International Journal of Latest Trends in Engineering and Technology
Special Issue NCRTCC 2017, pp.014-018
e-ISSN:2278-621X

AN INNOVATIVE PARALLEL CLOUD STORAGE USING PROXY RE-ENCRYPTION

M.Abinaya[1], C.Yogapriya[2], R.Bhuvaneswari[3], A.Ponmalar[4]

ABSTRACT -- We develop a secure cloud storage system that supports the function of secure data forwarding by using an AES and Proxy re encryption. In this model initial phase owner will upload the data (text, audio, video, images) with AES Encryption. In this step the plain text is encrypted and then the converted cipher text will be taken in the Next phase and the Proxy re encryption will be applied and then it is encoded (bit conversion) , inside of cloud again the data has divided into small pieces, for this process we will apply a dividing key. Data will place in different storage location. The information of data storage will monitor by a unique data distributors. If the valid user accessing the data and then if it matches with the already existing password then the data will be decoded and then decrypted. When the client asks for the data is retrieve in a reversible manner ,after that the corresponding uploaded data will be download. In this Data Robustness is maintained and the performance increases by replicating the data in a multiple server.

Keywords: AES ,Proxy Re- Encryption, multiple server, dividing key, data segregation

I. INTRODUCTION.

High-speed networks access become available to users for access anywhere at any time. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Cloud storage is a networked online storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large datacenters and people who require their resources to be host buy or lease storage capacity from them.
The data center operators, in the background, virtualizes the resources according to the customer requirement and expose as storage pools, which the customers themselves use to store files or data objects. Physically, the resource may span across multiple servers.

Data robustness is the main characteristics needed for storage systems. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. A decentralized erasure code is suitable for use in a distributed storage system.

II. BACK GROUND

[1] *Department of Information Technology, Sri Sai Ram Institute of Technology, Chennai – 600044, Tamilnadu, India.*
[2] *Department of Information Technology, Sri Sai Ram Institute of Technology, Chennai – 600044, Tamilnadu, India.*
[3] *Department of Information Technology, Sri Sai Ram Institute of Technology, Chennai – 600044, Tamilnadu, India.*
[4] *Department of Information Technology, Sri Sai Ram Institute of Technology, Chennai – 600044, Tamilnadu, India.*

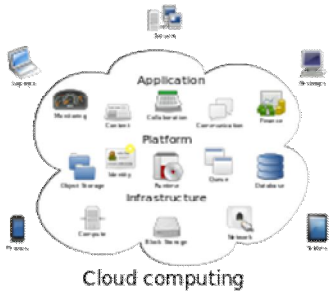


Fig 1:cloud computing architechture

Cloud computing is a Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. Cloud computing is a model for enabling ubiquitous and on-demand access to a shared pool of configurable computing resources (computer networks, storage, applications and services),which can be rapidly provisioned and released with minimal effort. Cloud computing and storage solutions provide users with various capability to store and process their data in either privately owned, or third-party data centers that may be located far from the users in distance from across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility over an electricity network.

III.RELATED WORK

This section is split into two sub-sections (III-A, III-B). Section III – A deals with the description of the proposed system and a brief description about its architecture. Section III – B deals with the modules in the system. The modules in the proposed system are registration, sharing data, secure cloud storage, proxy re-encryption, data retrieval.

III-A PROPOSED SYSTEM

In our proposed system we address the problem of forwarding data to another user by storage servers directly under the command of the data owner .The system model consists of distributed storage servers and key servers. Instead of storing cryptographic keys in a single device, a user distributes his cryptographic key to key servers that shall perform cryptographic functions on behalf of the user. These key servers are highly protected by security mechanisms.

Here Storage system has allocates by different data container. Once owner uploads the data with AES encryption mechanism, system again takes the data and makes Secure Data segregation process. All the data pieces will be save in different location in cloud storage. Here public distributor monitors all the data and corresponding positions where it is saved. When a proper client asking the data, cloud system will provide the data in reversible manner. So our system will prevent our data from both Inside and Outside attackers.

The architecture diagram for innovative parallel cloud storage using proxy re-encryption is shown in the fig.no.2.

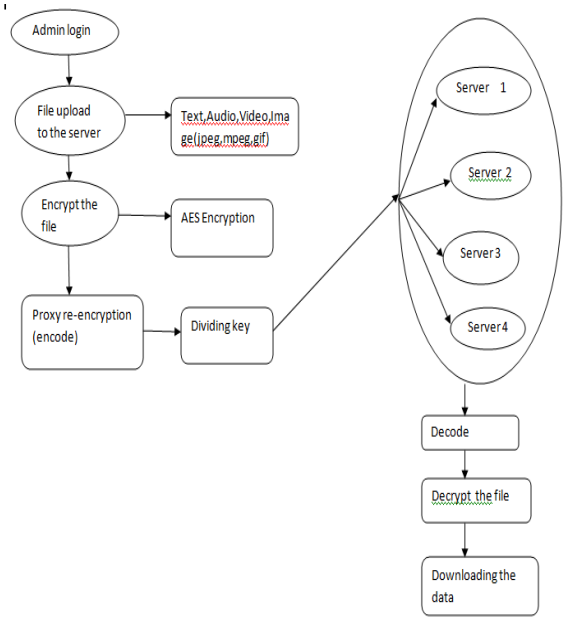
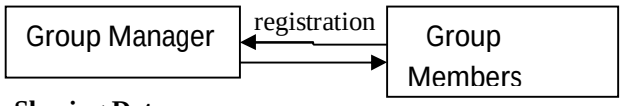


Fig 2:Architecture diagram

III-B. MODULES

Registration:

Initially user has to be registered with identity ID the group manager randomly selects a number and adds into the group user list which will be used in the traceability phase.After that user obtains a private key which will be used for group signature generation and file decryption.



Sharing Data:

The canonical application is data sharing. The public auditingproperty is especially useful when we expectthe delegation to be efficient and flexible. The schemes enable a content provider to share her data in a confidentialand selective way, with a fixed and small ciphertext expansion, by distributing to each authorized user a single and small aggregate key.

Secure Cloud Storage:

The major requirement for cloud storage is data robustness. There have been many proposals for storing the data over storage servers. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message.A decentralized erasure code is suitable for use in a distributed storage system.

Proxy re-encryption:

Proxy re-encryption schemes allow third parties (proxies) to alter a cipher text which has been encrypted for one user, so that it may decrypted by another user. By using proxy re-encryption technique the encrypted data (cipher text) isagain altered by the user in the cloud .The data which is stored in the cloud is highly secured .Then every user will have a public key and private key. Public key of every user is known to everyone but private key is known only to particular user.

Data retrieval:

Reports and data are the two primary forms of the retrieved data from servers. There are some overlaps between the reports and data. But queries generally select a relatively small portion of the server, while reports show larger amounts of data. Queries also present the data in a standard format and usually display

it on the monitor; whereas reports allow formatting of the output however you like and is normally retrieved

.

IV ALGORITHMS

This section is split into three sub-sections (IV-A, IV-B). Section IV – A deals with the description of the most commonly used AES Algorithm. Section IV – B(i&ii)deals with proxy re-encryption and erasure code technique.

IV-A AES Algorithm

- KeyExpansion—round keys are derived from the cipher key
- Initial Round
  - AddRoundKey—each byte of the state is combined with the round key using bitwise xor
- Rounds
  - SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
  - ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
  - MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  - AddRoundKey
- Final Round (no MixColumns)
  - SubBytes
  - ShiftRows
  - AddRoundKey

IV-B i) Proxy re-encryption

Proxy re-encryption converts a cipher text under one key into an encryption of the same message under another key .The main trust is to place little trust and reveal as little information to the proxy,it is necessary to perform its translations .At least the proxy should not be able to learn the key participants or the content of the messages it re-encrypts. In all prior schemes,it is easy for the proxy to determine which participants can perform the cipher texts .for example ,in a secured distributed file system ,content owners want to use the proxy to help re-encrypt sensitive information without revealing the recipients.

In this work, we propose a key-private (or anonymous) re-encryption keys as an additional useful property for PRE schemes .It means for a PRE scheme to be secure and key-private. Also ,we show that this property is not captured by prior definitions. And finally, we propose the first key-private PRE construction and prove its CPA-security under a simple extension of Decisional Bilinear DiffieHellman assumption and its key-privacy under the Decision Linear assumption in the standard model.

IV-B ii)Erasure code technique

In information theory,Erasure code is a forward error correction(FEC) code for the binary erasure channel,it transforms a message of k symbols into longer message with n symbols.such that the original message can be recovered from asubset of ‘n’ sysmbols.The fraction r=K/n is called code rate and in the fraction k’/k,where k’ denotes thenumber of symbols**.**

Optimal erasure codes

Optimal erasure codes have the property of n code word symbols are sufficient to recover the original message (i.e., they have optimal reception efficiency) and they are maximum distance separable codes (MDS codes).Here optimal codes are often costly (in terms of memory usage, CPU time, or both), when n is large. Except for very simple schemes, practical solutions usually have quadratic encoding and decoding complexity. In 2014, Lin et al. [1] gave an approach with $O(n \log n)$operations.

V.FUTURE WORK

As a response proxy re-encryption as an alternative to backup has evovled as a method of protecting against drive failure.Raid just does not cut it in the age of high-capacity HDDs. The larger a disk's capacity, the greater the chance of bit error.And when a disk crashes, the Raid rebuild process begins, during which there is no protection against a second (or third) mechanism failure. So not only has the risk of crashing during normal operation grown with capacity, it is much higher during Raid rebuild, too. Also, rebuild

times were once measured in minutes or hours, but disk transfer rates have not kept rapidity with the rate of disk capacity expansion, so large Raid rebuilds can now take days or even longer.

VI.CONCLUSION

Erasure codes are promising for improving the reliability of the storage system due to its space efficiency compared to the replication methods. Traditional erasure codes split data into equalized blocks and encode them in different data blocks. It brings heavy repairing traffic when clients read parts of the data, since most strips read for repairing is not in the predicted blocks. our paper proposes a discrete data dividing method to completely avoid this problem. The key idea is to encode strips from the same data block. We could see that the repairing failed blocks, the strips to be read are either in the same data block with corrupted strips or from the encoded strips. Therefore, no data is wasted. Experiments over a small-scale shows that the proposed discrete data divided method avoids downloading data blocks that are not needed for clients during the repairing operations

VII.LITERATURE SURVEY

1. QoS Support for End Users of I/O-intensive Applications
Using Shared Storage Systems.
Author: Xuechen Zhang ECE Department Wayne State Universities Trans. Kei Davison Alamos National Laboratory Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.
2.Repair Locality from a Combinatorial Perspective.
Author:Anyu Wang and Zhifang ZhangKey Laboratory of Mathematics Mechanization, IEEE Dec.2014.
3. On the Effective Parallel Programming of Multi-core Processors.
Author: Prof.dr.ir. H.J. Sips Technische Universities Delft, promotor Prof.dr.ir. A.J.C. van Gemund Technische Universities Delft Prof.dr.ir. H.E. Bal. 7 December 2010
4. Parallel Reed/Solomon Coding on Multicore Processors.
Author:Peter Sobs Institute of Computer Engineering University of LuebeckLuebeck, Germany. 2010 EEE DOI 10.1109/SNAPI.2010.16
5.Privacy-preserving and Secure Distributed Storage Codes
Author: Nihar B. Shah, K. V. Rashmi, Kennan Ramchandran, Fellow, IEEE, and P. Vijay Kumar, Fellow, IEEE. 2011.
6. Pattern-driven Parallel I/O Tuning cloud storage
Author:Babak Behzad, Surendra Byna,Prabhat Lawrence Berkeley National Laboratory.2011 IEEE.
7. PErasure: a Parallel Cauchy Reed-Solomon Coding Library for GPUs
Author: Xiaowen Chu, Chongjin Liu, Kai Ouyang, Ling Sing Yung, Hai Liu. Hong Kong .2010 IEEE.
8. Parallel Reed/Solomon Coding on Multicore Processors
Author: Peter SobeInstitute of Computer Engineering University of Luebeck, Germany.2011,IEEE.