ISSN 2395-1621

Big data Security using Hybrid Cloud

[#1]Mr.V.P Rao, [#2]Gaurav Khandar, [#3]Manas Kulkarni, [#4]Shubham Nayab, [#5]Gaurav Shahane

[1]punnarao007@gmail.com
[2]gauravkhandar@gmail.com
[3]mskulkarni1995@gmail.com
[4]shubham.nayab@gmail.com
[5]shahanegaurav007@gmail.com

[#2345]Students Department of Computer Engineering,
Savitribai Phule Pune University

[#1]Assistant Professor Department of Computer Engineering,
Sinhgad Institute of Technology and Science,
Narhe. Pune 411041, India

ABSTRACT

Nowadays large amount of data is produced by many sources. The amount of data is being produced directly proportional with the rapid development of electronic technology and communication, which makes it hard to cost-effectively manage and store these big data. Cloud computing, which is a new business model, is considered as one of most attractive solutions for big data, and provides the benefits of low cost through sharing of computing and storage resources. However, the increasing concerns of the privacy of data which is stored in public cloud have slowed down the adoption of cloud computing for big data because very sensitive information may be contained among the big data or the data owner themselves do not want any other people to watch and observe their data. Since the data volume is huge and mobile devices are widely used, the traditional cryptographic methods are not suitable for big data. In this project work we are implementing the modified approach for the image and text encryption. Also in this work we proposed a approach for the efficient decryption technique by keeping the existing shuffling technique. With the encryption technique we have used steganography for text data storage. In this project we are going to use hybrid cloud mechanism to store the data. we store small amount of information about data on the private cloud as a reference and other data is store on the public cloud..

Keywords: **Cloud Computing, Big Data, Cryptography**

ARTICLE INFO

Article History

Received:30th October 2015

Received in revised form :

1st November 2015

Accepted:3rd November 2015

Published online :

6th November 2015

I. INTRODUCTION

We know the cloud is getting popular nowadays because it provide flexibility for data storage. Cloud support ubiquitous computing which means the user can access their data from anywhere, anytime and any condition. It also support large size of storage where user can store their data efficiently.

There are two main types of the cloud which are private and public cloud. Private cloud is considered as secure cloud because the information of user can only access by the user itself and no other person can access it. But the public cloud is not as much secure like private cloud. The information which is stored on the public cloud can be accessible to the cloud service providers. They can access the users information and can be used for their benefits they may use that information for advertising etc.

We know that nowadays large amount of data is being generated from different sources like social networking sites, online shopping this data can contain some sensitive information. Private cloud is safe place for storing this sensitive data but the private cloud is having small size and the cost for data storage on the private cloud is more so this is not efficient for the user. There is another option for this data storage which is public cloud but as we know the public cloud does not provide security like private cloud it is also not efficient. So can we use hybrid cloud mechanism? For securing our valuable data.

Hybrid cloud is a infrastructure which combine both private and public cloud. It store the users information on the public cloud by specifying their references on the private cloud.

Hybrid cloud stores little information about data on the private cloud and most of the data is store on the public cloud. While accessing the data from the public cloud there is need of communication between private and public cloud.
In this project we are propose a solution for security of the data using hybrid cloud which secure our image as well as textual data.

II. RELATED WORK

The data security and privacy in the cloud is proposed by the method named as attributed based encryption in which encryption and decryption is used for data security. In attributed based encryption where each data file is having some attributes associated with it and authorities are specify for each user to access that data file.
A framework had been proposed for controlling the private cloud access by using some authorization on the private cloud this method was efficient for the protecting our data from the unauthorized access but there is need to use traditional cryptographic algorithms which makes this framework unacceptable.
Another method is proposed for image security in which image is cut down into multiple pieces and the pixel values of that pieces are modified but in this method there is need of large computation because of this the method is become hard to use and it is not accepted by the user.
There is another method for the image security which secure the images on the public cloud. In this method the image is cut down into pieces and their pixel values get modified by using noise values and after that pieces gets shuffled. All the pixels in the same piece are modified using same noise value.

III.PROPOSED SYSTEM

In our project we propose a novel solution for securing the image and text data by using hybrid cloud infrastructure.
Figure 1 shows the architecture of the hybrid cloud. Hybrid cloud is consist of both private and public cloud. As we know the private cloud has less space but it is secure cloud and public cloud has large capacity to store data but it has less secure than the private cloud.
Hybrid cloud takes advantage of the both private and public cloud. It store the sensitive information on the private cloud and non-sensitive information on the public cloud. There is need of communication between the private and public cloud.
In our project we are propose a system in which we are going to use this hybrid cloud infrastructure for storage of big data. As the large amount of data cannot store on the private cloud because it has less capacity and the cost associated with storage is high therefore it is not efficient solution for data storage. So we store the small amount of data on the private cloud as a reference and the large amount of data is to be store on the public cloud. This reduces the cost of data storage and load of the private as most of the computation on the data is carried out on the public cloud.
Whenever the user wants to store their data on the cloud they will give their data to private cloud. Private cloud will store the small amount of information about that data on the private cloud as a reference in the encrypted form and other information will be stored on the public cloud which is also encrypted for security purpose. The private cloud store the keys to access the data from the public cloud that keys are also encrypted.
Whenever the user wants to access their data they will send the request to the private cloud. Then private cloud fetches the users data from the public cloud. After that data will be decrypted and then this data will be delivered to the user.

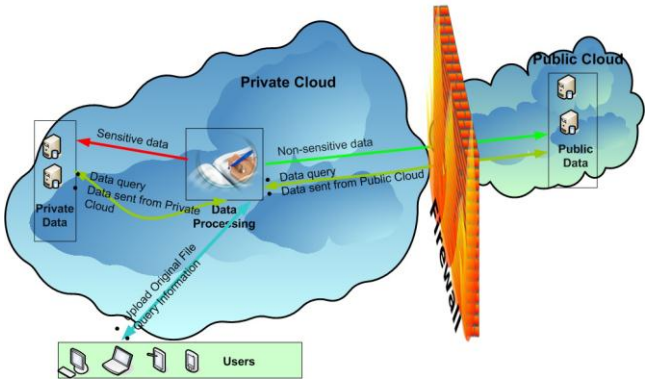

Fig1. Hybrid Cloud Architecture

IV.ALGORITHMS

In this project work, our aim is to achieve the image and text data privacy using hybrid cloud. But the drawback of existing system is, it takes much amount of time for the communication between the private and public cloud. So our first aim is to reduce the communication delay between the private and cloud.

Proposed encryption algorithm:
Algorithm 1:
Input: original image.
Output: Encrypted blocks of image.

```
//get the pixels of original image
OPix <- GetPixel(image);
//get width and height
W=getwidth(image);
H=getHeight(image);
// Obtain encrypted pixel values
mVal= OPix/ (NBloacks/g)
EPix= M*OPix*nBlocks + mVal;
// convert these pixels into final encrypted image
Eimg=ConstructImg(EPix);
// Divide encrypted image into small bloacks
sBloacks =GetBlocks(Eimg);
//  Perform shuffling
St <- {1,2,….nBloacks};
S <- {0,1,…...nBloacks-1};
S=S+St  if current block is chosen;
S=S+1;  Otherwise.
// store small information on private cloud.
```


Storeinfo(W,H,S,St,name);
Where,
Image= image.
OPix= original image pixel array.
W= width of image.
H= Height of image
EPix= Encrypted image pixels.
M= random parameter and m<no of block.
nBlocks = No of blocks to be generated.
mVal=Intermediate Value.
g=GCD of nBloacks and M.
sBloack= Array of encrypted block.

Algorithm 2:
Decryption :
Input: Image name (blocks of encrypted image).
Output: Original Image.
//Get information from private cloud.
Getinfo();
// get encrypted image from small blocks
Eimg=(sBlocks);
//get pixels of encrypted image
EPix= (Eimg);

//Obtain original image.
OPix= (EPix * nBloacks) / (M * $nBlocks^2$ +g) ;
// Get original Image
Image= ConstructImg(OPix);

V. CONCLUSION & FUTURE WORK

In this system we are implement the infrastructure for big data security. In this system we are using hybrid cloud framework for security purpose. This system is help to user to secure their data and easy retrieval whenever needed. Future work on this system comprises of more effective techniques and our contribution we improve the system by creating a instance randomly notifying a message system that should instead of blocking, or detecting the modifications of profile attributes that have been made for the only for defeating the filtering system. User will get mail notifications automatically. We will work on filtering posted audio and video messages. We can also reduce the communication time between the private and public cloud.

REFRENCES

[1] F. C. Lau, C. Wu L, Zhang, C. Guo, ,Z. Li, and "Moving big data to the cloud: An online cost-minimizing approach," JOURNAL ON SELECTED AREA IN COMMUNICATIONS, 2013.
[2] D. Chen and H. Zhao, " security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering(ICCSEE), 2012 International Conference on*, 2012.
[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *INFOCOM,2010 Proceedings IEEE*, 2010.
[4] J. Li, C. Jia, J. Li, and Z. Liu, "Framework for outsourcingand sharing searchable encrypted data on hybrid cloud," in *IntelligentNetworking and Collaborative Systems , 2012 4th International Conference on*. Springer, 2012.
[5] T. Jung, X.-Y. Li, Z. M. Wan, and Wan, "Privacy preserving cloud data access with multi-authorities," in *IEEE INFOCOM*, 2013.
[6] K.-W. Wong, Y. Wang, G. Chen, and X. Liao, "A new chaos-based fast image encryption algorithm," *Applied soft computing*, 2011.

