Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.786 – 791

RESEARCH ARTICLE

Data Security in Cloud Computing using Encryption and Steganography

Karun Handa, Uma Singh

PG Student, Department of Computer Science & Engineering, Delhi Institute of Technology and Management, Gannaur, India

Asst Professor, Department of Computer Science & Engineering, Delhi Institute of Technology and Management, Gannaur, India

Email: k7handa@yahoo.in

Abstract-- Cloud Computing is a technology that readily makes available resources that otherwise may require huge amount of investment. Besides, it increases the availability of resources since anyone can access the data using web. But this advantage comes at a cost. Firstly, the data is uploaded unsecurely which has a high risk of being hacked by some malicious people. Secondly, the data saved at remote servers is under the surveillance of unknown people who can do anything with our data. So, these data security risks are causing a hindrance in the development of the field of cloud computing. Thus, this paper has designed a scheme that can help, solve this issue.

Keywords-- Data Security, Cloud Computing, Encryption, Steganography, Data-centres

I. INTRODUCTION

Cloud computing is a new development in the field of computer science and networking. It has open the gates of opportunity to fulfill the aspirations of small and medium scale enterprises that do not want to waste money in buying hardware resources. It provides an equal opportunity for all to excel.

Cloud computing is based on the principle of virtualization, which means that there is a single large machine and multiple clients are sharing this machine with a view that they have their own dedicated resources. It basically has three level of services. First, Infrastructure as a service (IaaS), in this technique the hardware resources such as hard-disk, memory, networking resources etc are provided on rent and are charged as per the usage. Second, Platform as a service (PaaS), which not only provides all the facilities as in IaaS but also provides operating system facilities, their updates, etc hence make the overall work quite easy. Third,

© 2015, IJCSMC All Rights Reserved

Software as a service (SaaS) which is the most flexible and easiest to use. It has all the features of IaaS and PaaS and moreover provides the freedom to choose software applications from a bundle of already available resources.

Although, cloud computing is very useful in today's life but it has its own set of cons. Firstly, a general misconception is that the data is not secure. The reason for this is that the people can't trust that the service providers will not take advantage of the client data which is kept far away from them in any unknown server. Second, the concern of data security while it is being uploaded to the server has reached an alarming stage. Now-a-days, tools and video resources are available that can teach how to hack data packets, etc. Thus in this paper the scheme being used deals with these issues and provide a simple yet powerful method of securing data.

II. RELATED WORK

A. Enhancing Data Storage Security in Cloud Computing Through Steganography by Mrinal Kanti Sarkar and Trijit Chatterjee

Here the authors provide a very solid technique of maintaining the integrity of data. In this model, the data being sent to server is saved behind the images. Thus , the unauthorized access cannot perceive the data as it is hidden. The proposed model makes use of steganography using images for protecting the integrity of data which is a very good approach however , the security of data during transmission is not handled at all. Hence , even though its a very unique approach but could have been much better if integrity and confidentiality of data can be handled while uploading to cloud server.

B. Cloud Computing Security: From Single to Multi Clouds by Eric Pardede and Ben Soh

This paper deals with the data security issues related to multi cloud environment. Moreover, it promotes the use of multi-clouds for higher level of availability.

C. Enhancing security in cloud computing structure by hybrid encryption by Aparjita Sidhu and Rajiv Mahajan

This paper states a scheme where the plain text is first converted to whitened text, containing text in hexadecimal format using MD5, which is again converted to encrypted form using AES algorithm. Thus it uses two encryption algos one for plain text and another for already encrypted text. The scheme is very simple in its approach and can be easily implemented but from security point of view its feasibility is questionable as extensive use of encryption algorithms is done but no care has been taken to secure the keys used for encrypting the data.

D. Robust Data Security for Cloud while using Third Party Auditor by Ravi Kant Sahu and Abhishek Mohta

This paper uses the services of a third party auditor for checking cloud server provider reliability. Also it verifies that the data is intact and is responsible for its accountability. In short it deals with the problem of data privacy and its integrity.

E. A proficient model for high end security in cloud computing by R. Bala Chandar, M. S. Kavitha and K. Seenivasan

This paper presents a protocol that uses the services of a third party auditor not only to verify the integrity of data stored at remote servers but also in retrieving the data in intact form. The main advantage of this scheme is the use of digital signature to assure the integrity of data locally. However, the overall process is quite complex as the keys and data are also encrypted and decrypted respectively.

F. Cloud computing security using encryption technique by Sanjoli Singla and Jasmeet Singh

In this paper the authors deal with the issue of data security during transmission of data. The main concern here is to encrypt the data so that confidentiality and privacy can be achieved. The algorithm used here is Rijndael Encryption Algorithm along with EAP-CHAP.

G. Secure Data Storage and Retrieval in the Cloud by Vaibhav Khadilkar, Anuj Gupta and Bhavani Thuraisingham

In this paper, the authors have given importance to sharing of data to make it more useful. But to perform this action the issues are common storage space and secure access to shared data. The authors have given a comprehensive description of a technique using Hive and Hadoop with XACML policy to make this scheme work in a convenient way.

© 2015, IJCSMC All Rights Reserved

H. Cloud Computing Security and encryption by Varsha Alangar

In this paper the author has tried to attract analyst attention towards the problem of data security and as firmly believe that data encryption can help to solve this issue. The author has provided a list of various encryption techniques such as RSA , DES , etc.

I. Using Third Party Auditor for Cloud Data Security: A Review by Ashish Bhagat and Ravi Kant Sahu

In this paper the authors have tried to show that there may be a situation where the service providers are not very cooperative with the users and hence make this useful service very hard to accept. Also, the authors have provided a brief description of how this approach can be modified with the help of third party editor i.e an external entity takes care of integrity of data along with the user himself, which provides a better security.

J. Fingerprinting Based Recursive Information Hiding Strategy in Cloud Computing Environment by Varsha Yadav, Preeti Aggarwal

In this paper , the scheme describes the use of client fingerprints to encrypt user's data and again to decrypt while retreiving it.The algorithm is a very unique approach as no two persons can have the same fingerprints. Secondly , if this scheme is applied then its not always possible that the person using the cloud services will have fingerprint machine and if not then extra money is required to purchase respective machines and to make this model work.

III. PROPOSED WORK

This model to be presented is based on the principle of securing data both during transmission and while data-at rest at servers.

The cloud architecture being used is as shown below:-

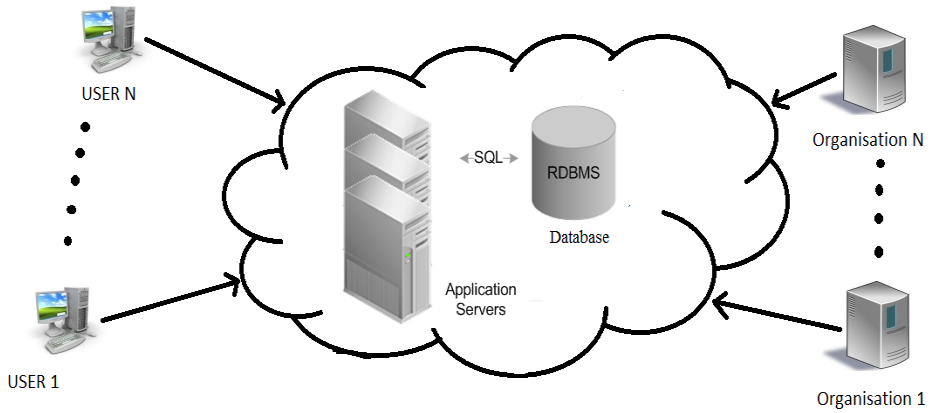

Figure 1 Cloud Architecture

The working of this model is as follows:-

A. Storing Process

Its working is described as follows:-

1) The user selects the data to be uploaded and this selected data gets encrypted using a strong algorithm such as AES algo.
2) The encrypted data is then uploaded to server.
3) On receiving data, one which came from user side a hiding algorithm is applied which randomly selects the bits positions from images where data is to be stored. The bit position is either 0^{th} , 1^{st} or 2^{nd} position.
4) This hiding algorithm is used to save the files or data behind the images. This process is called steganography using images.

© 2015, IJCSMC All Rights Reserved

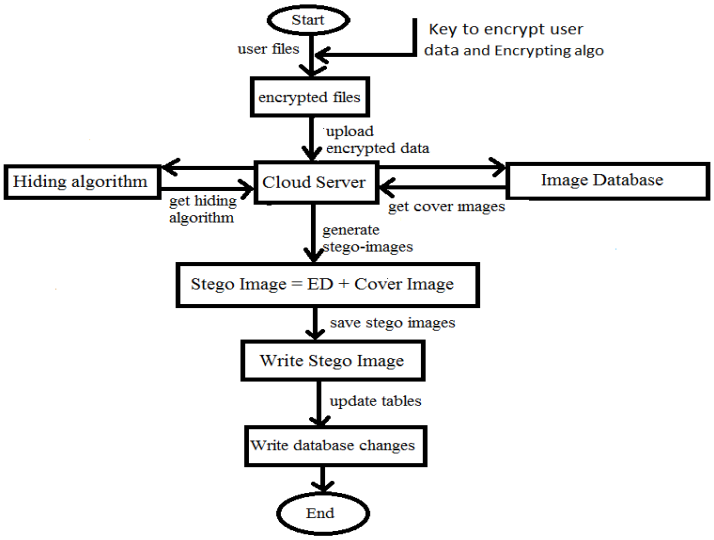

Figure 2 Storing Process

B. Retrieval Process

Its working is as follows:-

1) When user demands data back a retrieval algorithm extracts images and separates user data from them.
2) This extracted data is then sent to client.
3) On client side, the encrypted data is decrypted and the original data is retrieved.

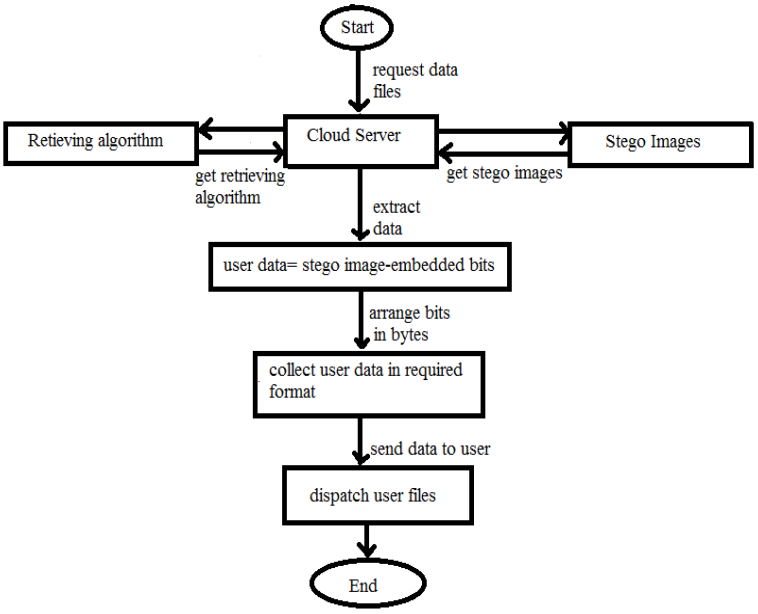

Figure 3 Retrieval Process

© 2015, IJCSMC All Rights Reserved

The above model addresses security of data at two levels, one when data is moved to remote servers and another while it is being saved and is guarded by the cloud service provider officials.

C. Results

In the above model, two basic processes of encryption and steganography have been performed. Now for the success of this model it is necessary that images produced after steganography must be well constructed so that it is not possible to differentiate between original and stego images and hence not possible to detect the presence of data.

The images used for the testing purpose are of 1920 x 1080 pixels. The bits per pixel is 24bpp.

Some of the samples are as follows:

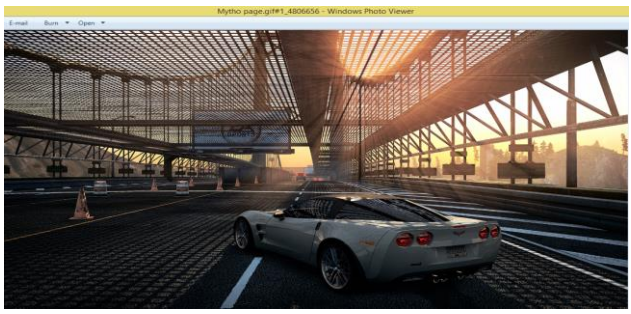

Figure 4 Image with encrypted Data

Figure 5 Original Image

IV. CONCLUSION

It is indeed that cloud computing can prove to be a boon in today's work environment hence this paper deals with data security issues related to cloud computing so that data centres can provide a good environment to keep data. The above mentioned scheme revolves around the problem of data security and with the help of encryption at client side and steganography at server side provides a highly secure model that will not only solve the issue of data safety but also simple in its implementation and hence usage. As per now the above mentioned scheme has been implemented using java. In future, the technique of image compression would be added to improve storage.

REFERENCES

[1] Security and privacy in cloud computing by Zhifeng Xiao and Yang Xiao in *IEEE Communications Surveys and tutorials*, 15.

[2] Data security in the world of cloud computing by Lori M. Kaufman John Harauz in *IEEE Computer and Reliability society.*

[3] Enhanced data security in cloud computing with third party auditor by Indrajit Rajput in *International Journal of Advanced Research in Computer Science and Software Engineering*, 3.

[4] Robust Data Security for Cloud while using Third Party Auditor by Abhishek Mohta,Ravi Kant Sahu and LK Awasthi, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol No. 2, Issue 2,Feb 2012.

[5] Cloud Data Security using Authentication and Encryption Technique by Sanjoli Singla and Jasmeet Singh in IJARCET Vol 2, Issue 7, July 2013.

[6] Survey on triple system security in cloud computing by Parul Mukhi and Bhawna Chauhan in IJCSMC, Vol. 3, Issue. 4, April 2014.

[7] Enhancing security in cloud computing structure by hybrid encryption by Aparjita Sidhu and Rajiv Mahajan in International Journal of Recent Scientific Research Vol. 5, Issue, 1, pp.128-132, January, 2014.

[8] Data Security in Cloud Computing by K. S. Wagh, Swapnil Chaudhari, Anita Deshmukh and Prajakta Khandave in International Journal of Current Engineering and Technology.

[9] A proficient model for high end security in cloud computing by R. Bala Chandar, M. S. Kavitha and K. Seenivasan in ICTACT journal on soft computing ,january 2014, volume: 04, issue: 02.

© 2015, IJCSMC All Rights Reserved

[10] Enhancing Data Storage Security in Cloud Computing Through Steganography by Mrinal Kanti Sarkar and Trijit Chatterjee in ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014.

[11] Enhancing Security in Cloud computing using Public Key Cryptography with Matrices by Birendra Goswami and Dr.S.N.Singh in Vol. 2, Issue 4, July-August 2012, pp.339-344.

[12] Fingerprinting Based Recursive Information Hiding Strategy in Cloud Computing Environment by Varsha Yadav and Preeti Aggarwal in IJCSMC, Vol. 3, Issue. 5, May 2014.

© 2015, IJCSMC All Rights Reserved