International journal of imaging science and engineering

ISSN: 1934- 9955www.ijise.net

Vol-02 Issue-01 May 2007

# A System for Guaranteeing the Safety of Data Storage in the Cloud

**K. A. CHORMULE** K. A. CHORMULE23@gmail.com

## ABSTRACT

Many see cloud computing as the backbone of the IT enterprise of the future. Cloud computing relocates application software and databases to massive data centers, where the administration of the data and services may not be entirely reliable, in contrast to conventional systems that have IT services under appropriate physical, logical, and human controls [3]. But this one-of-a-kind quality brings up a plethora of unanticipated security concerns. Cloud data storage security has always been a key component of service quality, and that is what we want to address here. We provide an efficient and adaptable distributed system with two distinguishing characteristics that, in contrast to its forerunners, will guarantee the accuracy of users' data stored in the cloud. Our technique accomplishes the combination of storage accuracy insurance and data error localization, namely the detection of misbehaving server(s), by integrating the homomorphic token with distributed verification of erasure-coded data. The novel technique goes above and beyond what has been done before by allowing for safe and efficient dynamic operations on data blocks, such as adding, removing, or updating data. The suggested technique has been through rigorous performance and security testing, and it has shown to be both efficient and resistant to Byzantine failure, malicious data alteration assaults, and server collusion attacks.

**keyword:** Data storage in the cloud, cloud computing, error localization, and cloud service providers Introduction

Organizations today are increasingly looking towards Cloud Computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and elastic services. The Cloud technology is a growing trend and is still undergoing lots of experiments. Cloud promiseshuge cost benefits, agility and scalability to the business. All business data and software are stored on servers at a remote location referred to as Data centers [1]. Cloud Computing is an Internet-based development. Users can now subscribe high quality services from data and software that reside solely on remote data centers. The pioneers of Cloud Computing Vendors are Amazon Simple

Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [5]. While these internet- based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data [2]. From the perspective of data security, which has always been an important aspect of quality of service,. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. . The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance [3].

International journal of imaging science and engineering

ISSN: 1934- 9955www.ijise.net

Vol-02 Issue-01 May 2007

## 1. Problem Statement

The proposed system has three important entities. User: Users store data in the cloud and depend on the cloud for all its computations on the data stored in the cloud.

Cloud Service Provider (CSP): CSP contains resources and expertise in building and managing distributed cloud storage servers, owns and operates and leases the live Cloud computing systems.

Third Party Auditor (TPA): TPA has expertise and capabilities that users may not have, is trusted toassess, audit and expose risk of cloud storage services on behalf of the users upon request from the users.

A special entity is considered to ensure the security and dependability of the Cloud Server referred to as Adversary Model. The adversary is interested in continuously corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user [4].

## 2. Cloud Data Storage Architecture With Existing System

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

**2.1** Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.

**2.2** Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, delete ion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

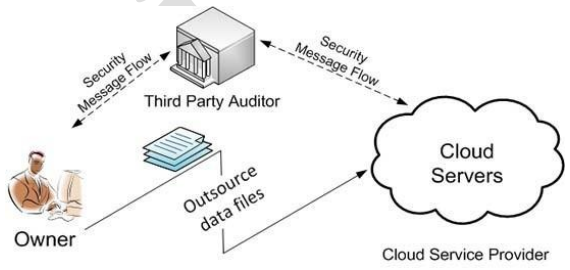


Figure 1.1: Cloud data storage architecture

**A. Limitations of Existing System :** These techniques, while can be useful to ensure the storage correctness

International journal of imaging science and engineering

ISSN: 1934- 9955www.ijise.net

Vol-02 Issue-01 May 2007

without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.[4]

**B. Proposed System**

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud.. This construction drastically reduces the communication and storage overhead ascompared to the traditional replication-based file distribution techniques. Whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s) [4].

**C. Advantages of Proposed System**

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge- response protocol in our work further provides the localization of data error.
2. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
3. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

**D. Token correctness**

It achieves assurance for data storage correctness and data error localization, using pre-computed token. Before sharing file distribution using pre- computes a certain number of shortest verification token are generated that will ensure security for a block of data in a file in cloud storage. When the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated block indices. After getting assurance of the user it again asks for authentication by which the user is

confirmed to be the authenticated user. Upon receiving assurance, each cloud server computes a short "signature" over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens pre-computed by the user. All servers operate over the same subset of the indices, the requested response values for integrity check must also be a valid codeword determined by a secret matrix. Suppose the user wants to challenge the cloud server's t times to make sure the correctness of data storage. Then, he must pre-compute t verification tokens for each function, a challenge key and a master key are used. To generate the ith token for server j, the user acts as follows the details of token Generations are shown in Algorithm 1.

International journal of imaging science and engineering

ISSN: 1934- 9955www.ijise.net

Vol-02 Issue-01 May 2007

- Derive an arbitrary value i and a permutation key based on master permutation key.
- Calculate the set of randomly-chosen index.
- Calculate the token using encoded file and the arbitrary value derived.

## 3. Algorithm for Token Pre-computation

1. Block of data is represented as l;
2. No. of .blocks is denoted as n;
3. Let f be the function and t be the token ;
4. Index per proof is denoted as r;
5. Generate M **k** and **C k ;**
6. For point G (j); j->1, n execute /*j server position*/
7. For round i->1, t execute /*i block index*/
8. Derive i = f (i) and k (i) from master key. Compute v(j)
9. End forEnd for
10. Store all the Vis locally.
11. End procedures

## 4. Correctness Verification and Error Localization

Error localization is a key requirement for eradicate errors in storage systems. However, many previous schemes do not explicitly consider the problem of data error localization. The challenges response protocol in our work future provides the localization of data error. This only provides binary results about the storage state across the distributed service in predecessors. The response values from servers for each challenge not only determine the correctness of the distributed storage, but also contain information to locate potential data error(s). Specifically, the procedure of the ith challenge response for a cross-check over the n servers is described as follows:

- The client reveals the i as well as the ith key k
  (i) to each servers
- The server storing vector G aggregates those r rows
- Specified by index k(i) into a linear combination R
- Upon receiving R is from all the servers, the user takes away values in R.
- Then the user verifies whether the received values remain a valid codeword determined by secret matrix.

Because all the servers operate over the same subset of indices, the linear aggregation of these r specified rows (R (1) i. . . R (n) i) has to be a codeword in the encoded file matrix. If the above

equation holds, the challenge is passed. Otherwise, it indicates that among those specified rows, there exist file block corruptions. Once the inconsistency among the storage has been successfully detected, we can rely on the pre-computed verification tokens to further determine where the potential data error(s) lies in. Note that each response R (j) i is computed exactly in the same way as token v (j) i, thus the user can simply find which server is

International journal of imaging science and engineering
ISSN: 1934- 9955www.ijise.net
Vol-02 Issue-01 May 2007

misbehaving by verifying.

## 5. Experimental Results

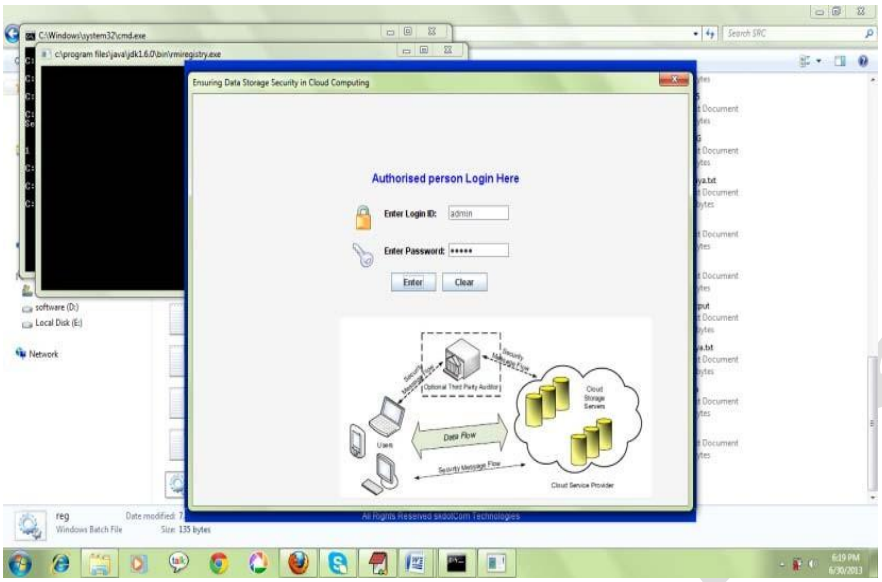


Fig.1.2 Authorized Person Login


Fig.1.3 Cloud Data Storage

International journal of imaging science and engineering

ISSN: 1934- 9955www.ijise.net

Vol-02 Issue-01 May 2007

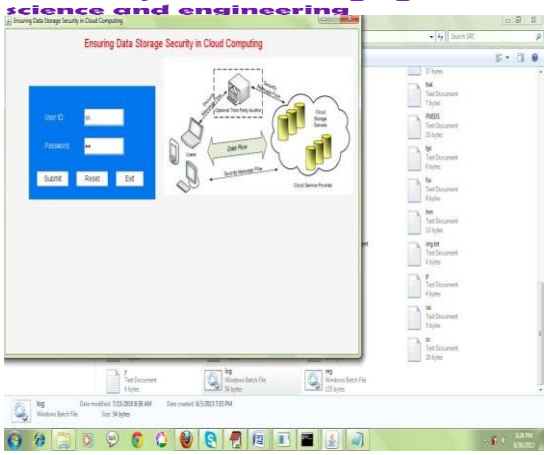


Fig.1.4 User Side Login

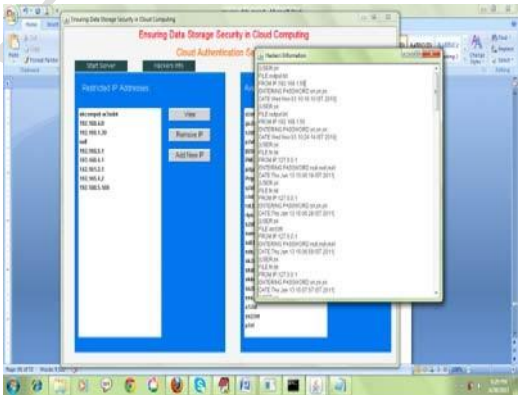


Fig.1.5 Misbehaving Server Model

## 6. Conclusion

In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data

dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost

guarantee the simultaneous identification of the misbehaving server(s)[3]. Through detailed security and performance analysis, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks. We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. We envision several possible directions for future research on this area.

## References

1) "Ensuring Data Storage Security in Cloud Computing," an IEEE paper written by Qian Wang, Cong Wang, and Kui Ren with Wenjing Lou as the author.

2. in "Towards publicly auditable secure cloud data storage services," Wang, K. Ren, W. Lou, and J. Li (2010), pp. 19-24 in IEEE Network Magazine, vol. 24, no. 4.

3. "Ensuring Data Storage Security in Cloud Computing" by Rampal Singh, Sawan Kumar, and Shani Kumar Agrahari, published in the International Journal of Engineering and Computer Science with the ISSN number 2319-7242. Security Concerns: Efficient Secured Data Storage Operations in a Cloud Computing Environment, by S. Mohamed Saleem and P. Sasi Kumar

vsrd international journal of computer science & information technology, vol. 2 no. 10 october 2012, issn no. 2231-2471 (online), 2319-2224 (print) © vsrd international journals : www.vsrdjournals.com

1. Vasu Raju, Raj Kumar, and Anand Raj," Techniques for Efficiently Ensuring Data Storage Security in Cloud Computing" Vasu Raju et al, Int. J. Comp. Tech. Appl., Vol 2 (5), 1717-1721 IJCTA | SEPT- OCT 2011 Available online@www.ijcta.com 1717 ISSN:2229-6093.

2. Case study: http://eyeos.org/ cloud desktop.

3. Amazon.com, "Amazon Web Services (AWS)," Online at http://aws. amazon.com, 2008

4. http://searchcloudcomputing.techtarget.com/reso urces#parentTopic4

5. K.Valli Madhavi, R.Tamilkodi, R.BalaDinakar," Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System", International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.

6. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

International journal of imaging science and engineering

ISSN: 1934- 9955www.ijise.net

Vol-02 Issue-01 May 2007

7.