

Priya

Volume: 1 Issue: 1

A MECHANICS FOR ASSURING DATA STORAGE SECURITY IN CLOUD COMPUTING

¹Priya, ²Pratibha Gangwar, ³Mamta Gadoria

¹M. Tech. Scholar, Jayoti Vidyapeeth Women's University, Jaipur, priya25mehta@gmail.com

²M. Tech. Scholar, Jayoti Vidyapeeth Women's University, Jaipur, er.pratibha20@gmail.com

³M. Tech. Scholar, Jayoti Vidyapeeth Women's University, Jaipur, mgadoria007@gmail.com

ABSTRACT

Cloud Computing has been visualized as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy [3]. This unique attribute however, poses many new security challenges which have not been well understood. In this we focus on cloud data storage security, which has always been an important aspect of quality of service. To provide the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. 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., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. 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.

Index Terms: Cloud Computing, Cloud Service Provider, Cloud data storage, Error localization

1. 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 promises

huge 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

Priya

Volume: 1 Issue: 1

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].

2. 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 to

assess, 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].

3. 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.

3.1 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.

3.2 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

Priya

Volume: 1 Issue: 1

insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

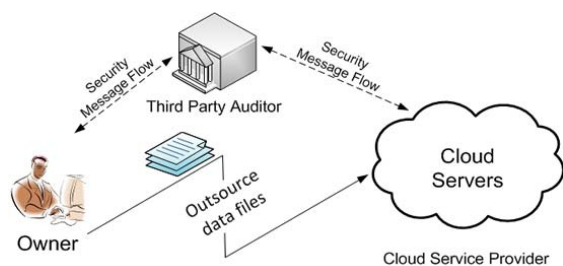


Figure 1.1: Cloud data storage architecture

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

compared 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

Priya

Volume: 1 Issue: 1

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 i th token for server j , the user acts as follows the details of token Generations are shown in Algorithm 1.

- 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.

4. 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); $j \rightarrow 1, n$ execute /* j server position*/
7. For round $i \rightarrow 1, t$ execute /* i block index*/
8. Derive $i = f(i)$ and $k(i)$ from master key. Compute $v(j)$
9. End for

10. End for
11. Store all the V is locally.
12. End procedures

5. 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 i th challenge response for a cross-check over the n servers is described as follows:

- The client reveals the i as well as the i th 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 ($R(1) \dots R(n)$) has to be a codeword in the encoded file matrix. If the above

Priya

Volume: 1 Issue: 1

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 $R(j)$ is computed exactly in the same way as token $v(j)$, thus the user can simply find which server is misbehaving by verifying.

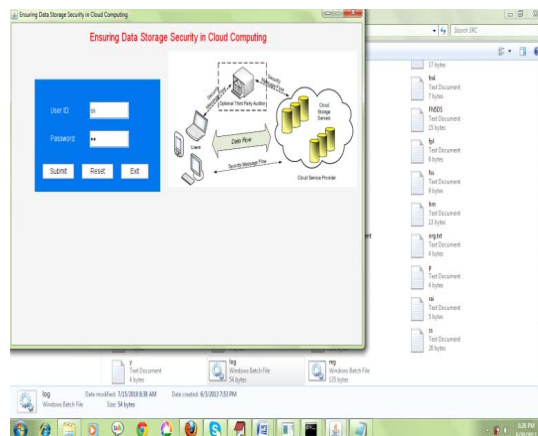


Fig.1.4 User Side Login

6. Experimental Results

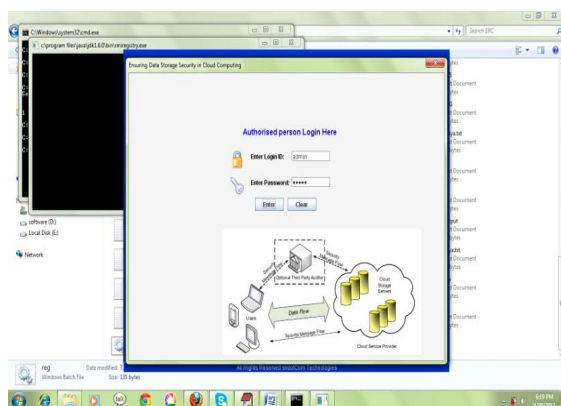


Fig.1.2 Authorized Person Login

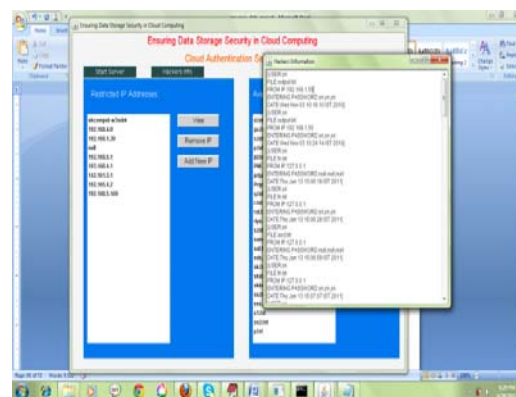


Fig.1.5 Misbehaving Server Model



Fig.1.3 Cloud Data Storage

7. 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

Priya

Volume: 1 Issue: 1

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. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing" IEEE Paper.
2. Wang, K. Ren, W. Lou, and J. Li, "Towards publicly auditable secure cloud data storage services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, 2010.
3. Rampal Singh, Sawan Kumar, Shani Kumar Agrahari, "Ensuring Data Storage Security in Cloud Computing", International Journal Of Engineering And Computer Science ISSN:2319-7242.
4. S. Mohamed Saleem and P. Sasi Kumar, "Security Issues : Efficient Secured Data Storage Operations In Cloud Computing Environment", 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.vsrjournals.com
5. 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.
6. Case study: <http://eyeos.org/> cloud desktop.
7. Amazon.com, "Amazon Web Services (AWS)," Online at <http://aws.amazon.com>, 2008
8. <http://searchcloudcomputing.techtarget.com/resources/#parentTopic4>
9. 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) NCRCTCST, ISSN 2249-071X.
10. 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/>.