Big Data Security Using Hybrid Cloud

Gaurav Khandar
Student Department of Computer Engineering
Sinhgad Institute of Technology and Science
Narhe, India

Manas Kulkarni
Student Department of Computer Engineering
Sinhgad Institute of Technology and Science
Narhe, India

Gaurav Shahane
Student Department of Computer Engineering
Sinhgad Institute of Technology and Science
Narhe, India

Shubham Nayab
Student Department of Computer Engineering
Sinhgad Institute of Technology and Science
Narhe, India

Mr. V.P. Rao
Assistant Professor Department of Computer
Sinhgad Institute of Technology and Science
Narhe, 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 approach for the efficient decryption technique by keeping the existing shuffling technique. With the image encryption technique we have used encryption 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 ,Hybrid cloud ,Encryption, Decryption, DES(Data Encryption Standard)

I. Introduction

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

While providing the services to the user cloud computing proposes two types of cloud which are private cloud 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 problem with private cloud is it is expensive it is not suitable to store large data because of expensiveness on the other hand public cloud is cheaper than the private cloud but 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 user’s information and can be used for their benefits they may use that information for advertising etc.

Today 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 an infrastructure which combines both private and public cloud. It stores the user 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 our project we are propose a solution for security of the data using hybrid cloud which secure our image as well as text 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.

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. System Design

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. Then the original data will be transformed into encrypted form after that 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 and that keys are also encrypted.

Whenever the user wants to access their data they will send the request to the private cloud. Then using the keys which are stored on the private cloud the users data will be fetch from the public cloud. After that data will be decrypted and then this data will be delivered to the user.

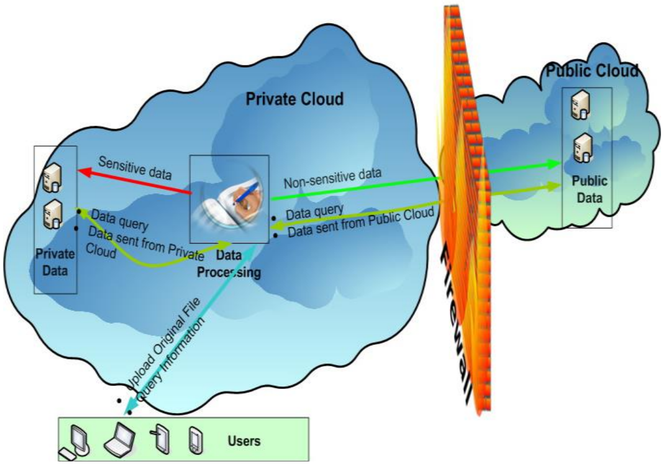

Fig. 1. System Design.

IV. Algorithms

To implement the system for providing security to data here we use two algorithm first is DES (Data Encryption Standard) used for text encryption and we propose second algorithm for image encryption and decryption which is based on encryption of block of data. In this algorithm the at first the width and height of image is obtained after that calculate the co-ordinates of each pixel of the image, after that image will be divided into number of blocks, once the image is divided into blocks are shuffled, then the keys which are required to decrypt the image are store on the private cloud of the user and all other blocks get store on the public cloud. Whenever user wants data from public cloud they send request to the private cloud, by using the reference of the data which are stored on the private cloud all the blocks of images and text data are fetched from the public cloud.

A. Image Encryption Algorithm

Input: Original image

Output: Encrypted block of image

Step1: Get the pixels of the original image.

Step2: Obtain the height and width of the image.

Step3: Obtain the encrypted pixel values.

Step4: Convert this pixels into final encrypted image.

Step5: Divide the encrypted image into small blocks.

Step6: Shuffle the encrypted image blocks.

Step7: Encrypt the keys and store it on the private cloud.

Step8: Store the encrypted data on the public cloud.

B. Image Decryption Algorithm

Input: Image name (block of encrypted image).

Output: Original Image.

Step1: Obtain the keys from the private cloud.

Step2: Get the encrypted image from small blocks.

Step3: Get the original pixels of the image.

Step4: Get the original image and send it to the user.

CONCLUSION

In this system we implement the infrastructure for big data security. In this system we are using hybrid cloud framework for security purpose. This system will help user to secure their data and easy retrieval whenever needed. Future work of this system comprises of more effective techniques for encryption and decryption of data. We can also implement the system with functionalities in which user will get mail notifications automatically whenever they login into their account. We are work on filtering posted audio and video messages. We can also reduce the communication time between the private and public cloud. We can also provide security to audio and video data.

REFERENCES

[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 outsourcing and sharing searchable encrypted data on hybrid cloud,” in Intelligent Networking 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.