ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

SEDAS: A Self Destruction for Protecting Data Privacy in Cloud Storage As A Service Model

Lalitha K[1], Sasi Devi J[2]

M.E. Student, Department of CSE, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India [1]

Head of the Department, Department of CSE, Dhanalakshmi srinivasan engineering college, perambalur, Tamilnadu, India [2]

Abstract- In Cloud computing focuses on maximizing the effectiveness of the sharing of resources. It is not only shared by multiple users but can also dynamically reallocating as per demand. Personal data stored in the cloud may contain account number, password, notes and other important information that could be used and misused by a miscreant, a competitor or a court of law. These data are cached, copied and archived by Cloud Service Providers (CSPs), often without user authorization and control. To overcome this problem to propose a Self Destruction method is protecting the user data privacy through Shamir Secret sharing algorithm, which can generate a pair of keys. Self Destruction method is associated with Time to Live (TTL) property to specify the life time of the keys. TTL trigger the Self Destruction operation, then the keys becomes destructed or unreadable after a user specified period. User can decrypt after timeout, either the user give correct keys. Shamir algorithm generates new keys to the user. Self Destruction mechanism reduces the overhead during upload and download file in the cloud. The result demonstrates that Self Destruction is practical to use and meet all privacy preserving goals.

Keywords:- Active storage, Cloud computing, data privacy, self-destructing data.

I. INTRODUCTION

In traditional method, People more or less request to submit some personal private information to the cloud. When people do this, they subjectively hope service providers will provide security policy to protect their data from leakages, so the people will not protect their privacy from the leakages. On the other hand, when data is being processed, transformed and stored by the others. However, people have no knowledge about these copies and cannot control them, so these copies may leak their privacy. On the other hand, their privacy also can be leaked via Cloud Service Providers (CSPs), hackers or intruder. These problem present formidable challenges to protect people privacy.

In this paper, Self Destruction (SeDas) present a solution to implement a self destructing data system, Which consist of two main parts: 1) secret key part-generate a pair of keys through shamir secret sharing algorithm. 2) survival time part-specify time limit to each keys. Through this it can meet the following advantages: 1) No explicit delete action by any third party. 2) The keys can be self destructed after user specified time and also reduces the communication overhead as well as network delay. 3) Increase processing speed and it will meet all the privacy preserving goals.

1.1 Shamir Secret Sharing Algorithm

Shamir algorithm are ideal for storing information that is highly sensitive and highly important. A secret sharing method can secure a secret over multiple servers and remain recoverable despite multiple server failure. The dealer may act as several district participants, distributing the shares among the participants. Each share may be stored on a different server, but the dealer can recover the secret even if several servers break down as long as they can recover.

1.2 Self Destruction using Time to Live property

Time to Live is a mechanism that limit the lifespan or lifetime of keys stored in cloud. TTL may be implemented as a counter or timestamp attached to or embedded in the keys. Once the prescribed event occur or timespan has elapsed, keys can be self destructed without any user intervention. In computing application, TTL is used to improve performance of caching or to improve privacy from the leakages.

II. LITERATURE SURVEY

J.A.Chandy, M.John and T.Ramani "An Active Storage System for High Performance Computing", Traditional active storage device execute custom application code on large amount of data by utilizing the unused processing power of the storage nodes for computation intensive application, the performance might be quite low due to insufficient processing power of storage nodes. H.Chai, D.Feng, C.Li and K.Zhou "Implementing and Evaluating Security Control for Object Based Storage System" The development of high performance computing has based on storage capacity and I/O performance, storage system has entered the peta byte era. The storage system scale of high performance computing is very large, the amount of storage nodes is very huge. Carns, P.Choudhary, S.Lang, B.Ozisikyilmaz and S.W.Son "Enabling Active Storage on Parallel I/O Software Stacks" As data sizes continue to increase the concept of active storage is well fitted for many data analysis kernals. The sedas system propose and evaluate an active storage system that allow data analysis, mining and statistical operations to be executed from with in a parallel I/O interface. H.Chai, D.Fang, c.li, W.Xial, L.Yingping and K.Zhou "QOS provisioning Framework for the OSD based storage system" Quality of Services is crucial for certain application such as multimedia. The main goal is to propose a QOS framework for OSD based storage system that integrate both the network QOS and storage QOS. Y.Kang, E.L.Miller and J.Yang "Object-based SCM: An Efficient interface for storage class memories" Storage Class Memory (SCM) has become increasingly popular in storage system. However, replacing hard drives with SCMs often forces either major changes in file system or suboptimal performance, because the current block based interface does not deliver enough information to the device to allow it to optimize data management for specific device characteristics such as out-of-place update.

III. BACK GROUND

Cloud computing is to allow user to take benefit from all the technologies, without the need for deep knowledge about or expertise with each one of them. It is not only sharing of resources but can also dynamically reallocating as per demands. User subjectively hope service providers will provide security policy to protect the data from the leakages. To protect these data is important also take more and more risk in cloud environment. To provide privacy they perform encryption using key. On the other hand, When data is being processed, transformed and modified by the hackers and intruders. To overcome these problem sedas system provide more security in cloud environment through Shamir algorithm and also reduce the runtime overhead as well as network delay.

IV. SYSTEM ARCHITECTURE

Shamir algorithm implemented in cloud server to generate a pair of keys to the user. The main components are key generation, encryption and decryption using Message Digest Algorithm. The user can also specify the lifetime of each keys. These keys associated with Time to Live (TTL) property. When the keys can be self destructed after user specified time without any user intervention. The encrypt and decrypt procedure uses a message digest algorithm (MD5) for encryption and decryption. MD5 has been utilized in wide variety of security application, and is also commonly used to check data integrity. Keys are stored in DHT, before download a data in cloud the Shamir algorithm check the keys match with hash table. Then only the given user is authorized to download data in cloud.

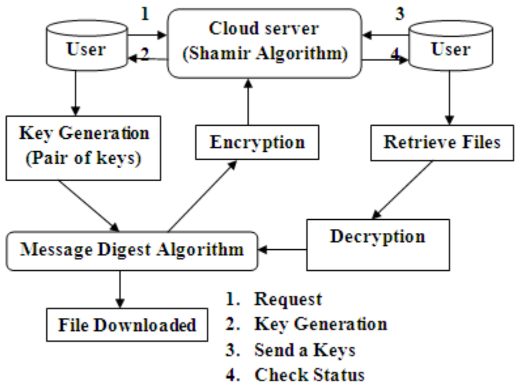

Fig 1.System Model

In Proposed system, sedas method implement automatic self destruction of keys to avoid explicit delete or modification of data in cloud environment by any third party or attackers. It leads several advantages are reduces communication overhead, network delay, generate pair of keys to single file (keys length is 2bytes) , increase processing speed, increase I/O performance and also it will meets all privacy preserving goals.

V. MODULES

User Authentication
Object Storage Devices (OSD)
Secret Key Part
File Uploading
Self Destruction Method
Downloading File
Performance Evaluation

5.1 Modules Description

User Authentication:- A new user has to first create a profile. This is done by registration. A user id and password are submitted by the user. The user can login successfully only if user id and password are entered correctly. The login is a failure if the incorrect user id or wrong password is entered by the user. This helps in preventing unauthorized access.

Object Storage Devices (OSD):- An OSD is a computer storage device, similar to disk storage but working at higher level. Instead of providing a block oriented a block oriented interface that reads and writes fixed sized block of data. Each object has both data (uninterpreted sequence of bytes) and metadata (an extensible set of attributes describing the object).The OSD is responsible for managing the storage the storage of objects and their metadata. OSD implements a security mechanism that provides the user data privacy. N extensible set of attributes describe objects. Some attributes are implemented directly by the OSD, such as the number of bytes in an object and the modified time of object.

Secret Key Part:- Shamir Secret Sharing is an algorithm in cryptography. It is a form of secret sharing. Where a secret is divided into parts, giving each participant its own unique part. Where some parts or all of them are needed in order to reconstruct the secret. Each of these pieces of information must be kept highly confidential. Secret sharing are ideal for storing information that is high sensitive and highly important and also allow arbitrarily high levels of confidentiality and reliability to be achieved.

File Uploading:- Before upload file in cloud the user perform encryption using pair of keys generated by Shamir algorithm through MD5.When a user upload only a encrypted file in cloud and stores his keys using sedas method, it should specify the file, keys and TTL as the arguments for uploading procedure. When the keys are self destructed after a user specified time.

Self Destruction Method:- Self destruction mainly aims at protecting the user data privacy. All the keys become self destructed or unreadable after user specified time. The result demonstrate that the sedas is practical to use and meet all privacy preserving goals described. Sedas does not affect the normal use of storage system and can also meet the requirement of self destructing data under a survival time by user controllable keys. These are multiple storage services for a user to store data. Meanwhile, to avoid problem produced by the centralized "trusted" third party, the responsibility of sedas is to protect the user keys and provide the function of self destructing data.

Downloading File:- Any user who has relevant permission can download data stored in the cloud. The data must be decrypted before use. If the self destruct operation has not triggered, the client can get enough key shares to reconstruct the keys successfully. During download process, Shamir algorithm checks the given keys are expired or not. If the keys are not expiring, the user can easily download. Otherwise, Shamir algorithm generates a new pair of keys to the authorized user.

Performance Evaluation:-Compare with the native system without self destructing data mechanism, throughput for uploading and downloading with the proposed sedas acceptably decreased by less than 72%, While latency for upload/download operations with sedas data mechanism increases by less than 60%.

VI. IMPLEMENTATION

The cloud environment which contain number of data. To provide more security to these data also protect the user data privacy from the leakages should implement sedas method in cloud. It can provide more security against the attacker through Shamir algorithm, which generate a pair of keys (2bytes) to the user to perform encryption also the user specify the lifetime of each keys using TTL property. TTL is a mechanism that limit the lifespan or lifetime of keys stored in cloud. Once the prescribed event occur or timespan has elapsed, keys can be self destructed without user intervention. This can improve performance of caching or to improve privacy from leakages.

VII. CONCLUSION

Each authenticated user, the Shamir algorithm generate a pair of keys also the user specify the lifetime of each keys. After user specified time the keys can be self destructed without user intervention. During the download process the Shamir algorithm check the validity of the keys. If the keys are expired, The Shamir algorithm generate new pair of keys to the user through this only the sedas system meet all the privacy preserving goals. The future work of the sedas system further to increase the key length to provide user data privacy in cloud infrastructure.

REFERENCES

[1] P.Carns, A.Choudhary, S.Ozisikyilmaz and S.W.Son "Enabling Acyive Storage on Parallel I/O Software Stacks" Mar.2010

[2] H.Chai, D.Feng, C.Li, w.Yingping and K.Zhou "24th IEEE Conf.Mass Storage System and Technologies(MSST), QOS Provisioning Framework for an OSD based Storage System" Jan 2011.

[3] D.Feng, Y.Kang, K.K.Muniswamy Reddy, Z.Tan and Y.Xie "Design and evaluation of oasis: An Active storage based on T10 OSD standard" Dec 2011

[4] Y.Kang, E.Miller and J.Yang "Object Based Storage Class Memories:An effient interface for SCM" in Proc.27th IEEE symp. Massive Storage System and Technology in April 2009.

[5] A.Shamir, ”How to Share a secret”, Commun.ACM, vol.22, no.11, pp.612-613”Dec 2010.

[6] R.Perlman,” File System design with assured delete,”in proc. Third IEEE Int. Security Storage Workshop(SISW), Dec 2009.

[7] S.W.Son, S.Lang, R.Ross, R.Thakur and B.Oziasikyilmaz and K.Liao, ”Enabling Active storage On Parallel System” Jan 2012.

[8] Y.Tang, P.P.C.Pee, J.C.Lui and R.Perlman, “FADE: Secure Overlay cloud storage with file assured deletion,” in proc.Secure Comm, Mar 2010.

[9] H.Chai, Z.Niu, W.Xiao and K.Zhou “Implementing and Evaluating Security in cluster storage system” Feb 2011.

[10] A.Devulapalli, T.Murugandi, D.Xu and P.Wyckoff, ”design of an Intelligent Storage Devices “April-2012.