ISSN 2277-3061

Enhancing Cloud Computing Security by Using Pixel Key Pattern

Randeep Kaur [1], Jagroop Kaur [2]
[1] Research Scholar, Department of Computer Engineering, Punjabi University, Patiala
ryna.sidhu@gmail.com
[2] Assistant Professor, Department of Computer Engineering, Punjabi University, Patiala
jagroop_80@rediffmail.com

ABSTRACT

Cloud is a term used as a metaphor for the wide area networks (like internet) or any such large networked environment. It came partly from the cloud-like symbol used to represent the complexities of the networks in the schematic diagrams. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices. Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. We will be implementing cloud security aspects for data mining by implementing cloud system. After implementing cloud infrastructure for data mining for cloud system we shall be evaluating security measure for data mining in cloud. We will be fixing threats in data mining to Personal/private data in cloud systems.

Keywords

Cloud Computing, Cloud Security, Confidentiality, Security Issues, Zones, Grouping.

Council for Innovative Research
Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol.14, No.7

www.ijctonline.com, editorijctonline@gmail.com

INTRODUCTION

Cloud computing is here. With its new way to deliver services while reducing ownership, improving responsiveness and agility, and especially by allowing the decision makers to focus their attention on the business rather than their IT infrastructure, there is no organisation that has not though about moving to the Cloud.

Several surveys from Gartner have shown the importance of cloud computing ranking it as the top priority for CIOs in 2010 [GAR11][1], also demonstrating the effort they are doing to adopt it by increasing their expenditures on cloud computing services [GAR10a]. There are several benefits, especially on infrastructure costs, but, as with all new technologies, cloud computing also has some drawbacks.

The move to the Cloud is a crucial step for any company, but has to be made with a lot of caution because it could turn against users. Organisations need to clearly understand the benefits and challenges, especially for the most critical applications. There are several concerns but, as shown in an IDC survey about the issues of the Cloud [GEN09], security is the main concern. The question is why security is such a complicated challenge in the decision of moving to the Cloud. The answer is easy: lack of control over their data.

When an organisation decides to move to the Cloud the data is no longer on their hands. Even if they just use the Cloud for processing and not storage, they are taking the data outside their private perimeter. IT infrastructures have been de-perimeterized, so security needs to be approached from another perspective; but this blurring of the perimeter is not the only issue.

RESEARCH MOTIVATION

Security [2] is the key for the Cloud success. As many surveys show [GEN09, IDC11], security in the cloud is now the main challenge of cloud computing. Until a few years ago all the business processes of organisations were on their private infrastructure and, though it was possible to outsource services, it was usually non-critical data/applications on private infrastructures.

Now with cloud computing, the story has changed. The traditional network perimeter is broken, and organisations feel they have lost control over their data [REE09]. New attack vectors have appeared, and the benefit of being accessible from anywhere becomes a big threat.

Many of the cloud computing issues are similar to the old ones but in a new setting [CHO09]. This requires re-assessing the risks related to each of the critical areas considering the new hazardous environment. The Cloud Security Alliance (CSA) defines 12 areas of concern for cloud computing [CSA09a] divided into two broad categories: governance and operations. All of these areas are critical and should be taking in consideration when evaluating the security of a cloud environment.

Amongst resilience and agility[4], the low costs that provide cloud computing is a real hook for companies trying to reduce costs. Start-ups looking for a place in the market pray for an economic solution that allows them to focus on their business without worrying on maintain an IT infrastructure.

With multi-tenancy resources are shared by multiple users. For example, two or more tenants could have their OSs running on the same server or two or running an instance of the same application with different data. Depending on the cloud deployment model the level of importance and sharing of multi-tenancy would be different [CSA09]; but without any doubt Infrastructure-as-a-Service (IaaS) in public clouds creates the most risks off all.

RELATED WORK

Prof: Asha Mathew (2012) discusses the security and privacy concerns of cloud computing and some possible solutions to enhance the security. Based on the security solutions suggested i have come up with a secured framework for cloud computing.

Te-Shun Chou (2013): In this work, three cloud service models were compared; cloud security risks and threats were investigated based on the nature of the cloud service models. Real world cloud attacks were included to demonstrate the techniques that hackers used against cloud computing systems. In addition, countermeasures to cloud security breaches are presented.

Keiko Hashizume, David G Rosad(2013): identifies the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.

Pankaj Sareen(2013): This study describes cloud computing, a computing platform for the next generation of the Internet. The paper defines clouds, types of cloud Provides, Comparison of Cloud Computing with Grid Computing, applications and concerns of Cloud Computing , Concept of Virtualization in Cloud Computing. Readers will also discover the working, Architecture and Role of I.T Governance in Cloud Computing.

Vijay.G.R , Dr.A.Rama Mohan Reddy(2013): This work mainly provides the basic idea on Cloud Computing with the Security Issue mainly faced in both larger and smaller scale organizations where Cloud Computing is implemented and necessary steps which can solve these problems to certain extent.

Mrinal Kanti Sarkar, Trijit Chatterjee(2014): The main objective of this study is to prevent data access from cloud data storage centers by unauthorized users. This scheme perfectly stores data at cloud data storage centers and retrieves data from it when it is needed. So, there are various issues that need to be addressed with respect to the management of data, service of data, privacy of data, security of data etc. But the privacy and security of data is highly challenging.

Sanjima Manocha, Sheveta Vashisht(2014): This research work explores the basic features of data mining techniques in cloud computing and securing the data using edge detection method. This research work tries to integrate data mining techniques into cloud computing and image processing making it a hybrid approach.

Khushboo Gupta, Neha Goyal, Puneet Rani(2014): Among the various technologies of web Cloud Computing is one of the recent internet based computing technology. It provide us a virtual server and a huge size of database to store our data over the internet. Since it is easy to store and manage the data many organizations moving their confidential data into the cloud. But as it is an internet based technology we are concerning about the security related issues like hacking, stealing, misusing etc.

Monjur Ahmed and Mohammad Ashraf Hossain(2014): This research presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest.

Sneha Arora, Sanyam Anand: In this paper, we proposed a technique to hide the text data into the color images using edge detection method. The alteration in edges cannot be distinguished well so edges can hide more data

PROBLEM STATEMENT

In the base paper, the author has tried to distribute the data into the multiple files before sending it to the cloud provider. The author has used the 3-step mechanism in which the client is sending his/her file to the gateway. Gateway is used to split the file into multiple parts. Afterwards, gateway is used to transfer the multiple files onto the cloud provider. The problem in the above said work is that when the client will send the original file to the gateway, then there is a possibility of file getting stolen by the third party (Man in the middle attack) without the permission of client, as shown in figure 1.

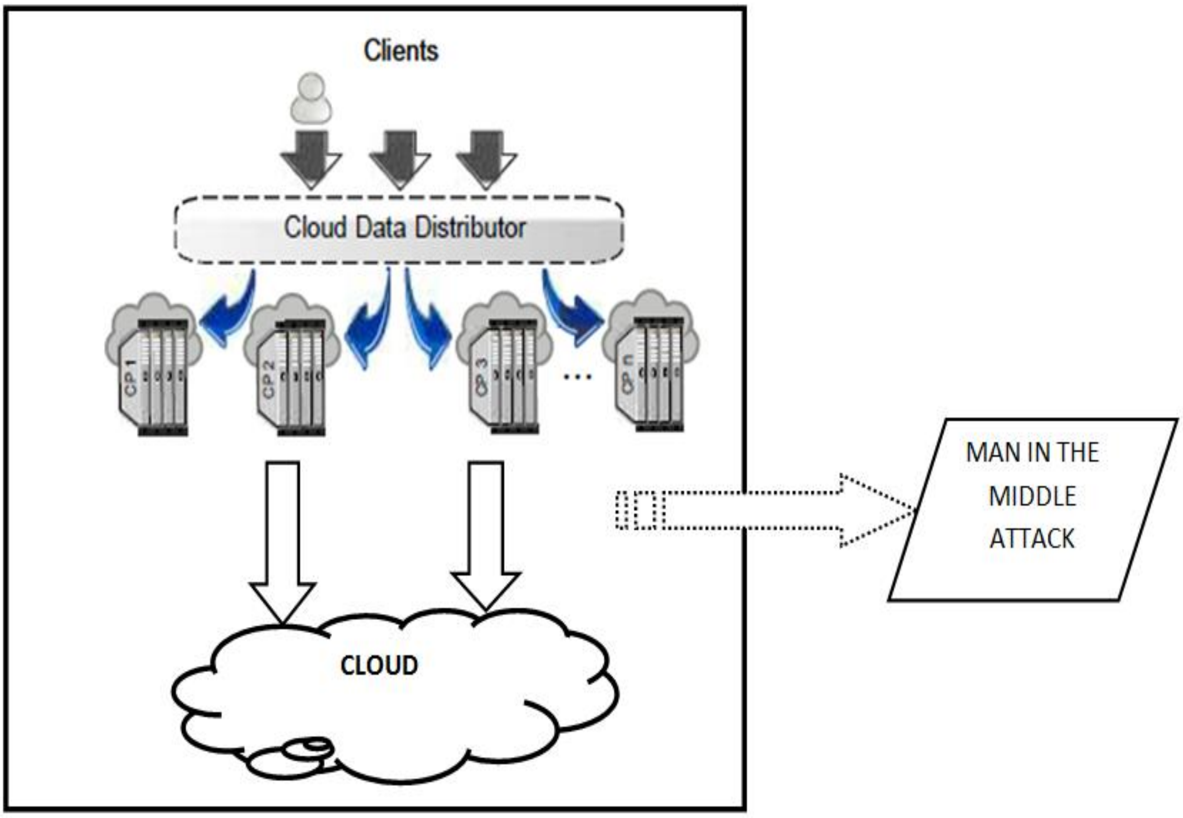


Figure 1 Man-In-the-Middle attack

Moreover, when the files are being stored at the cloud provider, there is a possibility of data mining attack on the files which will result in the useful information leaked from the cloud end.

RESEARCH OBJECTIVES

Our main objective is to enhance the security between the client and the cloud provider by using pixel key pattern for the steganography and by using the cloud data distributor to split the single file into multiple fragments.

- The security has a primary role in the services of Cloud computing because the data being transferred between the client and cloud provider is of utmost importance and thereby neither the client nor the cloud provider will sacrifice on the security of the cloud.
- The data is enclosed in the image by the client itself before sending it to the cloud. The cloud provider will never come to know about the original data of the client.
- Moreover, the image sent by the client is divided into multiple parts by the Cloud data distributor.
- These fragments (multiple parts) are being stored over the cloud.

These objectives are stated to ensure the privacy of the client's data when it is being transferred, processed or stored at the cloud provider.

METHODOLOGY

This thesis aims to provide an understanding of the different attack vectors created by multi-tenancy and virtualization in a public IaaS cloud. The vectors will be explored, focusing on the threats arisen from different tenants coexisting in the same physical host. A critical analysis of the different vectors will be provided along with guidance on how to approach them. This analysis will be performed using previous works from different entities and authors, along with personal knowledge obtained from experience. As part of the aim of this research, a strong foundation will be provided on the terms of cloud computing, multi-tenancy and virtualization. All these areas will be explored giving a strong definition.

The different security issues will be also explored in order to provide an introduction to the main focus of the research.

• Client will enter the data that has to be sent to the Cloud Provider.

• Client will automatically choose the image in which the data will be encrypted using pixel key pattern technique of Steganography. The data is encoded inside the image so that it is saved from outside interference and misuse. (Hidden from outside world)

• This encrypted/encoded image is then transferred to the gateway.

• Gateway will receive the file sent by the client and will split it into multiple files.

• Gateway will store the name of the files in the distribution table.

• Afterwards Gateway will transfer all the splitted files to the cloud provider for storage.

So, Using this approach, we have achieved two purposes.

- If anyone tries to hack the data while transferring from client to the gateway, he/she will get only encoded image.
- If anyone tries to perform the mining on the files stored at the cloud provider, no results will be retrieved

During Downloading the file from cloud end, the client will follow the following steps:

1. Client will ask the gateway to download his/her stored file.

2. Gateway will forward the request to the cloud provider and cloud provider will send all the stored splitted files of that client to the gateway.

3. Gateway will receive all the files and will try to combine them into a single file.

4. After linking of all the files, gateway will send the single linked file to the client.

5. Client will further perform the steganographic decryption to fetch the stored data inside the image.

ALGORITHM

1. client registers and logins with the cloud provider.

2. for all the images in the dataset, choose the random image say k.

3. the data (m) is stored in the variable named d.

4. compute the length of the m ; lets say 10.

5. find all the contours in the image using pixel key pattern,

6. if the contour's thickness > threshold_value

7. compute the matrix of that pixel

```
8.    else
9.    find the next contour
10.   convert the available matrix  as well as the data  into the bytes format.
11.   replace the redundant bits of the matrix with the bits of the data.
12.   create the new image with the help of available matrics.
13.   client sends the image to the available gateway.
14.   find the size of the file (say 1000kb)
15.   split the file using threshold value ( 100 bytes)
16.   for i=1 to 1000
17.   j =0;
18.   if( j < 100)
19.   read the data from the original file
20.   write into the new file
21.   j++;
22.   else
23.   create a  new file
24.   j = 0;
25.   end if
26.   end for
27.   send these fragmented files to the cloud provider for storage.
```

DECRYPTION ALGORITHM

```
1.    client logins with the cloud provider.
2.    Client sends the name of the file to be downloaded to the gateway
3.    Gateway forwards the request to the cloud provider.
4.    for all the fragments of the requested file.
5.    Cloud transfers the fragments to the gateway.
6.    join the file using threshold value ( 100 bytes)
7.    for i=1 to 100
8.    j =0;
9.    if( j < 100)
10.   read the data from the next part
11.   write data into the new file
12.   j++;
13.   else
14.   read from the next part
15.   j = 0;
16.   end if
17.   end for
18.   send the single linked file to the client.
19.   find all the contours in the image using pixel key pattern,
20.   if the contour's thickness  > threshold_value
21.   compute the matrix of that pixel
```

22. else
23. find the next contour
24. convert the available matrix into the bytes format.
25. find the data bits inside the matrix and store them in data array.
26. create the new image with the help of available matrics.
27. Convert the data array to the string format.

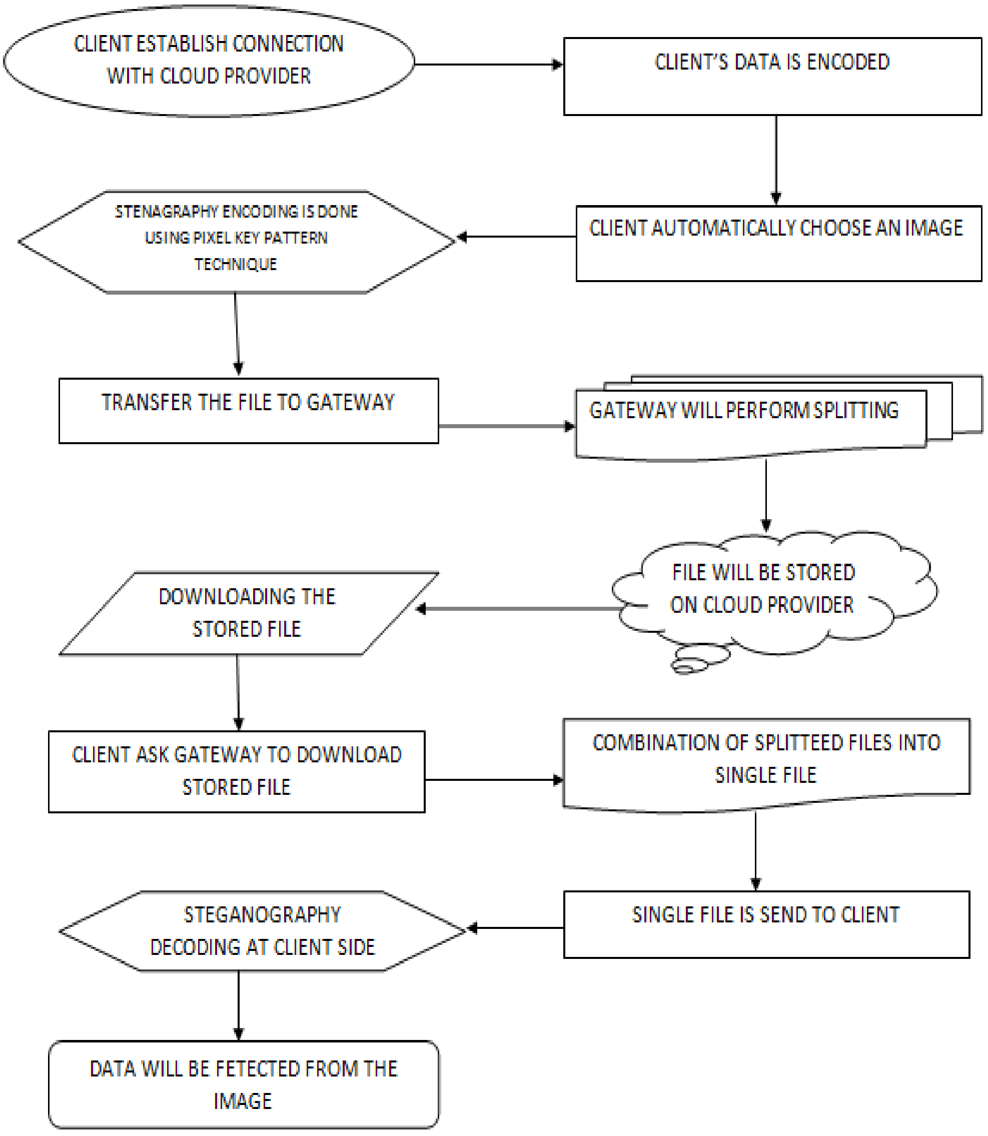

CLIENT ESTABLISH CONNECTION WITH CLOUD PROVIDER
CLIENT'S DATA IS ENCODED
CLIENT AUTOMATICALLY CHOOSE AN IMAGE
STENAGRAPHY ENCODING IS DONE USING PIXEL KEY PATTERN TECHNIQUE
TRANSFER THE FILE TO GATEWAY
GATEWAY WILL PERFORM SPLITTING
FILE WILL BE STORED ON CLOUD PROVIDER
DOWNLOADING THE STORED FILE
CLIENT ASK GATEWAY TO DOWNLOAD STORED FILE
COMBINATION OF SPLITTEED FILES INTO SINGLE FILE
SINGLE FILE IS SEND TO CLIENT
STEGANOGRAPHY DECODING AT CLIENT SIDE
DATA WILL BE FETECTED FROM THE IMAGE

Figure 2. Flowchart of Proposed Methodology

EXPERIMENTAL SET UP

This section gives the details of the experiments that we have conducted during the research period. Many images like nature wallpaper ,technology ,symbols ,kids wallpaper of different size are taken 4kb ,10kb ,25.6kb,40kb,105kb ,245kb, 560kb, 786kb,1.3mb like this 40 images are tested and data which is encrypted taken are of length; 5 words,100 words,4000 words,11000 words .

This experiments work on a machine with the following configuration:

IntelCore 2 CPU, 980 MHz, 1.99 GB RAM, Microsoft windows 7. We have the Java version 8 with the Netbeans IDE version 8.The working system calculate the processing time,cost ,number of files splitting, block size and image decryption time to enhance between the client and the cloud provider.

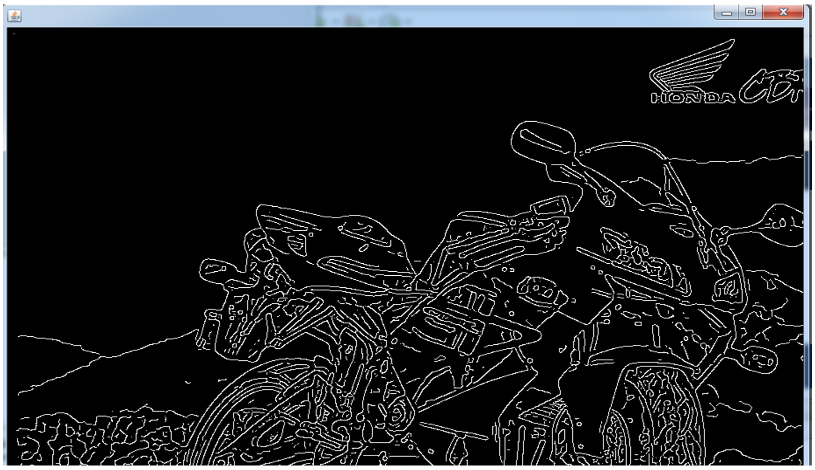
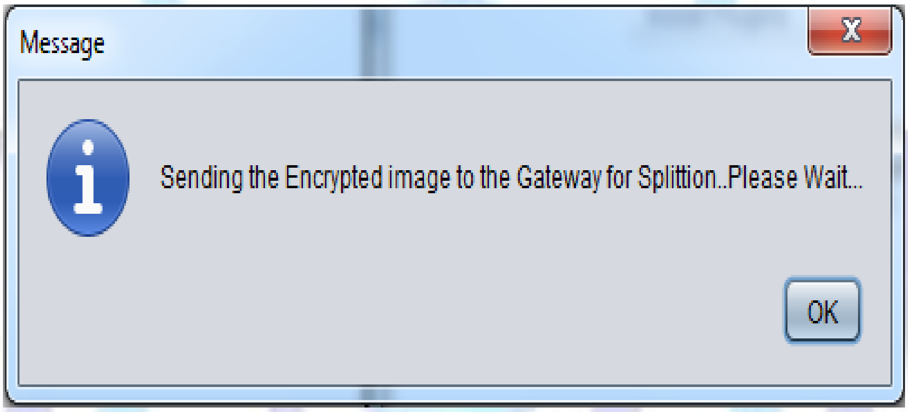
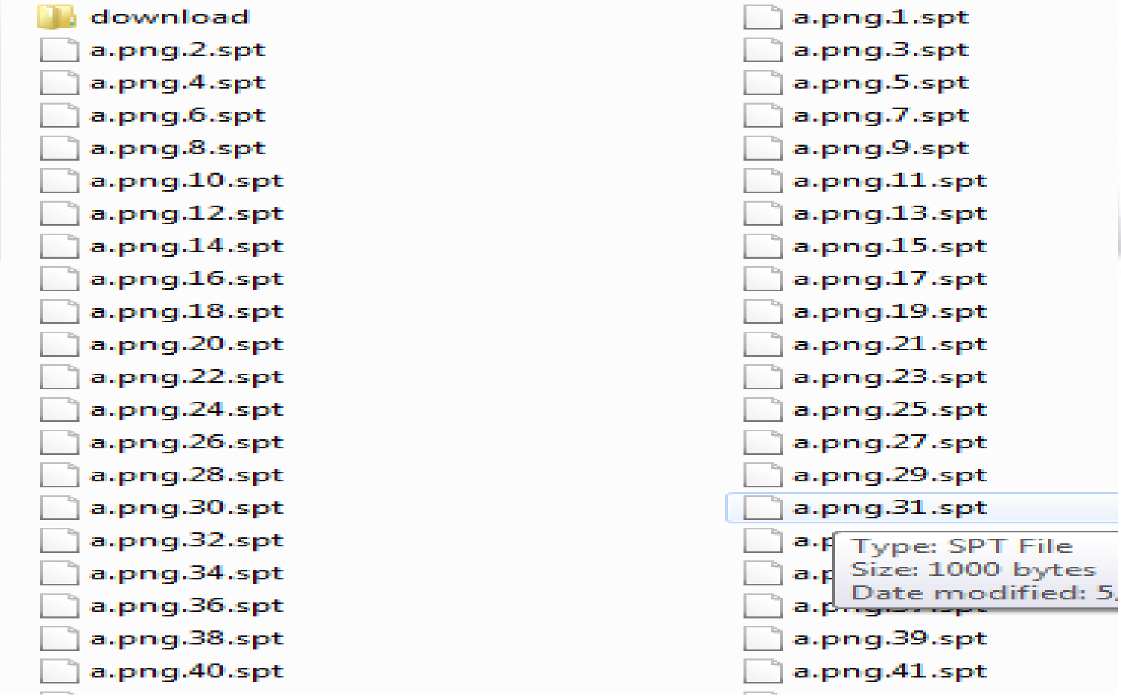


Figure 3. Using pixel key pattern find the contoures of the image



Sending the Encrypted image to the Gateway for Splittion..Please Wait...

Figure 4. Cloud data distributer will split the file into multiple files.



download
a.png.1.spt
a.png.2.spt
a.png.3.spt
a.png.4.spt
a.png.5.spt
a.png.6.spt
a.png.7.spt
a.png.8.spt
a.png.9.spt
a.png.10.spt
a.png.11.spt
a.png.12.spt
a.png.13.spt
a.png.14.spt
a.png.15.spt
a.png.16.spt
a.png.17.spt
a.png.18.spt
a.png.19.spt
a.png.20.spt
a.png.21.spt
a.png.22.spt
a.png.23.spt
a.png.24.spt
a.png.25.spt
a.png.26.spt
a.png.27.spt
a.png.28.spt
a.png.29.spt
a.png.30.spt
a.png.31.spt
a.png.32.spt
a.p
a.png.34.spt
a.p
a.png.36.spt
a.p
a.png.38.spt
a.png.39.spt
a.png.40.spt
a.png.41.spt

Type: SPT File
Size: 1000 bytes
Date modified: 5.

Figure 5. Gateway will store the name of the files in the distribution table.

S.NO	Size of image	Message length	Start time	Finish time	Processing time	Encryption time	No. of files splitted	Cost	Decryption time
1	4.96kb	1122	0.1	1.96	1.86	30105	64	18.56	7
2	5.79kb	5	0.1	1.9	1.8	9421	51	18.4	9
3	8.11kb	24	0.1	1.98	1.88	11899	71	18.84	11
4	8.16kb	15	0.1	1.91	1.81	8778	52	18.08	12
5	11.7kb	100	0.1	2.1	2.0	11920	89	19.1	12

Figure 6. Readings of the Proposed work when splition of the encrypted image is done.

Evaluation of the System

After implementing the proposed methodology, we have reached up to a solution that the cloud security can be enhanced by applying the steganography as well as data distribution on the client's data. The data sent/received by the client is of utmost importance and it needs to be handled carefully. We have been able to reduce the processing time, encryption time, processing cost which increases the overall efficiency of the system.

Accuracy of the System

Accuracy of the System can is enhance by measuring Processing time ,Cost and Data distribution as shown in the graphs below, which increases the overall efficiency of the system.

- **Processing Time**

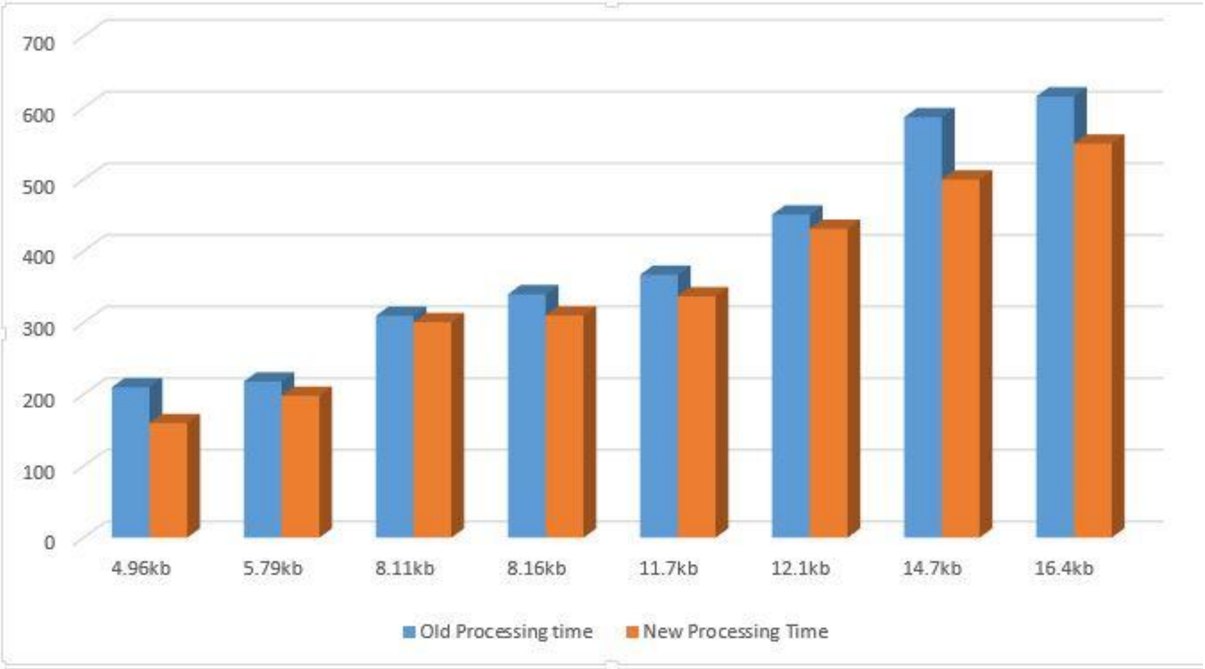


Figure 7. Processing time

From the above bar chart, it is clear that the processing time has been reduced. The processing time depending upon the size of the file. As the size of the file increases, the processing time will also increase. But we have been able to reduce the processing time of the proposed work as it will finally increase the overall efficiency of the system.

- **Cost**

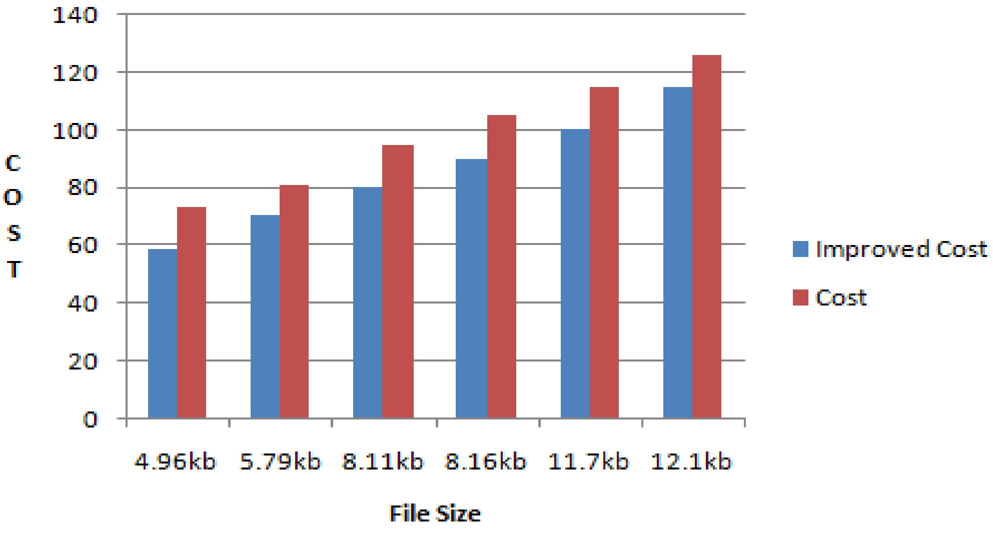


Figure 8 File Size v/s Cost

From the above bar chart, it is clear that the cost has been reduced. Usually Cloud Computing providers have detailed costing models which are used to bill users on *pay per use basis* The Cost depends upon the size of the file. As the size of the file increases, the Cost will also increase. But we have been able to reduce the Cost of the proposed work as it will finally increase the overall efficiency of the system.

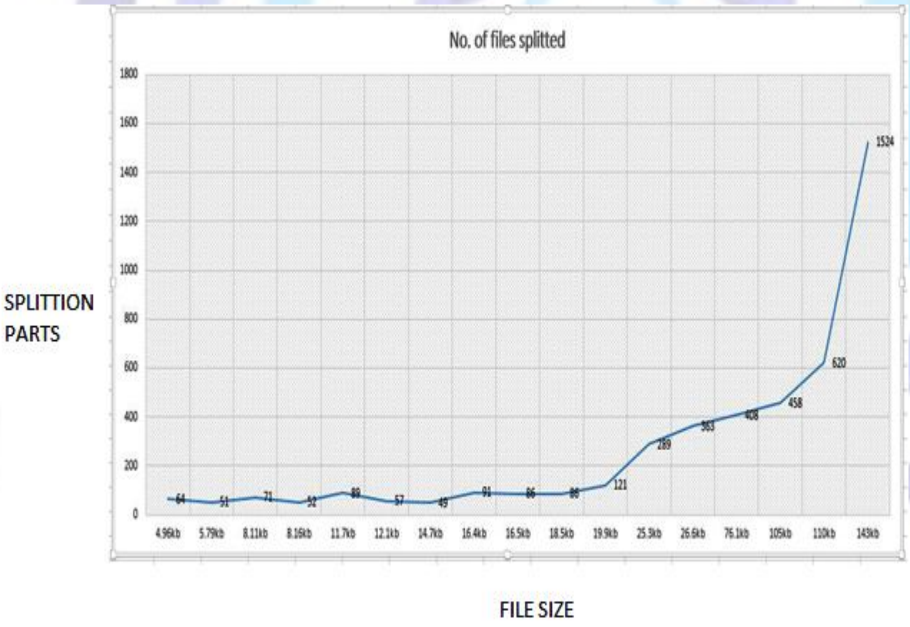


Figure 9 File Size v/s Parts

From the above bar chart, it is clear that as the file size increases number of partitions of the file also goes on increasing which helps to secure data at the cloud end. As data is not present in one file so it cant be hacked by the third party easily which hence ensuring the data security.

CONCLUSION

The primary conclusion of our research is that adoption of user-centric security models and shifting certain parts of communication and computation to the client side allows us to provide the cloud consumers with more visibility and control over their resources. Therefore, using this approach not only the security and privacy concerns of cloud consumers can be addressed more effectively, but also the burden of managing end-users' identities and access control will be reduced from cloud service providers.

This study collectively describes cloud computing security challenges in general and describes the mitigation practices that have been proposed to handle the identified challenges. We have successfully implemented the above proposed system and has reached to a solution that by splitting the files into multiple fragments we can achieve the better security in cloud computing. However, most important future work identifies here is that there are concrete standards for cloud computing security still missing. There are some open cloud manifesto standards and few efforts made by the cloud security alliance to standardize the process in the cloud. The cloud vendors and users do not encourage the usage of these standards as they are restrictive. In addition to this the cloud computing with such great offering such as storage, infrastructure and application designing capabilities on the go to the IT industry still fail to have proper standards for interoperability with other cloud service providers. This failure to provide concrete security standards, common underlying framework for data migration and global standards for cloud interoperability, make the leading technology the cloud computing" still a vulnerable option for aspiring users.

REFERENCES

[1] T. Lindeberg, Addressing cloud computing security issues , International Journal of Computer Vision, pages 117—154,1998.

[2] Buyya R, Murshed M. A review on cloud computing security issues & challenges.,Concurrency and Computation Practice and Experience 2002.

[3] L. Wang, Gregor Laszewski, Marcel Kunze, Jie Tao, “Cloud Computing: A Perspective Study”, New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008.

[4] R. Maggiani, Communication Consultant, Solari Communication, “Cloud Computing is Changing How we Communicate”, 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009.

[5] Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, Cloud Computing Types ,Architecture ,Application and Role in IT, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009.

[6] Kapil Bakshi ,Thunder in the Cloud: $6 Cloud-Based Denial-of-Service Attack, August 2009, Vol. 169, pp. 36-45, 2009.

[7]Torray Harries , Taking account of privacy when designing cloud computing services, CLOUD '09 Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52, IEEE Computer Society Washington, DC, USA, May 2009.

[8] Randy Marchany, A survey of trust in computer science and the semantic web,Journal of Web Semantics: Science, Services and Agents on the World Wide Web ,2010.

[9] Yanpei Chen, Vern Paxson,Electrical Engineering and Computer Sciences University of California at Berkeleyhttp://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html January 20, 2010.

[10] Wojciech Mazurch, Image Steganography by Variable Embedding and Multiple Edge Detection using Canny Operator , Future Generation Computer Systems ,2010.

[11] Dimitrious zissis , Dynamic trust enhanced security model for trusted platform based International Telecommunication Union, X-509 | ISO/IEC 9594-8, 2010.

[12] Paul Stryer, Establishing and managing trust within the public key infrastructure, Computer Communications ,2010.

[13] S.Sukashinin,V.Kavitha ,Security Issues in Cloud Computing and Countermeasures,International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

[14] Alexa Huth,James Cebula, Security Attacks and Solutions in Clouds,2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2011.

[15] Lee Butlen and Richard, Understanding Data centers and Cloud Computing ,44th Hawaii International Conference on System Sciences, pp. 1–10, Koloa, Hawaii, January 2011.

[16] Peter Mell, Timothy Grance,The NIST Definition of Cloud Computing, http://docs.ismgcorp.com/files/external/Draft-SP-800- 145_cloud-definition.pdf, 2011.

[17] Thomas W. Shinder, “Security Issues in Cloud Deployment models”, TechNet Articles, Wiki,http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud deployment-models.aspx,September 2011.