International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 16-17, 2013

Security for Effective Data Storage in Multi Clouds

T.NEETHA
Kommuri Pratap Reddy Institute of Technology
Hyderabad, India

CH.SUSHMA
Kommuri Pratap Reddy Institute of Technology
Hyderabad, India

ABSTRACT: Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multicloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

KeyWords: Cloud Computing, Behaviour Trust, Data integrity, Evaluation Strategy.

1. Introduction:

Currently, the cloud computing is welcome in scholars and enterprise, because of its good features such as low Investment, easy maintenance, flexibility and fast deployment, reliable service. At the same time, cloud computing can also reduce operating costs, improve operational efficiency. So many countries put the financial and material for the cloud computing.

Software as a service (SaaS): In this model, software applications are offered as services on the Internet rather than as software packages to be purchased by individual customers. One of the pioneering providers in this category is Salesforce.com offering its CRM application as a service. Other examples include Google web-based office applications.

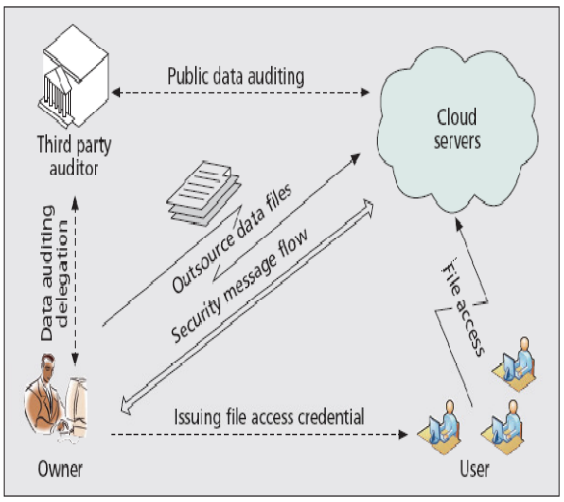
Infrastructure as a service (IaaS): Hardware resources (such as storage) and computing power (CPU and memory) are offered as services to customers. This enables businesses to rent these resources rather than spending money to buy dedicated servers and networking equipment.. As examples in this category, Amazon1 offers S3 for storage, EC2 for computing power, and SQS for network communication for small businesses and individual consumers.

Database as a service (DaaS): A more specialized type of storage is offering database capability as a service. Examples of service providers are Amazon SimpleDB, Google BigTable3, Force.com database platform and Microsoft SSDS4. DaaS on the cloud often adopts a multi-tenant architecture, where the data of many users is kept in the same physical table.

Platform as a service (PaaS): This refers to providing facilities to support the entire application development lifecycle including design, implementation, debugging, testing, deployment, operation and support of rich Web applications and services on the Internet. Most often Internet browsers are used as the development environment. Examples of platforms in this category are Microsoft Azure Services platform6, Google App Engine7, Salesforce.com Internet Application Development platform8 and Bungee Connect platform9. PaaS enables SaaS users to develop add-ons, and also develop standalone Web based applications, reuse other services and develop collaboratively in a team.

2. Ensuring Cloud Data Storage

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. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can always be the first step to fast recover the storage errors and/or identifying potential threats of external attacks.



The architecture of cloud data storage service.

To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that is needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function , chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure-coded server failures. Lightweight: to enable users to perform storage correctness checks with minimum overhead data .Subsequently, it is shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. The procedure for file retrieval and error recovery based on erasure correcting code is also outlined. Finally, we describe how to extend our scheme to third party auditing with only slight modification of the main design.

3. SECURITY:

Data Integrity

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers. One of the solutions that they propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al. State that this solution can avoid data corruption caused by some components in the cloud. However, Cachinetal.Claim that using the Byzantine faulttolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place.

Service Availability

Another major concern in cloud services is service availability. Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers . Both Google Mail and Hotmail experienced service downtime recently . If a delay affects payments from users for cloud storage, the users may not be able to access their data. Due to a system administrator error, 45% of stored client data was lost in LinkUp (MediaMax) as a cloud storage provider .

Data Intrusion

According to Garfinkel, another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

4. Future Work:

For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. Regarding service availability risk or loss of data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud provider fails, we can still access our data live in other cloud providers. This fact has been discovered from this survey and we will explore dealing with different cloud provider interfaces and the network traffic between cloud providers.

5. Conclusion

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multiclouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

6. References

[1] H. Shacham, B. Waters (Dec 2008), "Compact proofs of retrievability", in Proc. of Asiacrypt 2008, vol. 5350, pp. 90–107

[2] M.A.Shah, R.Swaminathan, M. Baker (2008), "Privacy preserving audit and extraction of digital contents", Cryptology ePrint Archive.

[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] [Online] Available : Amazon.com, "Amazon s3 availability event: (2008)," Online at http://status.aws.amazon.com/ s3- 20080720.html.

[6] Cloud Security Alliance, (2009) "Security guidance for critical areas of focus in cloud computing," 9, [Online]