we proposed data hiding system to increase the security of data in transmitting and increase to increase the security of data in residing in the "cloud". We increased the security of data by hide it within edges of color image. When these color images are keeping in *cloud data centers*, cannot view the original content of message by unauthorized.

The term *cloud* refers to a network or internet. The other words, we can say that cloud is something which is present at remote location.

Cloud computing refers to manipulating, configuring and accessing the application online. Cloud Computing offers online, data storage, infrastructure, and applications [7].

Data stored in cloud means a user uses the computer to connect to the database by using a web service, user can upload/download his information with help the cloud provider as shown in Figure 1.

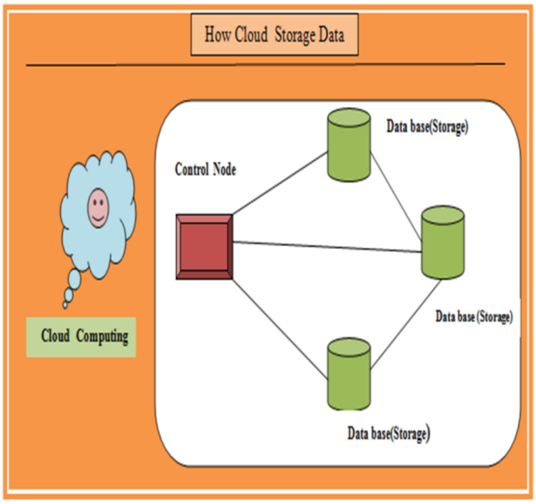

Figure 1: How cloud store the data.

Clients of cloud access cloud services through internet by use a web browser. Services do not need to buy any software to get the benefits of software. Examples of cloud computing: yahoo email, Gmail, Hotmail, etc. [8]. Cloud computing has several advantages [9]:

1. One can access application as utilities, over the Internet.
2. Manipulate and configure the application online at any time.
3. Reduce the cost and complexity of owning, computers and networks.
4. Make use of new innovations.
5. Flexible use.
6. Rapid deployment.
7. Scalability.
8. Reliability.

Cloud Computing Model is composed of three service models, and four deployment models:

DOI: http://dx.doi.org/10.23851/mjs.2017.27.4

1) **Service Models:** three types of services in cloud computing are shown in Figure 2.
   - **a. Software–as-a-Services (SaaS):** is a software that is owned, delivered, and managed remotely by one or more Providers [9].
   - **b. Platform-as-a-Service (PaaS):** an Operating System, Hardware, and Network are provided, and the customer install or develop its own software and/or applications [9].
   - **c. Infrastructure-as-a–Service (IaaS):** provides access to main resources (such as physical machines). IaaS provides the user the capability to processing, storage, networks, and other main computing resources [4].

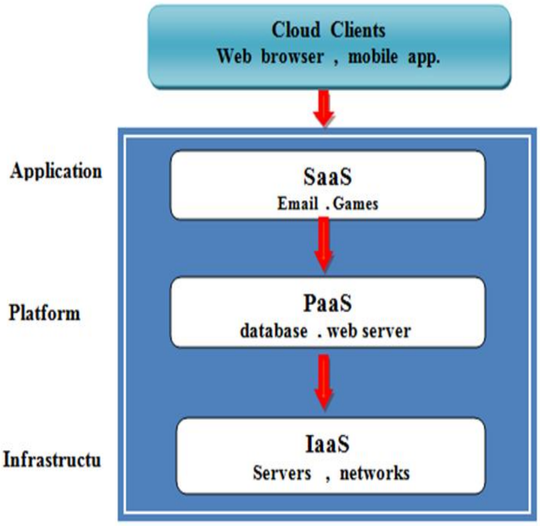

Figure 2: Cloud service delivery model.

2) **Deployment Models**: four main cloud deployment models are listed below [9]:
   - a. **Public Cloud**: allows systems and services to be easily accessible to the general public. Examples, e-mail services.
   - b. **Private Cloud**: allows systems and services to be accessible within an Organization. It has increased security because of its private nature.
   - c. **Community Cloud**: allows systems and services to be accessible by group of organizations.
   - d. **Hybrid Cloud**: model uses aspects of all other cloud models and this model used within large organization. The hybrid cloud is mixture of public and private cloud.

The main aim of security is to provide availability, confidentiality, and integrity to the data. Types of risk related with cloud computing such as [10]:

1) Information (data) can be attacked by an unauthorized (opponent) person.
2) Information (Data) can be changed by third party while transferring the data.

There are several types of attacks to cloud computing as listed below [4]:

1. Abuse of "cloud computing" (IaaS, PaaS).
2. Insecure interfaces and Application Programming Interface (API) (IaaS ,PaaS, SaaS).
3. Malicious insiders (IaaS, PaaS, SaaS).
4. Shared technology issues (IaaS).

The following new security and privacy challenges are the most important:

- ✓ Ensuring authorized access to user data.
- ✓ Both cloud provider and its customer should share responsibility for privacy and security [11].

There are several specific areas of the "cloud computing"[12] :

1. Security of data at rest.
2. Security of data in transit.
3. Authentication of user / applications /processes.
4. Robust separation between data to different customers.
5. Cloud legal and regulatory issues.

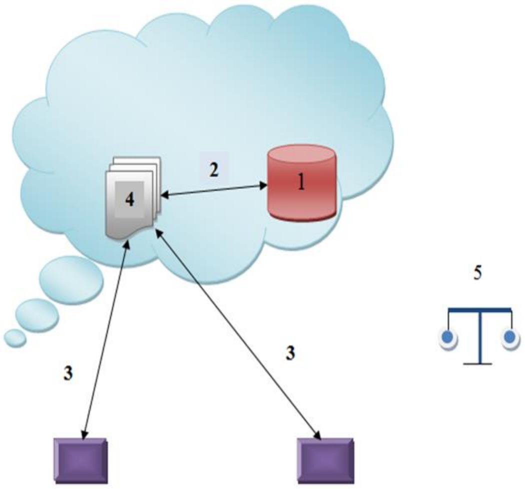

Figure 3: Areas of Cloud Computing.

Finally , there are several steps for access to cloud storage system; listed as follow:

1. User data request.
2. Apply request.
3. Data modified.
4. Data Replied.
5. Data storage.
6. Data response.

All steps above are shown in Figure 4.

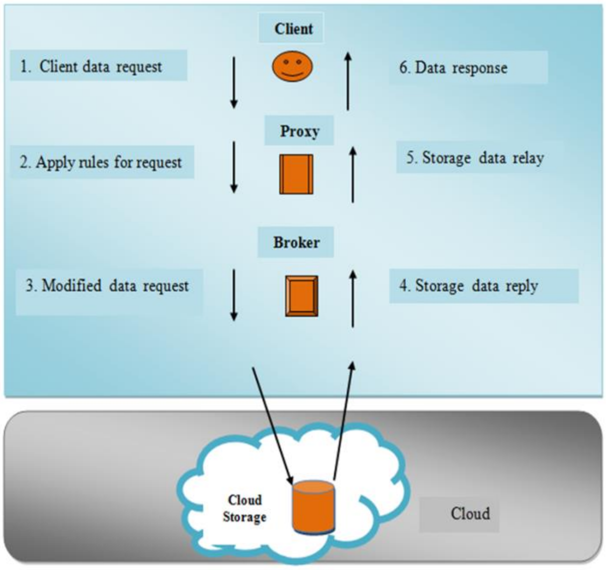

Figure 4: Steps for access to cloud storage system.

MATERIALS AND METHODS

Users frequently need to store, send or receive data in secure. Famous way to this is to transform the data into a various forms. Therefore, data can be understand only the one who can return it to its original form. This method is called as Encryption. Cryptography allow you to store secret data; therefore, it cannot be read by anyone except the intended receiver shown Figure 5.

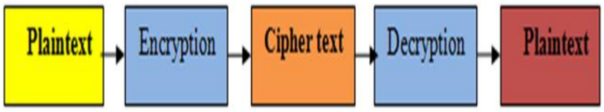

Figure 5: How does cryptography work.

Disadvantage of encryption is that the data is not hidden. If anyone have enough time, he/she could decrypt the data. A good solution to this is Steganography.
Steganography is the science that hide data into suitable cover to conceal the data and prevent the detect it (see Figure 6).

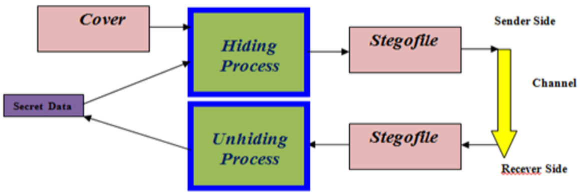

Figure 6: How does Steganography work.

All digital files formats can be used for steganography, but the formats that are more suitable which has high degree of redundancy [3].
The good covers for steganography must have two features; it should be popular and modification of the cover should not be visible to opponent [13]. Stenographic Techniques are classified according to the cover modifications into several techniques. The most common one of these techniques is the *Substitution Techniques*.
Substitution techniques are methods ranging from LSB coding. It encodes the secret data by replacing insignificant parts of the cover by the secret data bits.
In this paper we used Substitution Techniques. These methods range from LSB coding. LSB is One of the most popular methods is known as Least Significant Bit (LSB). The information is embedding into the least significant bits of the cover file. In LSB, the binary series of each byte of digital cover file is substituted with binary corresponding of secret message.

IMPLEMENTATION AND RESULTS

Proposed system is used is image steganography as image which are the most popular because of their frequency on the Internet. In this paper, we focus to increase security through transmission and store data in cloud storage data center. The system aims to secure data in rest and secure data over transferring, by hiding secret data within edges of color images, this way is called steganography.
To guarantee the security for cloud data from illegal users, we have designed efficient mechanism. This mechanism used random positions (pixels) in edges of color image to hide secret data bits. Color image is established of pixels, each pixel of color image is contain three bytes RGB: Red, Green, and Blue; each one has 8 bits. If we change the last bit. We putting our secret data into edges of color image and the stego-image is cutting in blocks and these blocks are separated into small pieces which has similar size. These small pieces are loaded in “cloud”. In this paper, the Robinson Mask with LSB method is used to hide secret information into edges of cover images and then sending these stego-images to storage area in the "cloud computing".
In this method, one byte of secret message is hidden in one pixel of edges of color image randomly:

STEP 1: Substitute 3-bits of the first byte of message instead 3-bit LSB of Red byte of edges of color image.

STEP 2: Substitute another 3-bits of the first byte of message instead 3-LSB of Green byte of edges of color image.

STEP 3: Substitute last 2-bits of the first byte of message instead 2-LSB of Blue byte of edges of color image as shown in Figure 7.

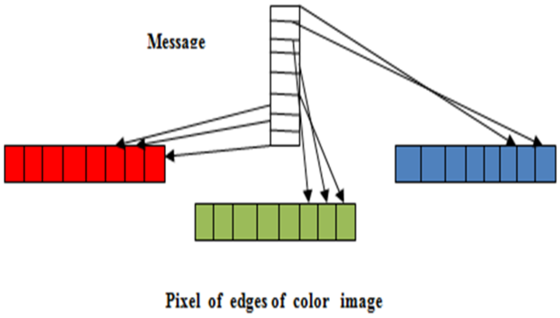

Figure 7: Hiding process.

The LSB algorithm inserts secret message data in cover image through handling the cover by using Robinson Compass filter to detect edges of the color image and selected these edges in array as pixels. Another array is used to select these pixels in randomly which used in Embedding Process will be described by the following steps and by Algorithm 1:

Step 1: Read the secret data.
Step 2: Determine the size of secret data file, and give the length of secret message as bytes.
Step 3: Load the cover image.
Step 4: Copy the first 54 bytes (header) of cover image and write it in a new stego file.
Step 5: Find the edges of image by using Robinson Compass filter specially to select edges of image.
Step 6: Compute the number of pixels of selected edges. And store the positions of these pixels in array(x,y). And
Step 7: Create new Random array corresponding the array of the positions of pixels.
Step 8: Select the position of edges according to the random array.
Step 9: While not end of secret message file: Read secret message file bytes sequentially. And convert to binary form.
Step 10: Hide first character(byte) of message into a pixel of edges of cover which selected by random array; Put first 3-bits of message byte instead 3-LSB of red color byte, and put next 3-bits of message byte instead 3-LSB of green color byte , and Put last 2-bits of message byte instead 2-LSB of blue color byte in sequentially.
Step 11: Repeat step 8 until while condition is satisfied.
Step 12: Take the complete cover file as stego-cover file.

Algorithm 1: Embedding Process.
Input: Cover file, secret message file.
Output: Stegocover file.

```
{
     While not end of secret message file
       {
         Read secret message file byte sequentially
         Convert to binary form
         {
             While not end of cover file
             {
                 Read edges of cover file as pixels
                 Put pixels in array.
                 Create random array of position.
                  Read an edges pixels as a bytes
                 sequentially.
             }
         }
         Put first 8 bits of secret data instead last of
         3-bytes of first pixel according to random
         array of position.
        } Repeat until while is satisfied.
         Take complete cover file as stego-cover file.
  }
```

Extracting Process will be described by the following steps and Algorithm 2:
Step 1: Read the stego file, Compute the length secret message.
Step 2: Find the edges of stego file by using the Robinson compass filter that is used in hiding process.
Step 3: Create array of random numbers that used in hiding process.
Step 4: According to the size of secret data , the length of Extracting process will be performed by reading the sequence bytes from stego file and extracting the secret data according to the random positions that are stored in array.
Step 5: Save the data of message in a new file.

Algorithm 2: Extracting Process.
Input: Stego file
Output: Secret message

```
Step 1:Read stego file.
Step 2:While not end of secret data file Do
Step 3:Cut the last bits from each byte of edges of
       stego data according to the random positions
       that are stored in array and the length of secret
       message
Step 4:Group these extracted bits in bytes
Step 5:Convert the secret data bytes into ASCII
       code. Then convert each ASCII code to
       characters
Step 6:Display the extracted string as a file
Step 7:End
```

CONCLUSION

The big problem of "cloud computing", is a security which is important of a spread storage system. Increasing the security of data in stealthy into cloud storage become very necessary. We proposed an efficient steganography method to improving security on data center and over transmission. This method is used edges of color images to hide the secret data. If the stego-images are stored in the cloud data Centre, our data have high secure from any attacks by opponents.

REFERENCES

[1] P. Mell , T. Grance; "NIST Definition of Cloud Computing", National Institute of Standards and Technology, vol. 15, no. 10.07, 2009.

[2] J.SRINIVAS, K.VENKATA SUBBA, Dr. A.MOIZ QYSER^3; “Cloud Computing Basic”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 5, pp. 343-347, 2012.

[3] Rajeev Kumar ; " Data Hiding Images Using spread spectrum in Cloud Computing"; International Journal

of Technical Research and Applications, vol. 1, Issue 3, PP. 76-79, 2013.

[4] Al-khanjari, Z. , Alani, A.; "Developing Secured Interoperable Cloud Computing Services"; European Scientific Journal, vol. 10, no.24, pp. 341-350, 2014.

[5] Marinal Kanti Sarkar, Trijit Chatterjee; “Enhancing data Storage Security in Cloud Computing through Steganography”; ACEEE Int. on Network Security, vol. 5, no.1, pp. 13, 2014.

[6] Sanjima Manocha, Sheveda Vashesht. “A Novel Hybrid Approach for Secure Cloud Mining using Lossless Image Format"; International Journal of Computer Applications, vol. 98, no. 7, pp. 7-11, 2014.

[7] Tutorialspoint, "Cloud Computing Tutorial", online Tutorial available on www.TutorialsPoint.com.

[8] Jijo .S. Nair , BaholaNath Roy, “Data Security in Cloud "; International Journal of Computational Engineering Research (IJCER).

[9] "Introduction to Cloud Computing", Office of the Privacy Commissioner of Canada. www.priv.gc.ca.

[10] Garima Saini, Naveen Sharma, “Triple Security of data in cloud computing”; International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5, 2014.

[11] Tariq Ahmed, Abdulla Aljumah; "Cloud Computing and Steganography-attack Threat Relation"; MAGNT Research Report, vol.2, no.4, pp.72-75, 2014.

[12] Jaydip Sen; "Security and Privacy Issues in Cloud Computing "; Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India, pp. 1-45, 2013.

[13] Wojciech Mazurczyk, Krzysztof Szczypiorski; " Is Cloud Computing Steganography-Proof?"; Institute of Telecommunications, Warsaw University of Technology Warsaw, Poland, pp. 441-442, 2011.