ISSN 2395-1621

Achieving Bigdata Privacy Via Hybrid Cloud

[#1]Borge Shraddha G, [#2]Doke Poonam S, [#3]Gabadule Asmita G, [#4]Devkar Pooja S

[1]shraborge12345@gmail.com
[2]doke.poonam4@gmail.com
[3]poojarahulkadam2611@gmail.com
[4]asmita.gabadule@gmail.com

[#1234]Zeal College of Engineering, Narhe , Pune, Maharashtra, India.

ABSTRACT

Nowadays the amount of data is being produced exponentially with the rapid development of electronic technology and communication, which makes it hard to cost-effectively storeand manage these big data. Cloud computing, a new business model, is considered as one of most attractive solutions for big data, and provides the advantage of reduced cost through sharingof computing and storage resources. However, the growing concerns in term of the privacy of data stored in public cloud have slowed down the adoption of cloud computing for big databecause sensitive information may be contained among the big data or the data owner themselves do not want any other people to scan their data. Since the data volume is huge and mobiledevices are widely used, the traditional cryptographic approach are not suitable for big data.

Keywords— bigdata; hybrid cloud; bigdata privacy,encreption & decreption algorithm.

ARTICLE INFO

Article History

Received :2nd December 2015

Received in revised form :

5th December 2015

Accepted:6th December , 2015

Published online :

9th December 2015

I. INTRODUCTION

Existing work in cloud computing has considered the storage on a private cloud in order to make the data storage secure. In this system we use the hybrid cloud where concept of public cloud is used for large data storage and private cloud is used for the small information storage. Existing work has proposed hybrid cloud for image data, but we propose the algorithms for the image data as well as we extend our work for the text data with existing image data.

In this project work, our aim is to achieve the image 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 public cloud. Secondly to reduce the overhead caused by the creation and shuffling of images block using complex algorithm with implementation of simple algorithm,. Third this is to reduce the amount of data stored on the private cloud.Also we are extending our work for the encryption of data stored on the private cloud. This is the major contribution we added to the project.

II. MOTIVATION OF THE PROJECT

With the rapid development of electronic and communication technology, the amount of data produced by medical systems, surveillance systems or social networks has been grown exponentially, which makes it hard for many organizations to cost-effectively store and manage these big data. Cloud computing, a new business model, is considered as one of most attractive and cost-effective solutions for big data, and provides the advantage of reduced cost through sharing of computing and storage resources. It utilizes an on demand provisioning mechanism and a pay-per-use model, and has drawn a lot of attentions in recent years. However, the growing concerns in term of the privacy of data stored in public cloud have delayed the adoption ofcloud computing for big data. On one hand, a large amount of image, such as medical systems or social networks, may contain sensitive information. On the other hand, Cloud Service Providers (CSPs), who own the infrastructures on which clients' data are stored, have full control of the stored data. Therefore, the data stored in

public cloud may be scanned by CSPs for advertisement or other purposes. Furthermore, attackers may be able to access data stored in cloud if there is not sufficient secure mechanism provided by CSPs. Most existing solutions (e.g., employ traditional cryptographic algorithms, such as AES, to encrypt data andthen store encrypted data in public cloud. However, for image data, which have much larger size than text data, heavy computation overhead will be introduced by this approach. Meanwhile, for the mobile devices, which have been widely used, much battery energy will be consumed, and it will increase delay because of the limited computation resources.Therefore, the traditional cryptographic approaches are not
suitable for big data privacy.

In recent years, various image encryption algorithms havebeen proposed to speed up the process, among which thechaos-based approach with a substitution-diffusion layout appears to be a promising direction . In the substitutionstage, the positions of pixels of the image are shifted viasome chaotic map, and then the pixel values of the shuffledimageare changed by chaotic sequences in the diffusion stage.However, the chaos system itself causes large computationOverheadAnother approach is to take advantage of hybrid cloud byseparating sensitive data from non-sensitive data and storingthem in trusted private cloud and un-trusted public cloudrespectively. However, if we adopt this approach directly,all images containing sensitive data or the ones that wouldnot like to be seen by others have to be stored in privatecloud, which would require a lot of storage in private cloud.Most users want to minimize the storage and computation inprivate cloud, and let public cloud do most of the storageand computation. To address the above challenge, we need toanswer an important problem: How to efficiently achieve bigdata privacy by using hybrid cloud? Compared to using publiccloud only, using hybrid cloud would have communicationoverhead between private and public cloud. Besides achievingdata privacy, we want to reduce storage and computation inprivate cloud, as well as communication overhead betweenprivate and public cloud. In addition, the delay introduced bycommunications between private and public cloud should besmall.

III. LITERATURE SURVEY

Name of topic	Published in	Merits	Demerits
Privacy preserving cloud data access with multi-authorities	Apr-2013	1.Anonycontrol function 2.multi-authority	Encryption and decryption is slow
Cloud computing and security issues in the cloud	Jan-2014	Integrated security model	Security issue is sensitive
A probabilistic image jigsaw puzzle solver	2010	1.Accuracy 2.compatibility	Object and texture representation
Achieving secure,scalable and fine-grained data access control in cloud computing	2010	1.High efficient 2.User access confidentiality	Untrusted server attack
*Achieving Bigdata privacy via hybrid cloud	2014	1.Security in public and private cloud. 2.Image and text data security 3.Less communication delay	Handling huge data on public cloud is somewhat challenging

IV. MAJOR CONSTRAINTS

- **Private cloud:**

A private cloud is established for a specific organization and limits the access to it.It offers increased security because of its private nature.

- **Public cloud:**

It is the traditional cloud computing.As the name indicates it can be accessed by any subscriber who has an internet connection and access to the cloud space.The public cloud may be less secure because of its openness.

- **Hybrid cloud:**

It is a combination of at least two clouds,where the clouds can be public,private or community.when there is a public and another private cloud combination,then the critical activities are performed using private cloud and non critical activities are performed using public cloud.

- Hybrid cloud for image and text data storage.also we are enhancing file data.
-

4.1 Equestion

Fme:functions used
1.upload()
2.download()
3.getinfo()
4.decryptimage()
5.encryptimage()

Formulae:
OPix= (EPix * nBlocks) / (M * $nBlocks^2$ +g)

$$P' = (M * P * n) + \frac{P}{\frac{n}{g}}$$

Success Conditions: we can achieve the image data privacy using hybridcloud.

Failure Conditions: If the delay between the private and public cloudis more then the system fails to achieve the image data

4.2 Methodologies of Problem solving and efficiency issues

Encryption

- It means convert the original form of data into the cipher text form
- cipher text is the unreadable form of data.

Decryption

- It means convert the cipher text into the original form of text.

Efficiency issues

All functions on totaly depends on the system configuration.

4.3 Architectural Design of proposed system

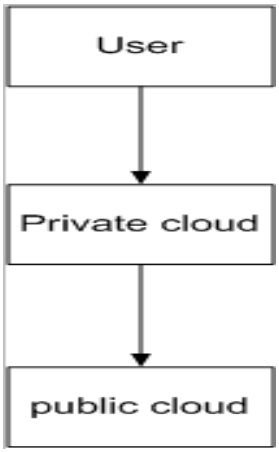

Fig:-Architectural Design of proposed methodology

4.4 Encreption

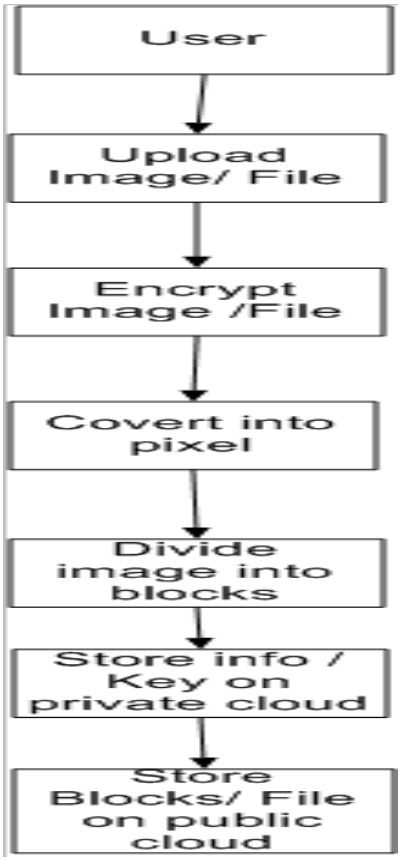

Fig-:process steps in encreption algorithm

4.5 Decreption

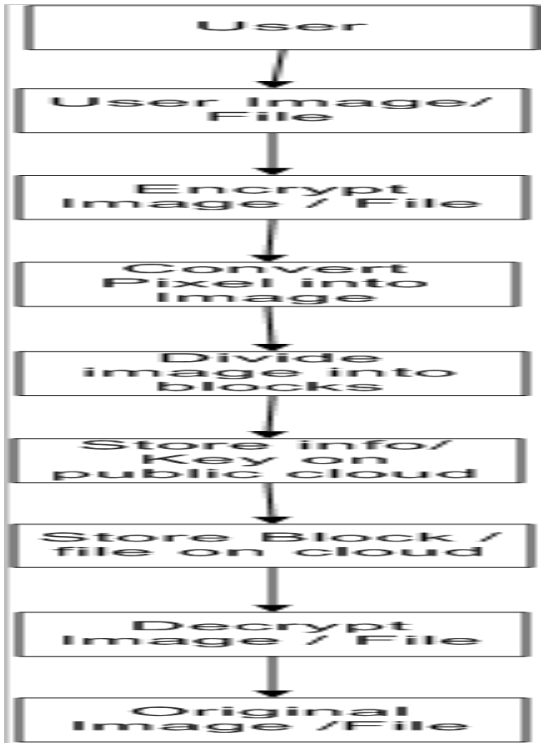

Fig-:process steps in decreption algorithm

4.6 Architectural Design

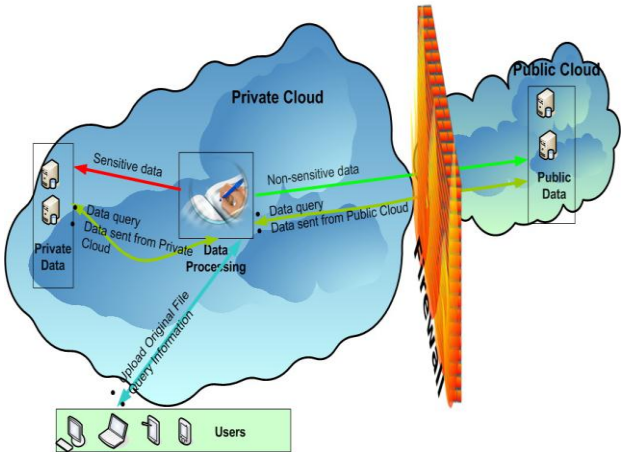

Fig.Architecture of system

The original data come from private cloud, and are processed on servers within private cloud. If there are no sensitive data, the original data may be sent to public cloud directly. Otherwise, the original data will be processed to make no sensitive data leaked out. After being processed, most data are sent to public cloud, and a small amount of sensitive dataare kept in private cloud. When a user queries the data, both private cloud and public cloud will be contacted to provide the complete query result. consider an un-trusted public cloud who are curious and may intend to browse users' data. The public cloud has full control of its hardware, software, and network.

V. CONCLUSION

We can conclude with points such as our project is reduced time for communication between public and private acloud.We decreased the data load on private cloud.and try to balance the data on public cloud.We provide the security for the image data strored on public cloud.This project is useful for image,text,file data security and storage.

ACKNOWLEDGEMENT

There are several people without whose help this project would never have been successfully completed. We take this opportunity to thank them for their help and timely support throughout the making of this project. First and foremost, We wish to express our sincere thanks to our Internal guide, guide**Mr. AvinashL.Golande** their invaluable guidance to us and their constant motivation has not let our spirit die.. We will forever remain grateful for tconstant support and guidance extended by guide, in making this project successful till now. Through our many discussions, he helped us to form and solidify ideas. The invaluable discussions we had with her, the penetrating questions he has put to us and the constant motivation, has all led to the development of this project till now with great passion.

REFRENCES

[1] X. Huang and X. Du, "Ensuring data privacy by hybrid cloud," in IEEE ICC, 2013.

[2]L. Zhang, C. Wu, Z. Li, C. Guo, M. Chen, and F. C. Lau, "Moving big data to the cloud: An online cost-minimizing a1]Xueli Huang and XiaojiangDu,"Achieving Big Data Privacy via Hybrid Cloudpproach," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 2013.

[3]D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, 2012.

[4] T. Cho, S. Avidan, andW. Freeman, "A probabilistic image jigsaw puzzle solver," in Computer Vision and Pattern Recognition (CVPR), 2010 IEEE Conference on, 2010.

