Enhancing Security for Storage Services in Cloud Computing

S.Suganya[1], P.Damodharan[2]

[1]II-M.E, Department of Computer Science,
Akshaya College of Engineering and Technology, Coimbatore-642109.
E-Mail: sugi25@gmail.com

[2]Associate professor, Department of Computer Science,
Akshaya College of Engineering and Technology, Coimbatore-642109.
E-Mail: damodharan@acetcbe.edu.in

Abstract- Storage Services in cloud computing allows users to store away for the high quality cloud applications on-demand to enjoy without the hassle of managing their own hardware and software their data. While the benefits of these services are more, there are new security threats in the direction of the accuracy of the data in the cloud due to the physical possession of their outsourced data. To address this new problem and improved security and reliable cloud storage service to realize, we propose a distributed storage integrity auditing mechanism, by utilizing the homomorphic token and distributed erasure-coded data in this article. The proposed design allows users to monitor the cloud storage with very lightweight communication and computation costs. This provides strong cloud storage accuracy, and also allows for faster fault location data, that is to say, the identification of misbehaving server. The proposed design supports continued safe and efficient dynamic activities, including block modification, deletion and append. The proposed system is very effective against server colluding attacks and data modification attacks.

I. INTRODUCTION

Processors cheaper and more powerful, along with the software as (SaaS), service computing architecture, are transforming data centers into service groups to large scale computing. The growing connections reliable and flexible network that is still possible that users can now subscribe high quality services from data and software that resides only in remote data centers

The movement of data in the cloud offers convenience to users because they do not have to worry about the complexities of direct hardware management. Online services do not offer large amounts of storage space and customization of computer resources. Bu users are at the mercy of their cloud service providers (CSP) the availability and integrity of their data. Because users cannot save a local copy of the external data, CSP has to behave unfaithful to cloud users. CSP can even try to hide the loss of data in order to maintain a reputation. In order to achieve the assurance of the integrity and availability of data in cloud and enforce the quality of storage service in the cloud, on-demand that allows verification of correctness of the data on behalf of users of the cloud.

To achieve guarantees of integrity and availability of data cloud and enforce the quality of cloud storage services have to enable the effective methods that correct the review letter, the data on behalf of the cloud users, be developed. However, prohibiting the fact that users no longer physically in possession of the data directly in the cloud over the traditional cryptographic primitives for the purpose of protecting the integrity of the data. Therefore, check the accuracy of cloud storage space without explicit knowledge of the entire data files must be. Meanwhile, cloud storage is not only a third of the data storage. The data is stored in the cloud not only accessible, but also uses updated frequently, including insertion, deletion, modification, attachments, etc. Therefore, it is important to integrate these dynamic roles in correcting supports cloud storage backup, the system design difficult. Last but not least, the use of cloud computing data centers, driven and worked on a distributed concurrent. It is more advantages for individual users to store data redundantly across multiple physical servers to reduce the data integrity and availability threats. Therefore distributed protocols for ensuring storage correctness is most important in achieving systems robust cloud storage and insurance. However, this important area has not been studied in the literature.

In this paper, we propose a verification scheme efficient and flexible distributed storage with explicit dynamic data support to ensure the accuracy and availability of user data in the cloud. We erasure correction code in the file distribution preparation to provide redundancies and guarantee the data reliability Byzantine servers in a storage server may fail arbitrarily. This construction drastically reduces the communication and storage overhead compared to the distribution techniques traditional file-based replication. By using homomorphic signal with the verification of erasure-coded distributed data, our scheme achieves the storage correctness insurance as well as data error localization: whenever corruption is detected during verification data storage of the correction, our scheme can almost guarantee simultaneous localization error data, i.e., identification of misbehaving server (s). In order to achieve a good balance between error resilience and dynamics data, we explore the algebraic property over our symbolic computation and data erasure coded, and demonstrate how efficiently support dynamic operation of data blocks, while maintaining the same level of storage correctness assurance. To save time, computing resources, and even load-related online

users, we also provide the extension of the main scheme proposal to support third-party audit, where users can safely.

The data presented in cloud storage are insured, but the integrity and availability is not assured. The data can be hacked in the cloud storage and databases can get corrupted. To overcome this problem, an intermediate TPA is enhanced with encryption techniques, authentication and auditing.

II. PROBLEM STATEMENT

2.1 System Model

Representative Network Architecture cloud storage service can be identified as follows:

• User: an entity that has data to be stored in the cloud and cloud-based data storage and calculation, can be either company or individual clients.

• Cloud Server (CS): an entity that is managed by the cloud service provider (CSP) to provide a data storage service and has storage and computation significant resources (we will not differentiate CS and CSP onwards).

• Auditor of others: the optional TPA, which has experience and capability that users can not have, is trusted to assess and expose risk of storage services in the cloud, on behalf of the users on request.

As users no longer have their data locally, it is vital to ensure users that their data is being stored and maintained properly. That is, users must be equipped with safety means for them to make assurance continuity correction (to enforce a service level agreement cloud storage) of your stored data, even in the absence of local copies. If users do not have at the moment, feasibility or resources to manage their data online, you can delegate the audit data to a trusted TPA Optional their options. However, to safely introduce such TPA, for leaking external data users to the TPA through the audit protocol should be prohibited.

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

2.2 Design Goals

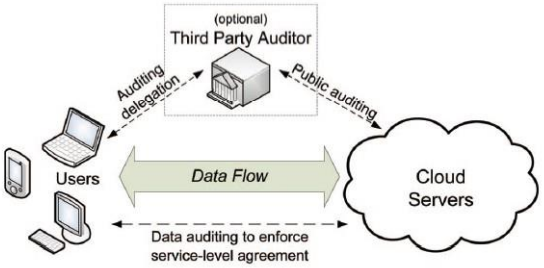
To ensure safety and reliability for cloud data storage in former adversary model, our goal is to design effective mechanisms for dynamic data verification operation and the achievement of the following objectives:

1. Correction storage: to assure users that their data is actually stored properly and kept intact all the time in the cloud.
2. Quick data error localization: to locate the server is running effectively when detected data corruption.
3. Dynamic Data Support: to maintain the same level of assurance of the correctness of storage, although users to modify, delete or add data files in the cloud.
4. Reliability: to improve the availability of data against Byzantine failures, data modification and collusion malicious server attacks, i.e. minimizing the effect brought by data errors or failures of the server.
5. Lightweight: to allow users to perform accuracy checks with minimal overhead storage.

III. PROPOSED STATEMENT

In the data storage system in the cloud, users store their data in the cloud and do not have the data locally. Therefore, you should ensure the correctness and availability of the data files that are stored on distributed cloud servers. One of the key issues is effectively detect any modification and unauthorized data corruption, possibly due to the commitment of the server and / or random Byzantine fault. Furthermore, in the case when detecting distributed successfully these inconsistencies, to find that the data server error is in is also very important, since you can always be the first step to quickly recover storage errors and / or identifying potential external threats attacks.

To address these problems, our main scheme to ensure cloud data storage is presented in this section.



The first part of the section is devoted to a review of the basic tools of coding theory in our distribution program files needed by cloud servers. The token is used homomorphic next. The counter is one of a calculation based on universal family of hash function is selected to obtain the homomorphic properties which can be seamlessly in the verification of erasure coded data is integrated. Then it is shown how to obtain a challenge-response protocol to verify the proper storage and labeling of crashed servers. The method of file recovery and troubleshooting based on erasure correcting code are also described. Finally, we describe how tight third parties only with a slight modification of the core extend audit procedures to our plan.

3.1 Toward Third Party Auditing

As discussed in the architecture, in the event that the user does not have the time, viability, or the resources to carry out the verification of the correctness of storage, which may delegate this task to an independent external auditor, so that the cloud Storage publicly verifiable. However, as the recent work safely introduces an effective TPA should the audit process to bring in no new vulnerabilities to the privacy of user data. That is, should not learn TPA content of user data through data auditing delegates. Now we can show that only with a slight modification, the protocol can support privacy preserving audit by a third party.

The new design is based on the observation of the linear property blinding process parity vector based. Recall that the reason for the process of blinding the secret matrix P to cloud servers to protect. However, this can be either through blinding glare of the parity vector or vector data (assuming k <m) can be achieved. Therefore, if we blind data vector before coding file distribution, then the storage inspection task can be delegated preserves successful testing by third parties in a way that privacy.

The proposed system overcomes the security risks through the implementation of Third Party Audit (TPA) authentication

capability. TPA stores user information such as user password, date and time. It is envisaged, where the loading and unloading of data encryption and decryption algorithms. If there is no change in the facts that informs the user TPA. This ensures greater security, availability and integrity

IV. PROVIDING DYNAMIC DATA OPERATION SUPPORT

So far we have assumed that F represents the static data or archived. This model can be adapted to some application scenarios, such as libraries and academic records. Nevertheless, the storage of data in the cloud, there are many scenarios where data is stored in the cloud dynamically as electronic documents, pictures, or log files, etc. Therefore, it is important to consider the dynamic case, where a want to perform user update various block-level operations, delete and append to change the data file while the ensure storage correctness.

Since the data are not in the local user of the site, but the domain of management cloud service provider supports dynamic data operation can be quite difficult. On the one hand, the CSP must request material to process dynamic data without knowledge of the secret key. On the other hand, the user must ensure that every request for dynamic data operation has been faithfully processed by CSP.

To address this problem, we focus briefly explain our methodology and provide the details later. Dynamic operation for all data, the user must have the appropriate blocks and parity files first revolution. This part of the operation performed by the user, since only he knows the secret matrix P. In addition, to ensure that data block changes reflected correctly in the domain address cloud, the user also has to check token corresponding change memory to accommodate changes in data blocks. Just check sheets changed accordingly storage, the challenge-response protocol discussed above are performed on success, even after the data dynamics.

V. RELATED WORKS

Juels and Kaliski Jr., described as a proof of retrievability model, formal ensure the integrity of the remote database. His plan to combine randomly checked and an error correction code, both owned and exploitable guarantee.

Shah et al suggested that keep online storage honest first encrypting the data, send a set of pre-computed hash TPA symmetric key encrypted data to the auditor. However, the system works only encrypted files and auditors should receive long-term illness. Black Miller proposed to improve the reliability of static files distributed across multiple servers, in which ensure the encryption and block-level verification of the integrity of the deleted file. We have adopted some of his thoughts on distributed storage authentication protocol. However, studies show our support system, the dynamic disk problem and crashed the server when they are identified. Recently, Wang et al to check many existing solutions for remote data integrity and discuss their advantages and disadvantages in different scenarios project cloud storage services safely.

VI. CONCLUSION

In this paper, we study the problem of data security in data storage in the cloud, which is essentially a distributed storage system. To achieve guarantees of integrity and availability of data in the cloud and enforce service quality reliable cloud storage to users, distributed propose an efficient and flexible scheme. By utilizing the homomorphic token with distributed verification of erasure coded data, our system is the integration of storage correctness insurance and data error localization, i.e. achieved, we can ensure the simultaneous identification of misconduct server (s). Given time, computing resources, and even user online sensitive cargo, we also provide an extension of the main scheme proposed third party audit, where users can safely delegate tasks supports the auditors check integrity of others and be free of concerns to use cloud storage services

With the adoption of the proposed system, the correction of the integrity and availability of cloud data, encrypting stored data can be achieved. The resulting system will be protected against data corruption and piracy. Unauthorized access by CSP is preventable.

REFERENCES

[1] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, “Toward Secure and Dependable Storage Services in Cloud Computing” IEEE Transactions on services computation vol. 5, no. 2, April-June 2012.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality of Service (IWQoS ’09), pp. 1-9, July 2009.

[3] A. Juels and B.S. Kaliski Jr., “PORs: Proofs of Retrievability for Large Files,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 584-597, Oct. 2007.

[4] Sun Microsystems, Inc., “Building Customer Trust in Cloud Computing with Transparent Security,” https://www.sun.com/offers/details/sun_transparency.xml, Nov. 2009.

[5] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[6] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, “Auditing to Keep Online Storage Services Honest,” Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS ’07), pp. 1-6, 2007.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. 14th European Conf. Research in Computer Security (ESORICS ’09), pp. 355-370, 2009.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[9] J. Hendricks, G. Ganger, and M. Reiter, “Verifying Distributed Erasure-Coded Data,” Proc. 26th ACM Symp. Principles of Distributed Computing, pp. 139-146, 2007.

[10] K.D. Bowers, A. Juels, and A. Oprea, “Proofs of Retrievability: Theory and Implementation,” Proc. ACM Workshop Cloud Computing Security (CCSW ’09), pp. 43-54, 2009.