

REVIEW OF SECURITY AND PRIVACY ISSUES IN CLOUD STORAGE SYSTEM

SAHIL DALWAL & PANKAJ VAIDYA

Department of Computer Science Engineering, Shoolini University, Himachal Pradesh, India

ABSTRACT

The objective of this paper is to know about the Cloud storage for cloud computing, and its security and privacy issues and the some cloud interfaces or future scope in our society. The various issues related to data security, privacy and availability with storing data on third party service providers, more commonly termed as cloud service. There is a lot of research being done to point out issues with these service providers and cloud security. In general in this paper I have look at the various current researches being done to solve these issues, the current trends in securing, ensuring privacy and availability of these data on cloud storage services.

KEYWORDS: Cloud Computing, Cloud Storage, Cloud Data Management Interface, Security, Privacy

INTRODUCTION

Cloud computing has become a very emerged and integrated field in today's society as we all are using communication technology and networking in any way, whether it is our mobile phones, cctv camera or internet. Cloud Computing is a technique which involves the use of computing resources. Internet has widely changed the computing world. Starting from parallel computing to distributed computing and then to grid computing and finally to Cloud Computing. Cloud Computing originated from telecommunications company which began to offer VPN (Virtual Private Network) using point to point data circuits.

Cloud computing is a computing model in which virtualized resources are provided as a service over the internet. The concept introduced the infrastructure as a service (**IaaS**), platform as a service (**PaaS**), software as a service (**SaaS**). Cloud computing services usually provide common business applications online that are accessed from a web browser.

Cloud computing has brought up major advancement to IT industry. In spite of all the advantages delivered by cloud computing, several challenges are hindering. On top of the list is the security and privacy concerns arising from the storage and processing of sensitive data on remote machines that are not owned, or even managed by the customers themselves. Cloud computing providing major benefits to organizations from a cost, flexibility, and scalability perspective etc. these are some advantages that cloud computing is providing.

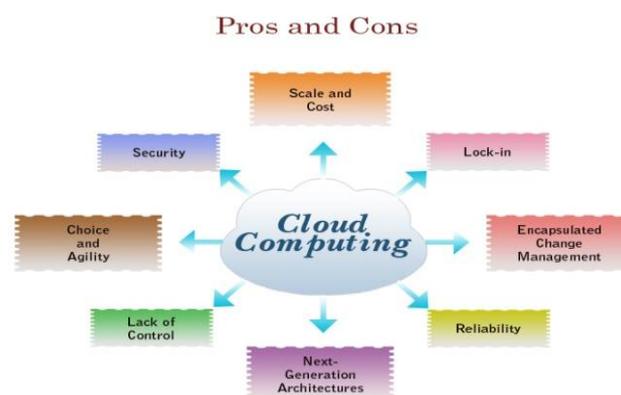


Figure 1

The rest of the paper is organized as follows: in section 2. I have present the cloud storage for cloud computing. In section 3. Discusses the security and privacy of cloud data storage. In section 4. I have considered the cloud data management interface for ensuring the storage and accessibility of customer data. In section 5. I continue with a discussion on a data storage security. Conclusion and future scope are presented in section 6.

CLOUD STORAGE

Cloud storage has rapidly grown in popularity over the past few years. The first form of web-based data storage is called cloud storage. This is a form of networked data storage where data files are stored on multiple virtual servers. Just like Cloud Computing, Cloud Storage has also been increasing in popularity recently due to many of the same reasons as Cloud Computing. Cloud Storage delivers virtualized storage on demand, over a network based on a request for a given quality of service (QoS). There is no need to purchase storage or in some cases even provision it before storing data.

We just only pay for the amount of storage our data is actually consuming. The servers used for cloud storage are typically hosted by third-party companies who operate large data centers. The best-known cloud storage service today is probably Amazon.com's Simple Storage Service (S3). Cloud storage is also offers by many other companies, with services either planned or rumored from IBM, Google, and EMC.

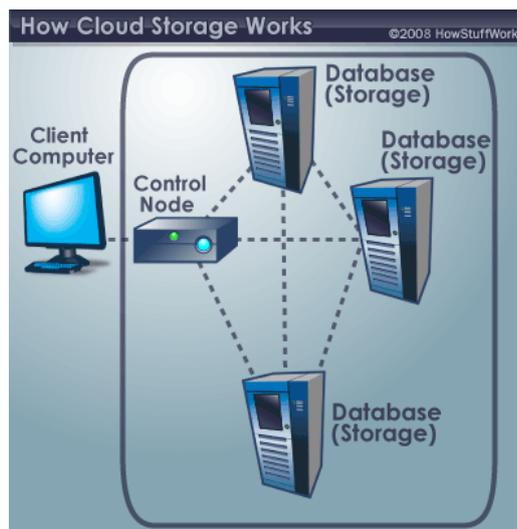


Figure 2

The above figure shows how the cloud storage works. It does nothing it just store the clients data into the data base and then clients data is stored on different different servers. This processing basically called as virtualization. The cloud storage is also known as distributed computing because of the virtualization.

Why is cloud storage such a big deal—especially to large companies? There are three primary benefits to cloud storage:

Scalability: When we rent cloud storage space, we can use as much or as little space as we need. It's easy to “flip and switch” and increase our storage space if we suddenly have larger storage needs. We don't have to buy the additional computers required to manage the extra data, but rather can use more of the space available in the cloud

Reliability: If someone've ever had their company's server go down, they know how important it is to have access to backup data. Cloud storage can be used as giant online backup drive. Even if we rely on cloud services for our primary data storage, we still have the peace of mind that comes from knowing our data is duplicated on multiple servers.

Lower Costs: How much do we pay per terabyte of storage? Even with hard disk prices coming down.

It's still cheaper to use the virtual servers in the cloud. Cloud storage services offers lower storage rates because they more efficiently use the server space they have; space gets reassigned to users almost instantly, on an as-needed basis. It's a lot cheaper to use excess space in the cloud than it is to purchase a new server or hard disk drive.

As cloud storage provide some benefits it also has some issue like integrity of data, reliability, security and user error or access ability. It's hard to trust the cloud services completely. Because it's not necessary that our data will always be save in the cloud data base. Whether we use are data after few months. There must be some technical problems like if the internet goes offline etc.

Data Availability: As the system ensures the availability of data by returning the read value if there is any reachable and correct node. Additionally it also ensures that if a version of the object is available in any of the correct nodes before the object is removed by the garbage collector then the value of the object is returned by the read ensuring durability of the read operation.

Data Integrity: The data objects should never be updated by unauthorized clients and in order to achieve this limitation the system ensures that only correct and authorized client are able to perform the updates. Each of the volume is configured at start to be associated with a particular range of keys to particular public keys of nodes, so effectively only a subset of the client's object collection can be updated by any particular node.

SECURITY AND PRIVACY ISSUES

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. There are various types of issues that a cloud storage user both at enterprise level and as an individual consumer might face during the use of the service. Most of the issues are with integrity of the data, ensuring that the data is confidential and available when it is needed.

Let us look at these facts in a more detailed manner. This is not an exhaustive list but certainly covers some of the more significant issues.

Trusting Data Stored in the Cloud

Data when stored in the cloud needs to be not only be confidential but also should be correct every time it retrieved after uploaded or after a modification, there should not be a loss of integrity of the data. This is a valid scenario when third party storage services are compromised by the malicious agents, the data that is being provided by the corrupted service might not be correct or fresh. This can be sometimes very hard to detect and hence certain amount of errors lies on the service user to trust the provider that what he provides is correct. inside the boundary of integrity check guidelines that have been agreed upon between the service provider and the user, but which might be not be correct when the service provider's infrastructure has been compromised or encountered an error. To an extent this problem is due to the fact that service providers may sacrifice trust for providing high data availability.

Lack of Provable Security in Cloud Service Provider Agreements

As we move towards the use of the cloud storage service it will become more of a commodity business, security would be needed and be necessary to differentiate service providers and systems. In the industry since most of the cloud service providers today provide service level agreements with emphasis on high data availability with little guarantee on

the security of the data. Due to internal errors or sometimes malicious changes to their system the data might be exposed or provided to the users of the system with the integrity being compromised.

Data History

One of the significant features we can enjoy with local data storage is the presence of metadata features which allow us to view the history of a data object. This allows the systems to provide data integrity checks and rollback capabilities when a corruption or compromise is detected in the system. These features are almost non prevalent in the present cloud system and if present there are substantial security vulnerabilities associated with it because of the scale of the service. This feature which has become the fact for ordinary storage system on local systems and provided by most of the data storage systems needs to be implemented in the cloud service context effectively considering the scale of the system.

Provable Data Possession

This issue is loosely related to one of the other issues I looked into on how to trust the data stored on the service provider. When a data is retrieved from the service provider on performing an integrity check, it would be very hard to determine how the data was stored in the service providers system. This is to ensure that the data is not leaked to a third party to whom the service provider is outsourcing the data, when the agreement for service is being agreed upon by the service provider and customer. The present service providers provide hardly any sort of security on where and how the data is being stored and how secure the systems are the claims by the service provider.

Use of Cloud Storage Service as an Online Slack Space

The cloud service providers have various business objectives when providing the service based upon these the product might be designed. If one of these priorities is to provide quick syncing capabilities, then some sort of system design must be provided so as to not sync data that is already present in the cloud storage even if it belongs to a different user. This leads to a situation where in the link between data and user might not be direct, this would allow user to modify the system to use storage space anonymously without provable data ownership. This could lead to various legal issues if this service is used to provide illegal services.

CLOUD DATA MANAGEMENT INTERFACE

The Cloud Data Management Interface--better known as CDMI--is a SNIA standard that specifies a protocol for self-provisioning, administering and accessing cloud storage.

CDMI defines HTTP operations for assessing the capabilities of the cloud storage system, allocating and accessing containers and objects, managing users and groups, implementing access control, attaching metadata, making arbitrary queries, using persistent queues, specifying retention intervals and holds for compliance purposes, using a logging facility, billing, moving data between cloud systems, and exporting data via other protocols such as NFS.

The Cloud Data Management Interface defines the functional interface that applications will use to create, retrieve, update and delete data elements from the Cloud. As part of this interface the client will be able to discover the capabilities of the cloud storage offering and use this interface to manage containers and the data that is placed in them. In addition, metadata can be set on containers and their contained data elements through this interface. This interface is also used by administrative and management applications to manage containers, accounts, security access and monitoring/billing information, even for storage that is accessible by other protocols. The capabilities of the underlying storage and data services are exposed so that clients can understand the offering.

CDMI v1.0

- SNIA Technical Position: Cloud Data Management Interface (CDMI) v1.0
- CDMI is applicable for three types of cloud storage such as :
- Cloud storage for cloud computing.
- Public storage cloud.
- Private cloud storage

CDMI v1.0.1

- SNIA Technical Position: Cloud Data Management Interface (CDMI) v1.0.1
- CDMI v1.0.1 Errata (changes since v1.0)

CDMI v1.0.2

- SNIA Technical Position: Cloud Data Management Interface (CDMI) v1.0.2
- CDMI v1.0.2 Errata (changes since v1.0.1)
- ISO/IEC 17826:2012 Information technology -- Cloud Data Management Interface (CDMI)

CONCLUSIONS

Cloud computing technology has prove to be a great asset to human society. As the demand of cloud computing increases these days. The importance of cloud storage is also increases. And the cloud storage will also give the great assets to our human society. Its scope is increasing as the globe is connected with internet and many other types of network which are increasing its web in every corner of the society. And it increases the value of database storage over the network. Including this it generate the questioning about the security of the data in the cloud storage system.

FUTURE SCOPE

As per some surveys conducted by several leading organizations, 70% of Americans will be getting benefited from cloud and it various applications in next decades for official and personal use. And this is not an overestimate or exaggeration, as we are already using cloud and its applications in one form or another. Using email and connecting to social media through smart phones, watching movies over smart phones and uploading and accessing pictures from websites like Flickr are common examples of cloud computing in our day-to-day life.

Let us have a look on what makes the future of cloud computing so bright.

- Presence of Internet will boost its future.
- No more software updates.
- Hardware optional.
- Entertainment unlimited.
- Medical treatments simplified and many more.

REFERENCES

1. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, Dept. Of ECE, Illinois Inst. of Technology, Ensuring data storage security in cloud computing, 17th International Workshop on Quality of Service, 2009.
2. Survey Paper on Security & Privacy Issues in Cloud Storage Systems, Anup Mathew The Institute for Computing, Information and Cognitive Systems (ICICS), University of British Columbia Vancouver, BC V6T 1Z4 Canada.
3. Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online.
4. Cloud Storage for Cloud Computing the Storage Networking Industry Association and the Open Grid forum.
5. http://en.wikipedia.org/wiki/Cloud_Data_Management_Interface.
6. http://www.snia.org/tech_activities/standards/curr_standards/cdmi.
7. http://www.dmtf.org/sites/default/files/cloud_storage_presentation.pdf.
8. <http://www.roseindia.net/cloudcomputing/future-cloud-computing.shtml>