Security in Multi Clouds

Alekya Vasa [#1], S.P Glory[#2]
#1Student, MCA, Dept. of Computers, Maris Stella College, Vijayawada, Krishna Dist.,
#2Assistant Professor, MCA, Dept. of Computers, Maris Stella College, Vijayawada, Krishna Dist.,

Abstract:. Sometimes, there could be a problem regarding service efficiency such as private cloud lacking the capacity or resource for security. Cloud computing can and does mean different things to different people. In order to solve such kind of temporary difficulties, ways to support HW resources (memory, server, and network) are necessary. The common characteristics most share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and dislocation of data from inside to outside the organization *in terms of low cost and accessibility of data*. For this reason, "multi clouds" are needed to cooperate between simple single clouds which provide accessible resources. In this paper, multi-clouds are proposed due to its ability to reduce security risks that affect the cloud computing user. If one cloud provider fails, we can still access our data live in other cloud providers. We replicate the data into different cloud providers in order to reduce service availability risk or loss of data.

I INTRODUCTION

The advantages of using cloud computing include: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter.

In addition to major cloud infrastructure providers, such as Amazon, Google, and Microsoft, more and more third-party cloud data service providers are emerging which are dedicated to offering more accessible and user friendly storage services to cloud customers. The many advantages of cloud computing are increasingly attracting individuals and organizations to move their data from local to remote cloud servers. It is a clear trend that cloud storage is becoming a pervasive service. Along with the widespread enthusiasm on cloud computing, however, concerns on data security with cloud storage are arising due to unreliability of the service.

Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds". Cloud providers should address privacy and security issues as a matter of high and urgent priority.

In this paper, multi-clouds are proposed due to its ability to reduce security risks that affect the cloud computing user. We replicate the data into different cloud providers in order to reduce service availability risk or loss of data. If one cloud provider fails, we can still access our data live in other cloud providers.

II REALTED WORK

The content keys are all encrypted with a master public key, which can only be decrypted by the master private key kept by the data owner. Ateniese et al proposed a secure distributed storage scheme based on proxy re-encryption. Specifically, the data owner encrypts blocks of content with symmetric content keys. The data owner uses his master private key and user's public key to generate proxy re-encryption keys, with which the semi-trusted server can then convert the ciphertext into that for a specific granted user and fulfill the task of access control enforcement. The main issue with this scheme is that collusion between a malicious server and any single malicious user would expose decryption keys of all the encrypted data and compromise data security of the system completely.

In addition, user access privilege is not protected from the proxy server. User secret key accountability is neither supported.

According to Armbrust et al. "Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. Wang *et al*. consider dynamic data storage in a distributed scenario, and the proposed challenge-response protocol can both determine the data correctness and locate possible errors. They only consider partial support for dynamic data operation.

Filho et al. proposed to verify data integrity using RSA-based hash to demonstrate uncheatable data possession in peer-topeer file sharing networks. However, their proposal requires exponentiation over the entire data file, which is clearly impractical for the server whenever the file is large.

The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds".

Shah *et al.,* proposed allowing a TPA to keep online storage honest by first encrypting the data then sending a number of precomputed symmetric-keyed hashes over the encrypted data to the auditor. However, their scheme only works for encrypted files and auditors must maintain long-term state. Schwarz *et al.,* proposed to ensure file integrity across multiple distributed servers, using erasure-coding and block-level file integrity checks. However, their scheme only considers static data files and does not explicitly studies the problem of data error localization.

III BACK GROUND

Cloud computing can be classified based on the services offered and deployment models. According to the different types of services offered, cloud computing can be considered to consist of three layers. IaaS or Infrastructure as a Service (*IaaS) is the lowest layer that* provides basic infrastructure support service. PaaS – the Platform as a Service (*PaaS)* layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. *Software as a Service (SaaS)* is the topmost layer which features a complete application offered as service on demand.Irrespective of the above mentioned service models, cloud services can be deployed in four ways depending upon the customers' requirements: public cloud, private cloud, community cloud, hybrid cloud.

IV DESIGN GOALS

• **Availability and Reliability:** By accessing any *k*-combination of *n* storage servers, the data user could successfully retrieve encoded data and recover all the original data. The data retrieval service remains functional when up to $n - k$ storage servers are corrupted in one round, and corrupted servers can be repaired from other healthy servers.

• **Security:** The designed storage service protects the data confidentiality and periodically checks the integrity of data in cloud servers to prevent data dropout or corruption.

• **Efficiency:** Above goals should be achieved with low storage, computation and communication cost for the data owner, data users and cloud servers.

V MULTI CLOUDS SYSTEM

. The multi Clouds algorithm exists in the client machines as a software library to communicate with each cloud. These single clouds are storage clouds, so there are no codes to be executed. The multi Clouds architecture consists of simple single clouds and each cloud uses its own particular

ISSN-2320-7884 (Online)
ISSN-2321-0257(Print)

interface The multi Clouds library permits reading and writing operations with the storage clouds. As the multi Clouds system deals with different cloud providers, the multi Clouds library deals with different cloud interface providers and consequently, the data format is accepted by each cloud.

The multi Clouds system model contains three parts: Service request protocol, SLA(Service Level Agreement, and another cloud storage providers. Cloud storage providers in the multi Clouds system model. The multi Clouds protocols require two communication round-trips to read or write the metadata and the data files that are part of the data unit, independently of the existence of faults and contention. The clouds are storage clouds without the capacity of executing users code, so they are accessed using their standard interface without modifications. The multi Clouds algorithms are implemented as a software library in the clients. This library offers an object store interface, similar to what is used by parallel file systems, allowing reads and writes in the back-end. The multi Clouds data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

To ensure the data reliability in multi cloud storage systems, various data redundancy techniques can be employed, such as replication, erasure codes, and network coding.

(1) Replication Technique:

Replication is the most straightforward way of adding data redundancy where each of *n* storage servers stores a complete copy of the original data as shown in Fig. 1. Data users can retrieve the original data by accessing any one of the storage servers, and the corrupted server can be repaired by simply copying the entire data from a healthy server.

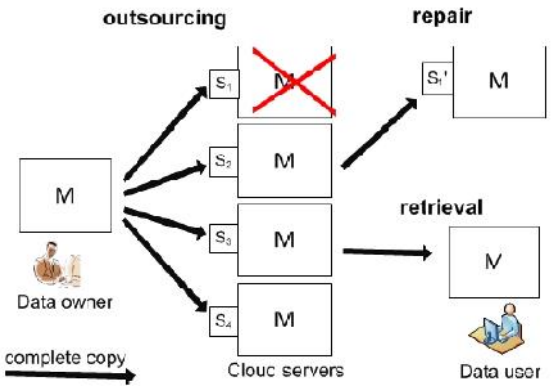

Fig 1: storage systems based on replication.

(2) Erasure-Code technique:

Data users can recover the entire *m* original packets by retrieving the same number of encoded packets from any *k*-combination of *n* servers, and therefore every server only needs to store *m/k* encoded packets which is regarded as the property of optimal redundancy-reliability tradeoff as shown in fig 2. Quadratic decoding is used by data users to recover data during data retrieval. Moreover, the communication cost to repair a failed storage server is equal to the size of the entire original data in the optimal erasure codes-based storage system.

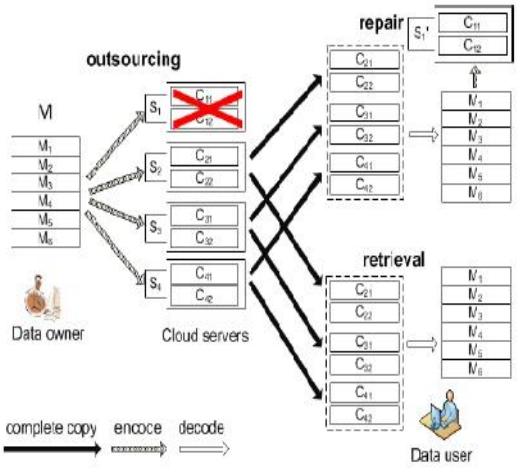

Fig 2: storage systems based on optimal erasure codes

(3) Network coding-based Technique:

Network coding-based Technique reduce the repair communication cost to the information theoretic minimum by combining encoded packets in the healthy servers during the repair procedure, where only *m/k* recoded packets are needed to generate the corrupted *m/k* encoded packets. Each server needs to store $2m/(k+1)$ encoded packets, which is more than optimal erasure codes, to guarantee that data users can retrieve *m* linearly independent encoded packets from any *k*-combination of *n* servers.

VI PERFORMANCE

The data owner raises a challenge for every encoded packet to cloud servers. Taking into consideration the large number of encoded packets with substantial data redundancy in cloud servers, the cost of such private integrity check is somehow burdensome in terms of both computation and communication for data owners. In this paper, we utilize the public integrity verification which enables the data owner to delegate the integrity check task to a third party server. Once there is a server failing to pass the integrity check, the third party server immediately reports it to the administrator of the cloud server who will then activate the repair process. The repair task is started and accomplished by generating the exactly same packets as those previously stored in corrupted storage servers. Such repair method does not introduce any additional linear dependence among newly generated packets and that packet stored in healthy storage servers, and therefore maintains the data availability.

VI CONCLUSION

Cloud computing is promising paradigm for delivering IT services as computing utilities. In this paper, multi-clouds are proposed due to its ability to reduce security risks that affect the cloud computing user. We replicate the data into different cloud providers in order to reduce service availability risk or loss of data. Clouds are designed to provide services to external users; providers need to be compensated for sharing their resources and capabilities. But, due to loss of service and data availability has caused many problems for a large number of customers recently. If one cloud provider fails, we can still access our data live in other cloud providers.

VII REFERENCES

[1] Michael Armbrust, Armando Fox, and et al. Above the clouds: A Berkeley view of cloud computing. Technical Report UCB-EECS-2009-28, University of California, Berkeley.

[2] Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik. Scalable and efficient provable data possession. In *Proceedings of the 4th international conference on Security and privacy in communication netowrks*, SecureComm '08, pages 9:1–9:10, New York, NY, USA, 2008. ACM.

[3] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou (2009), "Enabling public verifiability and data dynamics for storage security in cloud computing", in Proc. of ESORICS'09, Saint Malo.

[4] Wang, K. Ren, W. Lou (2010), "Achieving secure, scalable, and fine-grained access control in cloud computing", in Proc. of IEEE INFOCOM'10, San Diego, CA, USA.

[5] K. V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran. Exact regenerating codes for distributed storage. In *Proc. Allerton Conf. Control Comput. Commun.*, pages 337–350, 2009.