ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Distributed Storage and Integrity Auditing Mechanism for Secure Cloud Storage

G.Mahinder[1], S.Srinivas Kumar[2], G.Sudhakar[3]

(M.Tech) Department of Computer Science and Engineering, Aurora's Scientific Technological and Research Academy, Hyderabad, India[1]

Senior Assistant Professor, Aurora's Scientific Technological, and Research Academy, Hyderabad, India[2]

Academic Assistant-Lecturer, Department of SIT, Jawaharlal Nehru Technology University, Hyderabad, India[3]

Abstract: 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. Several trends are opening up the era of Cloud Computing that is mainly focusing on internet usage and storage, use of computer technology. Moving data into the cloud offers great convenience for users to remotely store their data and enjoy the on-demand high quality cloud applications without the obligation of local hardware and software management. As the benefits are well-defined, such a service is also relinquishing users physical possession of outsourced data, which certainly posses new security risks toward the correctness of the data in cloud and to increase the profit margin by reducing cost, it is possible for cloud service provider to discard rarely accessed data without being detected in a timely fashion and even attempt to hide data loss incidents so as to maintain a reputation. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper flexible distributed storage integrity auditing mechanism with effective service level agreement, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage and this auditing result not only ensures storing cloud storage correctness guarantee, but also concurrently achieves immediate data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature the proposed design supports secure and efficient dynamic data operations on outsourced data .

Index Terms: Auditing Mechanism, Data Integrity, Distributed Storage, Error Verification, Dynamic Data Operations And Service Level Agreements.

1. INTRODUCTION

MANY trends are opening up the era of cloud computing, which is an Internet-based development and use of computer technology. The powerful processors, together with the Software as a Service (SaaS) computing architecture, that are transmitting, data storage into pools of computing service on huge scale. Shifting data into the cloud offers great convinces to users since they don't have to worry about the complexities of direct hardware and software management. The pioneer of cloud computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Cloud (EC2) are both well-known examples.

The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.While these internet-based online services do provide huge amount of storage space and customizable computing resources, the shift to cloud storage is eliminating responsibility of local machines for data maintenance at the same time. On the one hand, although the cloud infrastructures are much more powerful and reliable than personal computing devices, certain extent internal and external threats for data integrity occurs.

For example, to increase the profit margin CSP may delete frequently accessed data without being detected in a timely fashion . Similarly, CSP may even attempt to hide data loss incidents so as to maintain a reputation. Therefore, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale storage of data integrity and availability may impede its wide adoption by both enterprise and individual cloud users.

In order to achieve the assurances of cloud data integrity and availability and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to design. The user did not have physical possession of data in the cloud prohibits the direct

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

adoption of traditional cryptographic primitives for the purpose of data integrity protection. Hence, the verification of cloud storage correctness must be conducted without explicit knowledge of the whole data files . Meanwhile, cloud storage is not just a third party data warehouse. The data stored need not be accessed but also be frequently updated by the users , including some of the operations like insert , delete ,update , append Thus, it is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance, which brings a challenging design for the system . Last but not the least, the deployment of cloud computing is powered by data centers running in a simultaneous, cooperated, and distributed manner.

It is more advantages for individual users to store their data redundantly across multiple physical servers so as to reduce the data integrity and availability threats. Thus the protocols that are distributed for correctness assurance will be of most importance in achieving robust and secure cloud storage systems.

2. SYSTEM MODEL

Representative network architecture for cloud storage service architecture is illustrated in

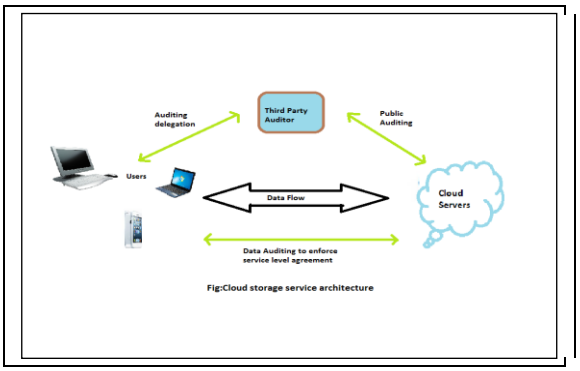


FIG: CLOUD STORAGE SERVICE ARCHITECTURE

The following entities can be described as follows:

User: An users and different organizations has data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise or individual customers.

Cloud Server (CS): an entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources.

Third-Party Auditor: an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

Service Level Aggrements:SLA's include service guarantee, service guarantee time period, service guarantee granularity, service guarantee exclusion, service violation measurement and reporting, service credit.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in simultaneous, cooperated, and distributed manner. Data redundancy can be employed with a technique of erasure correcting code to further tolerate faults or server crash as user's data grow in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert, and append. Note that in this paper, we put more focus on the support of file-oriented cloud applications other than non file application data, such as social networking data. In other words, the cloud data we are considering is not expected to be rapidly changing in a relative short period.

As users no longer possess their data locally, it is of critical importance to ensure users that their data are being correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance (to enforce cloud storage service-level agreement) of their stored data even without the existence of local copies. In case that user do not necessarily have the time, feasibility or resources to monitor their data online, they can delegate the data auditing tasks to an optional trusted TPA of their respective choices. However, to securely introduce such a TPA, any possible leakage of user's outsourced data toward TPA through the auditing protocol should be prohibited.

In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

3. CLOUD DATA STORAGE SYSTEM

Individual users and different organizations stores their data in the cloud and no longer possess the data locally in cloud data storage system Thus, we need to entrust the correctness an availability of the data files being stored on the distributed cloud servers. One of the important issues is to effectively detect any unauthorized data modifications and corruption, possibly due to server compromise are detected successfully, to find which server the data error lies in is also of important issue, as it is always be the initial step immediate recover of external attacks and/or storage errors.

In order to focus these problems, our main scheme for ensuring cloud data storage system is presented. The first part of the section is devoted to a review of basic tools from file distribution across cloud servers.Then,the homomorphic token is introduced. The

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

token computation function we are considering belongs to a universal hash function, chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure code data. Here it is shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying the systematical procure for file retrieval and error recovery bas on erasure-correcting code. At last we need to describe how to extend our scheme to third party auditing.

4. GOALS TO ACHIEVE

We aim to achieve efficient mechanism to perform Auditing process with significant service level agreements; we need to achieve the following metrics:

1) Storage correctness assurance and imposing service level agreements if misusing the rules tie up with the users and organizations.
2) Data to be kept intact all the time in the cloud.
3) Locating the malfunctioning servers when a data corruption has been detected.
4) Minimizing the effects brought by server failures.
5) Maintaining the same level of storage correctness, when Auditing process is done.

5. DISTRIBUTION OF FILE AND CHALLENGE TOKEN PRECOMPUTATION

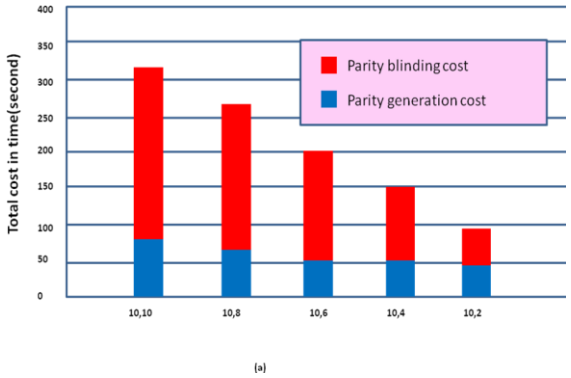
Here we perform storage correctness verification and Error localization. We also adhere the file retrieval and error recovery.It also supports dynamic data operations. Erasure-Correcting code is well know, that may be used to tolerate multiple failures in distributed storage systems.
In cloud data storage, we rely on this technique to disperse the data file frequently across a set of n=m+k distributed servers. An(m,k) Reed-Solomon erasure-correcting cod is used to create k redundancy parity vectors m data vectors can be reconstructed from any m out of the m+k vectors on a different server, the original data file can survive the failure of any k of the m+k servers without any data loss, with a space overhead of k/m. To support efficient sequential I/O to original file, our file layout is systematic, i.e., the Unmodified m data file vectors together with k parity vectors is distributed across m=k different servers.

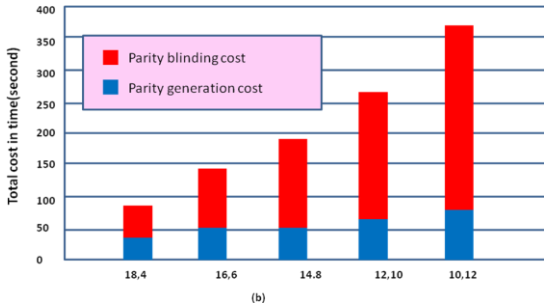
6. STORAGE CORRECTNESS VERIFICATION AND IDENTIFYING ERRORS

Error identifying is an important prerequisite for eliminating errors is storage system. It is also of critical significant to localization or identifies potential threats from external attacks. Many schemes do not explicitly consider the problem of data error localization, thus only providing binary results for the storage verification. Here, our scheme identify the misbehaving server .By our challenge response protocol outperforms those by integrating the storage correctness verification and error localization. The major advantage is our response value from servers for each challenge, but also identifies the potential data errors (s).

7. PROBILITY INTIFICATION FOR MISBEHAVING SERVERS

In this paper we modifies the data blocks among any of the data storage servers, here we are sampling analysing the scheme can be detected successfully when probability attack rate is high. When data modification is caught, the user will determine which server is malfunctioning, we can achieve it by the response values of the pre stored tokens. Here identifying the misbehaving servers can be computed in similar way as the earlier process.





In this figure we are performing the comparison between two different parameter settings for 1GB file distribution preparation.
The(m,k) denotes the chosen parameters for underlying Reed-Solomon coding.
For example:
Here (**10,2**) Denotes ,we split or divide the file into 10 data vectors.
We generate two redundant parity vectors.
In fig (a) *m* is fixed an *k* is decreasing.
In fig (b) *m+k* is fixed**.**

8. THIRD PARTY AUDITING WITH EFFECTIVE SERVICE LEVEL AGGREMENTS

In this paper, we mainly focus on efficient audit services for outsourced data in clouds, as well as the optimization for high-performance audit schedule. First of all, we propose architecture of audit service outsourcing

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

for verifying the integrity of outsourced storage in clouds. This architecture based on cryptographic verification protocol does not need to trust in storage servers providers. Based on this architecture, we have made several contributions to cloud audit services .

We provide an efficient and secure cryptographic interactive audit scheme for public audit ability. These two properties ensure that our scheme can not only prevent the deception and forgery of cloud storage providers, but also prevent the leakage of outsourced data in the process of verification. To detect abnormal situations timely, we adopt a way of sampling verification at appropriate planned intervals.

CONCLUSION

In this paper, we addressed the construction of an efficient audit service with effective service level agreements for data integrity in clouds.. To realize the audit model, we only need to maintain the security of the third party auditor and deploy a lightweight daemon to execute the verification protocol. Hence, our technology can be easily adopted in a cloud computing environment to replace the traditional Hash-based solution. More importantly, we proposed and quantified a new audit approach based on **SLA's,**it includes service guarantee, service guarantee time period, service guarantee granularity, service guarantee exclusion, service violation measurement and reporting, service credit on cloud audit services. This approach greatly reduces the workload on the storage servers, while still achieves the detection of servers' misbehavior with a high probability. Our paper clearly revels that our approach could minimize computation.

ACKNOWLEDGMENT

This work was supported in Aurora's Scientific Technological and Research Academy and Jawaharlal Nehru Technological University- Hyderabad, Andhra Pradesh, India.

I wish to express my sincere thanks to Mrs. Chepure Srilatha, Deputy Director, Aurora's Scientific Technological and Research Academy.

I place on record, my sincere gratitude to Mrs. Vemula Aruna-PhD, HOD, Department of Computer Science Engineering, for her constant encouragement extended to me.

I also thank Mr.S.Srinivas Kumar-M.Tech, Senior Associate Professor, Department of Computer Science Engineering, Aurora's Scientific Technological and Research Academy and Mr. G. Sudhakar, Academic Assistant (Lecturer), Department of School of Information Technology, JNTU - Hyderabad.

I take this opportunity to record my sincere thanks to all the faculty members of the Department of Computer Science Engineering from Aurora's Scientific Technological and Research Academy for their help and encouragement. I also thank my parents for their unceasing encouragement and support.

I also place on record, my sense of gratitude to one and all who, directly or indirectly, have lent their helping hand in this project.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing,"
[2]http://aws.amazon.com
[3]https:/www.sun.com/offers/details/sun_transparency.xml.

BIOGRAPHIES

G. MAHINDER received the B.Tech degree from Sree Kavitha Engineering College, JNTU-H in department of CSE in 2011. I am currently working toward Post Graduation degree (M.Tech) student in Computer Science and Engineering at Aurora's Scientific, Technological and Research Academy. My research interests are in the area of Security in cloud computing, secure data services in cloud computing, data integrity and data dynamics. I am a student member of CSTA.

S. SRINIVAS KUMAR received the M.Tech from Nizam Institute of Engineering and Technology-HYD . He is working as a Sr.Assistant.Professor, in the department of Computer Science and Engineering at Aurora's Scientific Technological & Research Academy-Hyd. His goal was to understand how technology can help people explore, understand and share complex information and knowledge. He applies and evaluates techniques from middleware technologies, software engineering, some other cutting edge technologies to bring out a final product .His research interests are in the areas of Software Engineering, Security and privacy in cloud computing.

G. SUDHAKAR received the M.Tech-Post graduation from Jawaharlal Nehru Technological University, Hyderabad-India. He is working as a Academic Assistant (Lecturer), in the School of Information Technology at JNTU-H. He is currently a PhD student at Jawaharlal Nehru Technological University-Hyderabad .His Research interests are in the areas of Security in cloud computing and software engineering, with a current focus on secure data services in cloud computing and secure computing outsourcing. He is a student member of IEEE.