Survey of Integrity Verification in Multi-Cloud Storage by Efficient Cooperative Provable Data Possession

Trilok Singh Pardhi
PG Scholar DoCSE
UIT-RGPV, Bhopal (India)

Rajeev Pandey, Ph.D
Asst. Prof. DoCSE
UIT-RGPV, Bhopal (India)

Uday Chourasia
Asst. Prof. DoCSE
UIT-RGPV, Bhopal (India)

ABSTRACT

Provable data possession (PDP) is one of the techniques to ensure the integrity of data in storage outsourcing. Here in this paper, we speak to the creation of an efficient PDP method for distributed cloud storage to maintain the scalability of service and data migration. On the basis on homomorphic verifiable response and hash index hierarchy we projected a cooperative PDP (CPDP) method. We confirm the security of our method based on multi-prover zero-knowledge proof scheme, which can satisfy knowledge soundness, fullness , and zero-knowledge properties. As well, we expressive performance optimization mechanisms for our method, and in particular present an capable method for selecting finest parameter values to reduce the addition expenses of storage service providers and client. Our experiment shows that our solution introduces lower addition and communication overheads in evaluation with non-cooperative approaches.

Keywords

Scalability, Data Migration, Homomorphic, Multi-Prover

1. INTRODUCTION

The term Cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer network diagrams as an abstraction of underlying infrastructure it represents. Typical cloud computing providers deliver common business application online which are accessed from web browser, while the software and data are stored on server.

2. LITERATURE SURVEY

2.1 Ensuring Data Storage Security In Cloud Computing Environment

Cloud Computing has been predict as the next creation construction in IT Enterprise. In contrast to predictable solutions, where the IT services are in correct logical , physical and personnel controls, Cloud Computing moves on application software and databases to access the large data centers, where the managing of the services and data may not be entirely reliable. This single attributes, on the other hand, posses many new security confronts that have not been well implied. In this article, we limelight on cloud data storage security, that has always been an vital facet of quality of service. To guarantee the correctness of cloud users' data in the cloud, we recommend an effective and flexible distributed method have two features, opposing to its ancestor. By utilizing the features, opposing to its predecessors. To obtain erasure-coded data we use of homomorphism token with distributed verification, our method achieves the combination of storage correctness, assurance and data error localization, i.e., the recognition of unruly server(s). Dissimilar most previous works, the new method further supports efficient dynamic operations safe and secure on data blocks, including: such operation like that data modification ,append and delete. Proposed method is vastly efficient supple against malicious data alteration attack, Byzantine collapse ,and even server colluding attacks prove based on general security and performance analysis.

Disadvantage

1. This method doesn't allow to automatic blocking the cloud server .
2. Less Security – None of the cryptographic techniques is used on the cloud data

2.2 Privacy-Preserving Audit And Extraction Of Digital Contents

Please

2.3 This paragraph is a repeat of 3.1

Please A growing number of online services providers, such as Google, Yahoo!, and Amazon, are suppose to charge users for their storage. With the help of these service cloud user store our important data such as video, emails , document and file backups. On the day, a cloud user must totally trust such external services to preserve the integrity of data and return it undamaged. Unluckily, there are no service is to keep on the trust. To build storage services responsible for data failure, we proposed protocols that permit a third-party auditor to sporadically confirm the data stored by a assist and service in returning the same as usual data to the customer. That used protocols are privacy-preserving, in that they not at all divulge the data contents to the assessor. This solution eliminates the burden of verification from the customer, improves both the storage service's and customer's data dread of data leakage, and offers a method for free arbitration of data preservation contracts.

Disadvantage

1. There are no features to prove integrity based on public key or any other key while based on file name.
2. The details of attackers are not dynamic store but use the log file to store details and used data mining concepts to viewing it, that is time consuming job and less security.

2.4 Provable Data Possession At Untrusted Stores

Some method to provide data availability and integrity that follow traditional cryptographic technologies based on signature scheme and hash function. It cannot work on outsourced data. And did not suitable for a large size file. So Provable Data Possession method come on picture , to ensuring the integrity and availability of file and based on RSA scheme and reduced the communication cost. But PDP method are suitable only for single cloud storage not for multi cloud storage. The cloud user maintains a invariable quantity of metadata to confirm the proof. We have two provably-secure PDP mrthods that are further competent than earlier solutions, when compared with methods that get weaker guarantees.

Disadvantage

i PDP method doesn’t allow to automatic blocking the cloud server.
ii Owner’s data will be stored in untrusted cloud servers.
iii Subsequent Pages Scalable and Efficient Provable Data Possession

2.5 Scalable and Efficient Provable Data Possession

To overcome the problem of Provable data Possession At Untrusted Store method they present the efficient new PDP method called The Scalable and Efficient Provable Data Possession . Which act as a powerfull deterrent to corrupt thus growing trust in the system . Recently proposed method are not capable for the large amount of data for that we use Scalable and Efficient Provable Data possession method . That method are based on an symmetric key cryptosystem and support to secure and efficient dynamic operation such as modification ,deletion ,append etc. That method gives probabilistic declaration of the untampered data which store in the server .That method are used for outsourcing of personal digital contact as a MAC, GMAIL, PICASA and OFOTO.

Disadvantage

1. By using the previous metadata orb response due to lack of randomness in the challenge server can deceive the owner .
2. The no of updates and challenges are limited .
3. Limitation of block insertion anywhere.

2.6 Page Numbering, Headers and Footers

Do not include headers, footers or page numbers in your submission. These will be added when the publications are assembled.

3. EXISTING SYSTEM

There survive different technologies and tools for multi cloud, like that Overt, VM Orchestrator and VMware vSphere. To create a distributed cloud storage podium for managing clients’ data these tools provide help to cloud provider. However, if such a significant platform is helpless to security attacks, it would bring irreversible wounded to the clients. For example, the private data in any venture may be illegitimately accessed during a remote interface which supplied by a multi-cloud, or annals and relevant data and possibly will be vanished or tampered with when they are store into an doubtful storage pool exterior the venture. Therefore, it is requisite for cloud service providers. To present security techniques to handle their storage services.

Disadvantage

1. In existing system doesn’t have feature of automatic blocking the cloud server.
2. Existing system are less secure because of no modern cryptographic technique are used.
3. There are no feature to prove integrity based on public key or any other key while based on file name.
4. The details of attackers are not dynamic store but use the log file to store details and used data mining concepts to viewing it, that is time consuming job and less security.
5. Cloud user data store in untrusted cloud servers.

4. PROJECT AIM

To compute the cloud securely monitoring by Third Party Authority and achieving the data integrity, batch auditing

5. MODULE DESCRIPTION

5.1 Multi cloud storage

The. Multi cloud storage refer to any large cooperation in which many small cloud storage used to store large amount of data . In our system the each cloud server have data blocks. Data uploaded into multi cloud by cloud user. Cloud computing surroundings is constructed based on open architectures interfaces, that have the ability to add in multiple internal and/or external cloud services mutually to afford elevated interoperability. We call such a distributed cloud surroundings as a multi-Cloud . A multi-cloud permits clients to fluently access his/her possessions remotely throughout interfaces.

5.2 Cooperative PDP

Cooperative PDP (CPDP) method is an efficient PDP method to verifying the availability and integrity in multi cloud storage. It contains three-layered index hierarchy and zero-knowledge property. Through this method computation cost of client and storage service providers would be reduced. This method based on modern cryptographic techniques without compromising data privacy.

5.3 Data integrity

Data Integrity is very key feature of cloud computing. The data should not obtain customized without intentionally. The data should remain intect unless it is customized by authorized person.

6. THIRD PARTY AUDITOR

The Trusted Third Party (TTP) is an organization that’s authorized by an another organization to manage or process identifiable data for a specific purpose . Trusted Third Party provide interaction between two parties and both trust the third party. In our system stored verification parameters and for these parameters provide public query services. The Trusted Third Party, observe the cloud user data and uploaded in the distributed cloud. In multi-cloud surroundings each cloud server have user data blocks. If any edition tried by cloud user a alert is sent to the Trusted Third Party.

7. CONCLUSION

In this paper we proposed the construction of an efficient PDP method for distributed cloud storage. On the basis on hash index hierarchy and homomorphic verifiable response we projected a cooperative PDP (CPDP) method, that’s support to dynamic query such as insertion ,deletion append and modification etc on multiple storage servers. We also explained that our method offer all security assets follow to zero knowledge interactive proof system, therefore that it can resist different attacks which deployed in cloud as a public audit service. Moreover, we optimized the probabilistic uncertainty and intervallic verification to recover the audit performance. These experiments clearly established that our approaches only introduce a less amount of communication and computation outlay. These method are more suitable for storing the large amount of data in multi cloud server .

8. REFERENCES

[1] Y.Zun, H. Hu, G. Joon Ahn, “Coopr ative provable data possession for Intrigrity verification in multi cloud storage,” IEEE Transaction on parallel and distributed system , vol: PP, issue 99, 14-02-2012.

[2] R. S. Montero, B. Sotomayor, I. M. Llorente, I. T. Foster, “Virtual infrastructure management in private and hybrid clouds,” IEEE Internet Computing, vol.13, no. 5, pp. 14-22- 2009.

[3] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, “Provable data possession at untrusted stores,” ACM Conference on Computer and Communications Security, P. Ning, S.D.C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598-609.

[4] A. Juels and B. S. K. Jr., “Proofs of retrievability for large files,” ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584-597.

[5] G. Ateniese, L. V. Mancini, R. D. Pietro and G. Tsudik, “Scalable and efficient provable data possession,” Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1-10.

[6] C. C. Erway, C. Papamanthou ,A. K¨upc¸ ¨u , and R. Tamassia, “Dynamic provable data possession,” in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213-222.

[7] H. Shacham and B. Waters, “Compact proofs of retrievability,” ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90-107.

[8] Q. Wang, J. Li, K. Ren, C.Wang and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355-370.

[9] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced storages in clouds,” SAC, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550-1557.

[10] K. D. Bowers, A. Oprea and A. Juels, “Hail: a high-availability and integrity layer for cloud storage,” ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187-198.

[11] Y. Dodis, S. P. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109-127.

[12] L. Fortnow, M. Sipser and J. Rompel “On the power of multiprover interactive protocols,” Theoretical Computer Science, 1988, pp. 156-161.

[13] Y. Zhu, G.-J. Ahn, H. Hu, Y. Han, and S. Chen, “Collaborative integrity verification in hybrid clouds,” in IEEE Conference on the 7th International Conference on Collaborative Computing*: October 15-18*, 2011, pp. 197-206.

[14] M. Armbrust, , R. Griffith, A. Fox ,A. D. Joseph, A. Konwinski, R. H. Katz, , G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep., Feb 2009.

[15] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in *Advances in Cryptology (CRYPTO’2001),* vol. 2139 of LNCS, 2001, pp. 213-229.

[16] O. Goldreich, *Foundations of Cryptography: Basic Tools*. Cambridge University Press, 2001.