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. 3, Issue. 8, August 2014, pg.390 – 394

RESEARCH ARTICLE

Secured Access Control Driven Pay per Usage and Logging of Cloud Resources

Sudha.V.Pareddy, Prof. Chandrakant.Biradar

Department Of Computer Science, PDA Engineering College, Gulbarga, Karnataka, India

[1] pareddyvsudha@gmail.com; [2] cbiradar@rediffmail.com

Abstract- Recent trends of the generation has given the unique platform to work on the Cloud based data sharing integrated with access control, which is the latest trend for sharing multimedia data form cloud with ease and secured way. However, managing the access log for such data sharing is complicated issue due to the data size, privacy and other issues related to the data. The data provider accept the detail analytical of every invent on this data by others getting the log file by others can link several critical information. In this work we propose novel approach for access of cloud based data handle and show that the security extension added with the work, which does not add extra overhead in terms of processing time. We also show that the system is applicable of new logging like real time event of Face book data sharing.

Keywords: data sharing, access control, log file, data handle, face book

I. INTRODUCTION

Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources it puts entire computing infrastructure hardware and software. Applications etc. online for user. Cloud Computing is a step towards the evolution of on demand information technology services and products. The cloud makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. Your cloud provider can both own and house the hardware and software necessary to run your home or business applications one requirement is that you need to have an internet connection in order to access the cloud. This means that if you want to look at a specific document you have housed in the cloud, you must first establish an internet connection either through a wireless or wired internet or a mobile broadband connection. The benefit is that you can access that same document from wherever you are with any device that can access the internet. These devices could be a desktop, laptop, tablet, or phone. Which can be any of different types of clouds like Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud are used as the requirement demands. Although there are many benefits to adopt Cloud Computing but still there are some significant barriers to adoption. The convenience and efficiency of this technology comes with security risks and data privacy. Significant barrier to the adoption of cloud services is the user's fear of losing confidential data and privacy in the cloud. Privacy is an important and basic human right that encompasses the right to be left alone, to provide this right many techniques are proposed under different systems and security models. No matter how careful you are with your personal data, by subscribing to the cloud you will be giving up some control to an external source. This distance

between you and the physical location of your data creates a barrier. It may also create more space for a third party to access your information although most cloud providers will have a great deal of knowledge on how to keep your data safe. A provider likely has more resources and expertise than the average user to secure the data.

II. RELATED WORK

In this section review related works addressing security in cloud. Security issue is very important in cloud there are many techniques available so here is review of all these.

"Secure cloud storage based on cryptographic techniques "Infrastructure as a service (Iasi) is a model of networked online storage where data is stored in virtualized pools of storage. As fast development and application of cloud and it expose secure cloud storage in which cryptographic techniques have been used to their designs and indicate what type of cryptographic techniques is mainly adopted in existing cloud storages and what role the cryptographic techniques play [1]

"Ensuring Data Storage Security in Cloud Computing "Cloud computing is the next generation architecture of IIT Enterprise. Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. [2]

III.EXISTING SYSTEM

Most of Existing systems adopt the Conventional access control approach, for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the two following reasons.

First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner.

As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

Drawbacks from existing systems are:

1. The conventional access control approach must require any dedicated authentication and storage system.
2. The user cannot have the information regarding usage or access of data by other users.
3. Requires third-party services to complete the monitoring and focuses on lower level monitoring of System resources

IV.PROPOSED SYSTEM

To overcome the issues n the existing system we propose the hybrid approach for data access and manage in the cloud where the data is secured using administrating access control, through the user name and password because SQL query does not support querying on encrypted data. In the proposed system the special enquire access log in generated for the events and encrypted barring the user ID field which retail the entity model. Hence log can be easily kept as encrypted data and can be decrypted as and when required.

Hence the system will be under the administrative supervision and log files will help for the time based inspection for system Audit.

Proposed system provides higher security because Images are stored as strings and one of the main advantages is Security and System provide logging hence unauthorized user cannot access the log and Some of the applications of proposed system are Public image sharing, Profit based resource sharing of a cloud and Secured data storage over the cloud session based data management of the cloud.

Figure (1) show the proposed system design for Secured Access Control driven Pay per Usage and Logging of Cloud Resources.

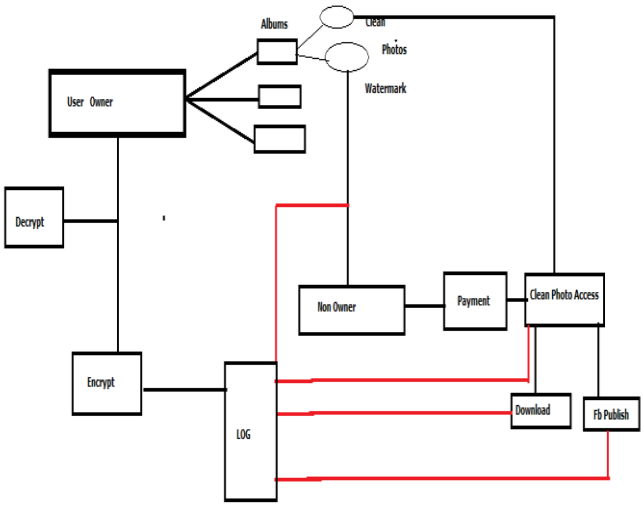


Fig 1: Secured Access Control driven Pay per Usage and Logging of Cloud Resources.

V. RESULTS AND ANALYSIS

The following section describes the results of the proposed system: Following figure shows the process of sign in and home showing process and uploading the data (image).

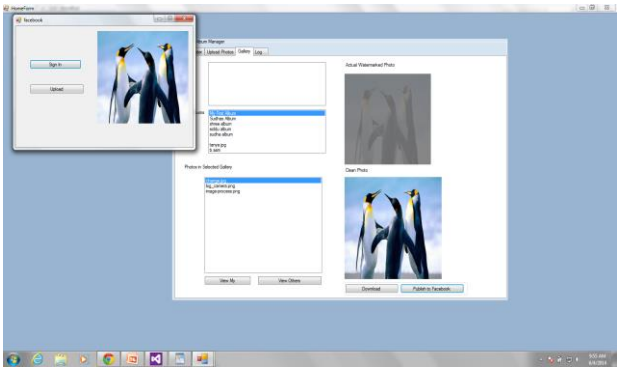


Fig 2 .Signing in and uploading data

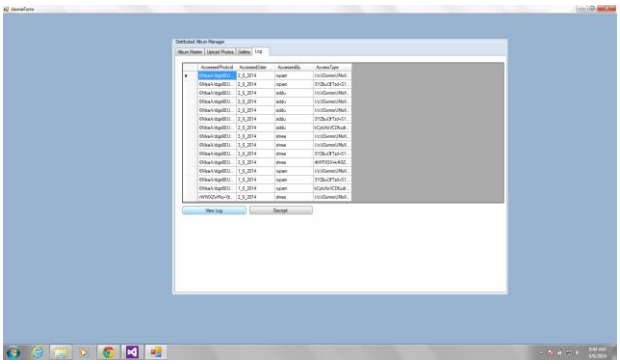


Fig 3 show the result of Encrypted log file.

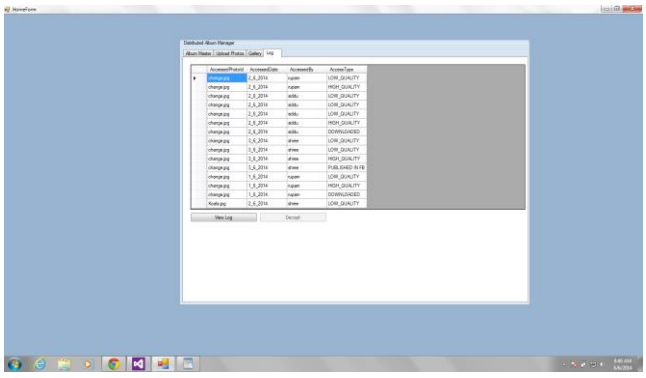


Fig 4 show the result of Decrypted log file

Access Time: Following graph shows the access time for data which show that the sizes of the log file is irreverent for access time and because the access time is independent of time and can be easily used for multi user multi access data categories

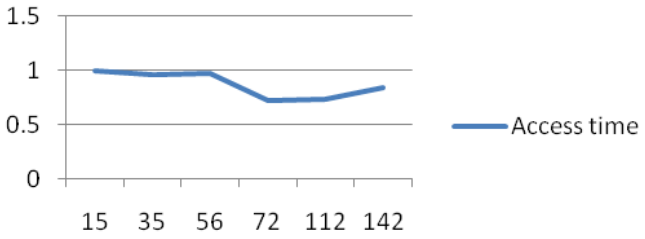


Fig 5 .Comparison Graph showing access time Vs Log file size.

Decryption time: Following graph shows the decryption time taken for the log file to be decrypted it can be seen that irrespective of the enter in the file the time is consistent. The variations are due to the communication overhead.

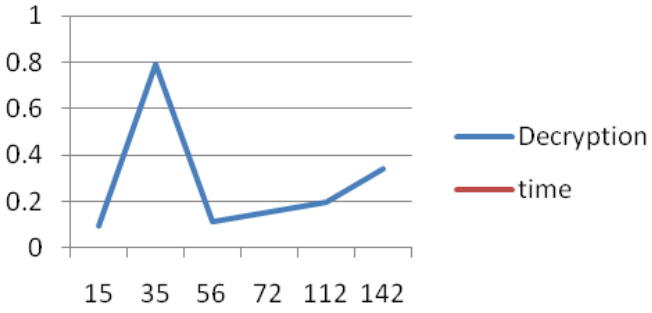
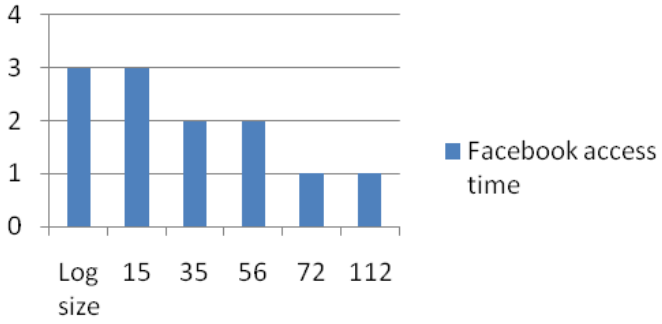


Fig 6 Comparison Graph showing Decryption time Vs Log file size

Face book access time:

Following graph shows the Face book access time taken for log entry and publish with respect to different log size of the image and communication delay therefore it is proved that managing the secured access log data sharing is independent of the user log access time increases and log time.



The Fig 7 Comparison graph for the Face book access time taken for log entry

VI. CONCLUSION

Hence we finally conclude the results show that processing overhead does not increase when log increases. It justifies the adopted security extension for the access log is perfect for real time application. The system is also tested under multiple users in the different machine by providing more efficiency and security.

The work can be further improving by extending the work to incorporate payment method.

REFERENCES

[1] PENG Yong, ZHAO Wei, XIE Feng, DAI Zhong-hual "secure cloud storage based on cryptographic techniques" 19 , Supplement 2 , Pg. 182-189 (2012)

[2] Ensuring Distributed Accountability for Data Sharing in the Cloud Author, Smitha Sundareswaran, Anna C.Squicciarini, Member, IEEE, and Dan Lin, IEEE Transactions on Dependable and Secure Computing ,VOL 9,NO,4 July/August 2012

[3] S. Pearson, Y. Shen, and M. Mowbray," A privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (cloudcom). VOL. 9, NO 4, pg 556-568, 2012

[4] P.T. Jaeger, J. Lin, and J.M. Grimes, "Cloud Computing and Information Policy: Computing in a Policy Cloud?" J. Information Technology and Politics, vol. 5, no. 3, pp. 269-283, 2009.

[5] S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (Cloud Com), pp. 90-106, 2009.

