ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 9 September 2013 Page No. 2761-2764

OBLIGING EVINCIBLE DATA CHATTELS FOR VERIFICATION IN DISTRIBUTED CLOUD APPLICATION

B.Nagalakshmi, Mr. Ramakrishna
M.Tech 2nd Year
College of Engineering and Technology, Nandigama
Asst Professor
College of Engineering and Technology, Nandigama

Abstract— Obliging Evincible Data Chattels is a technique for ensuring the integrity of data in storage outsourcing. In this paper, we address the construction of an efficient Provable Data Possession scheme for distributed cloud storage to support the *scalability* of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the client's data. We present a *cooperative obliging Evincible Data Chattels* scheme based on homomorphic verifiable response and hash index hierarchy. We prove the security of our scheme based on multi-prover zero-knowledge proof system. Our paper show that introduces *scalability and communication overheads in comparison with non-cooperative approaches.*
Index Terms: multiple, cloud, services, data scalability, chattels.

1 INTRODUCTION

Now a day, cloud storage service has become a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients' data. Since cloud computing environment is constructed based on open architectures and inter- faces, it has the capability to incorporate multiple internal and/or external cloud services together to pro- vide high interoperability. We call such a distributed cloud environment as a *distributed -Cloud* (or *hybrid cloud*). *Cloud storage* is an industry term for managed data storage through hosted network (typically Internet-based) service. Several types of cloud storage systems have been developed supporting both personal and business uses.

The most basic form of cloud storage allows users to upload individual files or folders from their personal computers to a central Internet server. This allows users to make backup copies of files in case their originals are lost. Users can also download their files from the cloud to other devices, and sometimes also enable remote access to the files for other people to share. Hundreds of different providers offer online file hosting services. File transfers work over standard Internet protocols like HTTP and FTP. These services also vary in:

- storage capacity and network bandwidth quotas
- network transfer speeds supported
- price (some are free or ad-based, while others are based on data usage)
- software interface (some are browser-based while others utilize dedicated application clients)

This service work as an alternative to home network storage systems (such as *Network Attached Storage (NAS)* devices) or email archives.

Motivation:

To provide a *scalable*, low-cost, location independent platform for managing clients' data, current cloud storage systems adopt several new distributed file systems, for example, Apache Hadoop Distribution File System (HDFS), Google File System (GFS), Amazon S3 File System, Cloud Store etc. These file systems share some similar features: a single metadata server provides centralized management by a global namespace; files are split into blocks or chunks and stored on block servers; and the systems are comprised of interconnected clusters of block servers. Those features enable cloud service providers to store and process large amounts of data. However, it is crucial to offer an efficient verification on the integrity Enterprise Storage Businesses can utilize cloud storage systems as a commercially-supported remote backup solution. Either continuously or at regular intervals, software agents running inside the company network can securely transfer copies of files and database data to third-party cloud servers. Unlike personal data that is generally stored forever, enterprise data tends to quickly grow obsolete and backup systems include retention policies that purse useless data after time limits have passed. Larger companies can also use these systems to replicate large amounts of data between branch offices. Employees working at one site may create new files and have them automatically shared with colleagues in other sites (either locally or in other countries). Enterprise cloud

storage systems typically include configurable policies for "pushing" or caching data efficiently across sites.

Building Cloud Storage Systems

Cloud networks that serve many customers tend to be expensive to build due to the scalability requirements for reliably handling large amounts of data. The decreasing cost-per-gigabyte of physical digital media storage has helped offset these costs somewhat. Data transfer rates and server hosting costs from an Internet data center provider.

Cloud storage networks tend to be technically complex due to their distributed nature. Disks must be specially configured for error recovery, and multiple geographically-distributed servers must typically be managed to cope with the high bandwidth requirements. Network security configuration aspects also require the expertise of professional who command relatively high salaries.

Choosing a Cloud Storage Provider

While using a cloud storage system brings advantages, it also has downsides and involves risk. Selecting the right provider for your given situation is critical. Consider the following:

- ***Cost.*** Vendors charge fees for at least their more advanced service offerings. Service plans may be divided into tiers according to usage, with penalty fees charged if you exceed the specified quotas. So-called "free" services can place serious restrictions (quotas) on the amount of data which can be stored in or accessed from the cloud. Carefully consider your storage needs before locking into a subscription: Buy enough capacity and capability to support you and your organization, and try to avoid long-term contracts that can cause serious issues later when your needs grow.

- ***Usability***. Cloud storage systems should make working with remote data almost as easy as data on your local hard drives. Test out carefully both the user interface (browser or separate application screens) and responsiveness of a vendor's system looking for major time-wasting usability limitations that sap your productivity.

- ***Reliability and Reputation***. Even a free cloud storage service can be costly if it suffers from frequent downtimes, loses or corrupts data, or has had past security incidents. Research the service providers you are interested in for reputation and their brand quality before committing to one. Consider also using a vendor's trial subscription before committing to a long-term investment with them (and do not load any particularly sensitive data onto a service during trial periods).

Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. Such composition expands deployment options for cloud services, allowing IT organizations to use public cloud computing resources to meet temporary needs. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds.

Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization only pays for extra compute resources when they are needed.

Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands.

By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure.

Hybrid clouds lack the flexibility, security and certainty of in-house applications Hybrid cloud provides the flexibility of in house applications with the fault tolerance and scalability of cloud based services.

2. RELATED WORKS:

Distributed cloud

Cloud computing can also be provided by a distributed set of machines that are running at different locations, while still connected to a single network or hub service.

Cloud management strategies

Public clouds are managed by public cloud service providers, which include the public cloud environment's servers, storage, and networking and data center operations. Users of public cloud services can generally select from three basic categories:

- **User self-provisioning:** Customers purchase cloud services directly from the provider, typically through a web form or console interface. The customer pays on a per-transaction basis.
- **Advance provisioning:** Customers contract in advance a predetermined amount of resources, which are prepared in advance of service. The customer pays a flat fee or a monthly fee.
- **Dynamic provisioning:** The provider allocates resources when the customer needs them, then decommissions them when they are no longer needed. The customer is charged on a pay-per-use basis.

Managing a private cloud requires software tools to help create a virtualized pool of compute resources, provide a self-service portal for end users and handle security, resource allocation, tracking and billing. Management tools for private clouds tend to be service driven, as opposed to resource driven, because cloud environments are typically highly virtualized and organized in terms of portable workloads.

In hybrid cloud environments, compute, network and storage resources must be managed across multiple domains, so a good management strategy should start by defining what needs to be managed, and where and how to do it. Policies to help govern these domains should include configuration and installation of images, access control, and budgeting and reporting.

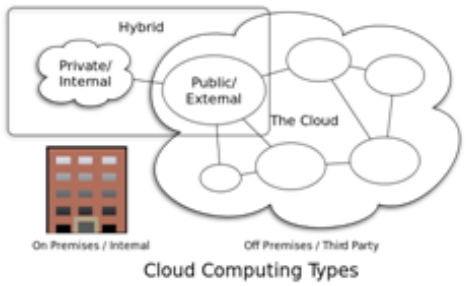
3 ANALYSIS

we present our verification framework for multi-cloud storage and a formal definition of CPDP. We introduce two fundamental

techniques for constructing our CPDP scheme: hash index hierarchy (HIH) on which the responses of the clients' challenges computed from multiple CSPs can be combined into a single response as the final result; and homomorphic verifiable response (HVR) which supports distributed cloud storage in a multi-cloud storage and implements an efficient construction of collision resistant hash function, which can be viewed as a random oracle model in the verification protocol.

3.1 Analysis:

Cloud computing enables highly scalable services to be easily consumed over the Internet on an as needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. In this paper, the authors address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which they consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. Offering strong data protection to cloud users while enabling rich applications is a challenging task.



Cloud Computing Types

Cloud computing provides dynamically scalable and virtualized resources as a service over the network at a nominal initial investment. Data-center works as backbone in cloud computing there a large number of servers are networked to host computing & storage needs of the users. We study and seek to improve the confidentiality of application data stored on third-party computing clouds. Scalable database services allow data query only by primary key rather than supporting secondary-key or join queries. We propose to identify and encrypt all functionally encrypt able data, sensitive data that can be encrypted without limiting the functionality of the application on the cloud. Many data intensive applications produce enormous amounts of data which travel on cloud network. As the cloud users grow, cloud architecture should accommodate movement of voluminous data to avoid data congestion in the network. Many other applications such as payment and online auction services cannot afford any data inconsistency. Cloud computing model provides benefits for private enterprise environments where a significant physical infrastructure already exists. Private cloud management platforms have been emerging in the last several years providing new opportunities for efficient management of internal infrastructures leading to high utilization.

In order to prove the integrity of data stored in a multi-cloud environment, we define a framework for CPDP based on interactive proof system (IPS) and multi-prover zero-knowledge proof system (MPZKPS), as follows:

Definition: (Cooperative-PDP): A cooperative provable data possession $\mathcal{S} = (KeyGen, T\ agGen, P\ roof)$ is a collection of two algorithms $(KeyGen, T\ agGen)$ and an interactive proof system $P\ roof$, as follows:

***KeyGen*(1κ):** takes a security parameter κ as input, and returns a secret key sk or a public-secret key pair(pk, sk);

***TagGen*(sk, F,$\mathcal{P}$):** takes as inputs a secret key sk, a file F, and a set of cloud storage providers $\mathcal{P} = \{Pk\}$, and returns the triples (ζ, ψ, σ), where ζ is the secret in tags, $\psi = (u,\mathcal{H})$ is a set of verification parameters u and an index hierarchy $\mathcal{H}$ for F, $\sigma = \{\sigma(k)\}Pk\in\mathcal{P}$ denotes a set of all tags, $\sigma(k)$is the tag of the fraction $F(k)$of F in Pk;

4 TECHNIQUES

The database (running on the cloud) is encrypted, but keys are not revealed to the cloud. The keys are stored by the organization that "outsources" its application and user data to the cloud. To fetch data from the cloud, the user first contacts the organization to get the appropriate key(s), and then sends the query to the cloud to fetch the data. The large number of service requests to fulfill the demands of millions of users will broaden the latency problem. Cloud service provider physically may be far away from the clients, compelling data to travel from several mediums and network equipments, there by imposing a time delay in getting Cloud services. Each transaction contains one or more sub-transactions, which operate on a single data, item each. The application must provide the primary keys of all accessed data items when it issues a transaction. The application model which is used to estimate the performance metrics of all the transactions in a multi -tiers cloud application. In our study, we use layered queuing model rather than regular network model proposed in previous research. In the proposed Cloud architecture data-centers work in master-slave paradigm. Nearest data-centers form a computing zone and users may opt for treating their instances in multiple zones.

The main entities involved in proposed architecture are:

1) Master /Slave Data-Center: Master data center is located at Cloud provider's administrative premises. User's accounting on pay-as-you-go basis is completed here. Slave data-center are geographically scattered to serve user's requests in minimum physical distance.

2) Users/ Brokers: Users directly communicate or via brokers submit requests which automatically reach at master data-center. Master data-center creates user instance at appropriate slave data-center considering minimum latency

3) Service Level Agreements (SLAs): Quality of Service and pricing negotiations are settled through SLAs. Master data-center scans SLA each time to host needs of the users.

5 CONCLUSIONS

Cloud computing is still in its infancy and needs exploration towards the efficient utilization of large scale IT infrastructure. Deploying and managing cloud effectively when good performance is required is hard when the cloud administrator does not have full control over the underlying hardware components. The cloud management platform provides centralized point for managing hosts with enabled virtualization. Many Web applications need strong data consistency for their correct execution. However, although the high scalability and availability properties of the cloud make it a good platform to host Web content, scalable cloud database services only provide relatively weak consistency properties. Data confidentiality is one of the key concerns that prevent organizations from widely adopting third-party computing clouds. Encrypted data on the cloud prevents privacy leakage to compromised or malicious clouds, while users can easily access data by decrypting data locally with keys from a trusted organization.

FUTURE WORK

- Moving IT to cloud works when maintaining the status quo – example your network is up and running and requires minimal changes.
- But when you do need changes, you may have lost your "expert" in helping you make decisions on your requirements because you outsourced the job.
- The customer and the service provider must have service-level agreements (SLAs) in place to decide what to do when things change, otherwise you end up spending even more money when the whole point of moving to the cloud was to cut costs.
- The customer should employ an expert-level consultant who understands the customer's needs and the technology required to achieve its goals.
- Cloud is that service providers may not offer expert consultancy to a customer. Customers will need a consultant to bridge the gap and make sure the right specification of products and services are available at the right time.
- Recovering from a failure only causes a temporary drop in throughput and a few aborted transactions. Recovering from a network partition, however, may possibly cause temporary unavailability of Cloud, as we explicitly choose to maintain strong consistency over high availability.

ACKNOWLEDGEMENT

The authors would like thank to our management of Professor RamaReddy College of Engineering and Technology, Nandigama. Director Dr. P Mohan Reddy, Principal Dr KeshavaReddy, and all colleagues for their precious Collaboration for providing facilities and system implementation.

REFERENCES

1. GoogleAppEngine: http://code.google.com/appengine/.
2. Amazon Web Service: http://aws.amazon.com/.
3. Eucalyptus: http://www.eucalyptus.com/.
4. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S.Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds".
5. K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds.
6. Y. Dodis, S. P. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed.