ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3 , Issue 4 , April 2014

Time Constrained Data Destruction in Cloud

P.Mani Priyadharsini[1], Mr.M.Gughan Raja[2]

PG Scholar[1] , Assistant Professor[2]

[1&2]Department of Computer Science and Engineering,SyedAmmalEngineering College, Ramanathapuram , Tamil Nadu ,India.

Abstract-This paper presents some of the important details of the client is stored in the cloud. Personal data that can be stored in the cloud and other important information that could be used by other user. These data are cached, copied by the cloud service providers. The security for the content stored in the cloud is very important. For that the system used in this to give the security in the cloud. The service provider owns the equipment and is responsible for housing, running and maintaining it. The data stored in the cloud is destructed automatically when the time limit exceeded. RSA is used for the data encryption and decryption. And also the time specification is also specified by the client. The data is deleted from storage node without interruption of the user. It is used in the time of uploading and downloading the data in the cloud. MAC is used to check the integrity of the data stored in the storage nodes.

Key Words: Cloud computing; data privacy; Active storage; Self-destructing data

I. INTRODUCTION

Several trends are opening up the era of Cloud Computing, is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management.

The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well-known examples. As people using more and more on the Internet and Cloud technology, security of their privacy takes more risks. When data is being processed, transformed and stored by the current computer system or network, systems or network must cache, copy it. These copies are essential for systems and the networks. People have no knowledge about these copies and cannot control them, hence these copies may leak their privacy. Their privacy also can be leaked via Cloud Service Providers negligence, hackers' intrusion or some legal actions.

A study of Vanish [1] supplies a new idea for sharing and protecting privacy. In this Vanish system, a secret key is divided and stored in a P2P system with distributed hash tables (DHTs). With joining and exiting of the P2P node, the system can maintain secret keys. According to the characteristics of P2P, the DHT will refresh every nodeafter about eight hours. With Safe vanish [4] To address the problem of Vanish, we proposed a new scheme, called *Safe Vanish*, to prevent *hopping attack*, which is one kind of the *Sybil attacks* [18], [19], by extending the length range of the key shares to increase the attack cost substantially, and did some enhancement on the Shamir Secret Sharing algorithm [20] implemented in the Vanish system.

The present work focusses on the related key distribution algorithm, which is used as the core algorithm to implement client (users) distributing keys in the object storage system. These methods are used to implement a safety destruct with equal divided key (Shamir Secret Shares [2]).Based on active storage framework, an object-based storage interface to store and manage the equally divided key.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3 , Issue 4 , April 2014

II. LITERATURE STUDY

Tang et al.[6] proposed FADE for the outsource data backup to third-party cloud storage services so as to reduce the data management costs, security concern arises in terms of ensuring the privacy and integrity of outsourced data. This FADE is designed as the practical, implementable, and readily deployable cloud storage system which focuses on protecting deleted data with policy-based file assured deletion.

FADE is built upon the standard cryptographic techniques, such that it encrypts the outsourced data files to guarantee their privacy and integrity. Most importantly, assuredly deletes files to make them unrecoverable to anyone (including those who manage the cloud storage) upon revocations of file access policies. This objective is implemented by a working prototype of FADE atop Amazon S3, one of today's cloud storage services, which provides policy based file assured deletion with a minimal trade-off of performance overhead. This work provides the insights of how to incorporate value-added security features into current data outsourcing applications..

Perlman et al. [8] describes a system that supports high availability of data, until the data should be deleted, at which time it is impossible to recover the data. This design supports three types of assured delete; expiration time known at file creation, on-demand deletion of individual files, and custom keys for classes of data. The obvious approach, of course, is to encrypt the data on non-volatile storage, and then destroy keys at the appropriate times.

Kang et al. [9] Object-based SCM: Storage class memories (SCMs) are playing an increasingly significant role in the storage hierarchy. The combination of lower power consumption, relatively large capacity, fast random I/O performance, and shock resistance make SCMs to attractive for use in desktops and servers as well as in embedded systems. Recently, deployment of Solid State Drives (SSDs) using NAND flash has rapidly accelerated, allowing SCMs to replace disks by providing an interface compatible with current hard drives. Systems using SSDs can deliver much better I/O performance than disk-based systems.

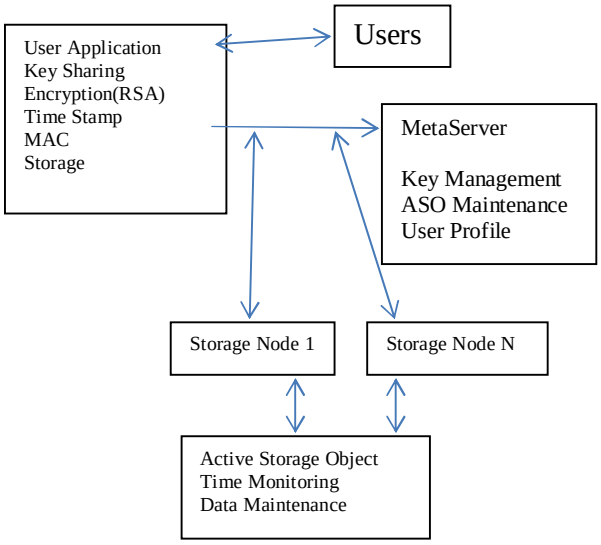
III. DESIGN AND IMPLEMENTATIONS

A. *System Architecture*

The following parameters are based on the active storage framework.

- Meta server: It is responsible for key management, User profile, active storage object (ASO) Maintenance.
- Application node: The application node is a client to use storage service.
- Storage node: Each storage node is an OSD. It contains two core subsystems: key value store subsystem and ASO runtime subsystem.

The key value store subsystem is based on the object storage component which is used for managing objects stored in storage node: lookup object, read and write object and so on. The object ID is used as a key and the associated data, attribute are Stored as values. The ASO runtime subsystem based on the active storage agent module in the object-based storage system is used to process active storage request from users and manage method objects and policy objects.



ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3 , Issue 4 , April 2014

B. *User and Storage node Key Sharing*

First of all the client register the details to the server. And then the storage node also register the details to the Meta server. The client use the blowfish algorithm to generate the keys. Sharing of keys between the Meta server and the User application. Enable N storage node for storing the data's. Sharing the storage node with Meta server for shamir key sharing technique. The client can see the data that already uploaded in the storage nodes. The data are stored according to the size of the storage nodes.

C. Data Process

Data processing can be in two main phases. Upload and Download.

- File uploading process: The client will send the Upload request to the server. Then the server gives permission to upload the data to the client. After accepting get the N keys randomly from the user key. Then the client split the data according to the size of the storage node. Splitting the File into the N parts using Shamir shared keys. Encrypt the file using the Key value. Provide the Time Stamp (TTL) for the File.
- File Downloading Process: The client will send the download request to the server. If the file available in the network accept the download request. Then the client can downloading the file And Merge it.

D. Active Storage Object

Using the active storage object we can access the Storage node. For this one first we receive the File split from the user application. Get the Time stamp for the user application file. Create the interface. Store the files to the storage node and apply the security mechanism.

E. Self-Destruction Model

Time monitoring process will held. If the time stamp exceed the document will be automatically destroyed. The storage node doesn't get permission from the client to delete the data. The Store space will be refreshed. Details of the document also removed from the Meta server. Because of this the attackers can't get the details of the data.

Result and Discussion

In existing system the latency of the data stored in the cloud is very low when compared to the proposed system. Because the security in the existing system is also low. DES and AES are used to provide the security to the data stored in the cloud. In proposed system RSA algorithm is used to provide the security to the data stored in the cloud. RSA is more secure than the existing algorithms because of the key size. The key size of the RSA is 1024. And also based on the file size the data is splitting into many parts. So the attacker can't predict the data present in the cloud. And the continuation of the data in the cloud is also increased because of the file size. So that the latency of existing is low when compared to the proposed system.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3 , Issue 4 , April 2014

IV.CONCLUSION

With development of Cloud computing and popularization of mobile Internet, Cloud services are becoming more and more important for people's life. People are more or less requested to submit or post some personal private information to the Cloud by the Internet. When data is being processed, transformed and stored by the current computer system or network, systems or network must cache, copy it. Data security is very important in the cloud computing. Using our system we can provide security to the data. It conclude that provides security and integrity to the data that is stored in cloud. Due to this reason, it automatically delete the data when time limit exceeds without client intervention. In addition, the decryption key is destructed after the user-specified time.

REFERENCES

[1] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in Proc. USENIX Security Symp., Montreal, Canada, Aug. 2009, pp. 299–315.

[2] Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[3] S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Halderman,C. J. Rossbach, B. Waters, and E. Witchel, "Defeating vanish with low-cost sybil attacks against large DHEs," in Proc. Network and Distributed System Security Symp., 2010.

[4] L. Zeng, Z. Shi, S. Xu, and D. Feng, "Safe vanish: An improved data self-destruction for protecting data privacy," in Proc. Second Int. Conf.Cloud Computing Technology and Science (Cloud Com), Indianapolis, IN, USA, Dec. 2010, pp. 521–528.

[5] L. Qin and D. Feng, "Active storage framework for object-based storage device," in Proc. IEEE 20th Int. Conf. Advanced Information Networking and Applications (AINA), 2006.

[6] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion," in *Proc. Secure Comm*, 2010.

[7] T. M. John, A. T. Ramani, and J. A. Chandy, "Active storage using object-based devices," in Proc. IEEE Int. Conf. Cluster Computing,2008, pp. 472–478.

[8] R. Perlman, "File system design with assured delete," in *Proc. Third IEEE Int. Security Storage Workshop (SISW)*, 2005.

[9] Y. Kang, J. Yang, and E. L. Miller, "Object-based SCM: An efficient interface for storage class memories," in *Proc. 27th IEEE Symp. Massive Storage Systems and Technologies (MSST)*, 2011.

[10] Y. Xie, K.-K.Muniswamy-Reddy, D. Feng, D. D. E. Long, Y. Kang,Z. Niu, and Z. Tan, "Design and evaluation of oasis: An active storage framework based on t10 osd standard," in Proc. 27th IEEE Symp. Massive Storage Systems and Technologies (MSST), 2011.