Middle-East Journal of Scientific Research 20 (4): 513-516, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.20.04.12032

Secured Cloud Info Storage in Addition to Integrity Products and Services

S. Thirunavukkarasu and M. Masthan,

Bharath University, Tagore Engineering College, India

Abstract: Cloud computing is the next stage in evolution of the internet, which provides large amount of computing and storage to customers provisioned as a service over the internet. However the prevalent problem associated with cloud computing is the cloud security and the appropriate implementation of cloud over the network. In order to make easier rapid deployment and to provide security, publicly auditable cloud data storage is established to reduce energy and save money. For the first time we formalize and implement effective utilization of single software through cloud, which can be accessed by several other systems for online testing. We consider the task of including a third party auditor (TPA) for client-side verification of data integrity. In order to regain the assurances of cloud data integrity and availability and to enforce the quality of cloud storage for users, we propose highly efficient and flexible distributed storage verification scheme by improving the existing model by manipulating the AES algorithm. The store and retrieve processes are done by crypto graphical methods. Numerical studies are extensively performed about the proposed scheme and the analysis shows that current cloud needs an order of magnitude in performance improvement to be useful for various storage and data integrity purposes and indicate which improvements should be considered first to make sure the quality and demand for the cloud increases.

Key words: Cloud computing · To provide security · Availability and to enforce · Data integrity

INTRODUCTION

Cloud computing is the sharing of resources over the internet by utilizing various hosted services provided by Cloud Service Providers (CSP).The CSP's provide services that can be broadly classified into three types namely: Infrastructure as a service (IAAS), Software as a Service (SAAS) and, Platformas a Service (PAAS). The advantage of cloud is cost savings. The prime disadvantage is security. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management [1-3]. The three Levels of Cloud 112 Computing are:Hardware Independence, Service Not Reliant on single Data Centre and Platform Agnostic Application Delivery. The biggest concerns about cloud computing are security and privacy. While most service vendors would ensure that their servers are kept free from viral infections and malware, it is still a concern considering the fact that there are number of users around the world are accessing the server. Privacy is another issue with cloud servers. Ensuring that the client's data is not accessed by any unauthorized users is of great importance for any cloud service. To make their cloud service more secure, cloud service vendors have developed password protected account, security service through which all data been transferred must pass and data encryption technique. After all, the success of the cloud service depends on its reputation and any sign of security breach would results in a loss of clients and business. Introducing a new and uniform security structure for all types of cloud is the problem we are going to tackle in this paper [3-6]. To ensure security, cryptographic techniques cannot be directly adopted. Sometimes the cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, we introduce an effective third party auditor to audit the user's outsourced data when needed. 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

Corresponding Author: S. Thirunavukkarasu, Bharath University, Tagore Engineering College, Inida.

more challenging. 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, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. In this paper we focus on providing dynamic integrity of the data stored as well as the security problems faced in cloud [7-11].

Problem Statement

A. System Design: The cloud computing network architecture consists of different entities or components as follows:

- Cloud User(CU)
- Cloud Server(CS)
- Cloud Service Provider(CSP)
- Third Party Auditor(TPA)

The cloud user accesses the cloud to store and retrieve his data in an efficient manner from the cloud server. The cloud users make use of various services in the cloud server from the cloud service providers. For the purpose of better and enhanced security for the user's data, a third party auditor is introduced.

Third Party Auditor: The main task of the TPA is to audit the user's data on his request. The TPA has no direct access to the data content stored by the user thus providing data privacy to the user. We assume the TPA, who is in the business of auditing, is reliable and independent and thus has no incentive to collude with either the CS or the users during the auditing process. As users no longer possess their data locally, it is of critical importance to assure users that their data are being correctly stored and maintained [12-14]. That is, users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the 113 existence of local copies. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA.

Cloud User (CU): Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

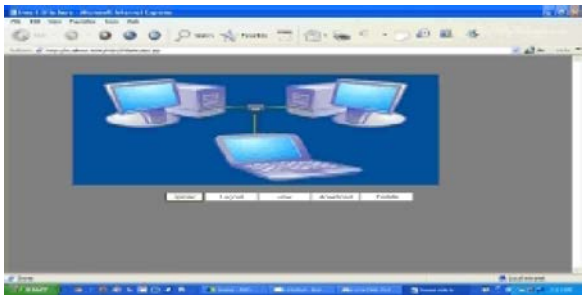
Cloud Service Provider (CSP): A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

Existing System: To introduce an effective third party auditor (TPA) for privacy and security, the following fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data and introduce no additional on-line burden to the cloud user. The third party auditing process should bring in no new vulnerabilities towards user data privacy. They utilized and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. This scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA. The security and performance is justified through concrete experiments and comparisons with the state-of-the-art [15-17]. In cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed or even hiding data loss incidents so as to maintain a reputation. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. Another problem is that data stored in the cloud does not remain static.

Proposed System: We enhance the scheme with explicit and efficient dynamic data operations for data storage security in Cloud Computing. Therefore, it is crucial to consider the dynamic case, where a user may wish to perform various block-level operations of update, delete and append to modify the data file while maintaining the storage correctness assurance. The straight forward and trivial way to support these operations is for user to

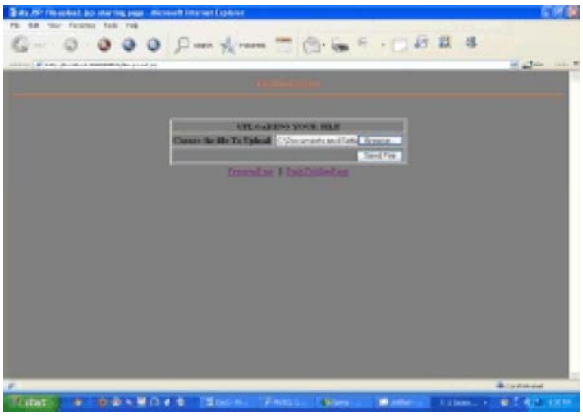
download all the data from the cloud servers and re-compute the whole parity blocks as well as verification tokens.

Dynamic Operations

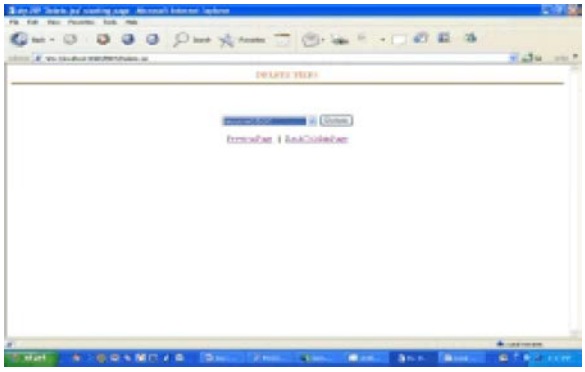


A. Update Operation: In cloud data storage, sometimes the user may need to modifysome data block(s) stored in the cloud, from its current value cd to a new one, cd + cd.We refer this operation as data update.

B. Insert Operation: The user may need to insert some data blocks into the cloud server dynamically. We ensure the dynamic insertion of data by uploading files required from the local host system.



C. Delete Operation: Sometimes, after being stored in the cloud, certain data blocks may need to be deleted. The delete operation we are considering is a general one, in which user replaces the data block with zero or some special reserved data symbol. From this point of view, the delete operation is actually a special case of the data update operation, where the original data blocks can be replaced with zeros or some predetermined special blocks.



CONCLUSION

The main purpose of this paper is to focus on the cloud security through the enhancement of TPA. The problem of ensuring data integrity is provided through auditing services by the third party auditor. The implementation of AES algorithm enables proper encryption and decryption of the user's data. We envision several possible directions for future research options on this area. The most promising one we believe in this model is that the TPA automatically updates whatever he has audited into the user's account directly. The dynamic operations over the user's data are carried out in an efficient manner.

REFERENCES

1. Amazon.com, 2008. "Amazon Web Services (AWS),"Online atttp://aws.amazon.com,
2. Gohring, N., 2008. "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html,
3. Juels, A., J. Burton and S. Kaliski, 2007. "PORs: Proofs of Retrievability forLarge Files," Proc. of CCS '07, 115: 584-597.
4. Shachamand, H. and B. Waters, Dec, 2008. "Compact Proofs of Retrievability," Proc.of Asiacrypt '08
5. Bowers, K.D., A. Juels and A. Oprea, 2008. Proofs of Retrievability: Theoryand Implementation," Cryptology ePrint Archive, Report 2008/175, http://eprint.iacr.org/.
6. Ateniese, G., R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, 2007. Provable Data Possession at Untrusted Stores," Proc. OfCCS '07, pp: 598-609.

7. Ateniese, G., R.D. Pietro, L.V. Mancini and G. Tsudik, 2008. Scalable andEfficient Provable Data Possession," Proc. Of SecureComm'08, pp: 1-10.
8. Schwarz, T.S.J. and E.L.Miller, 2006. "Store,\ Forget and Check: UsingAlgebraic Signatures to Check Remotely Administered Storage," Proc.of ICDC'06, pp: 12-12.
9. Lillibridge, M., S. Elnikety, A. Birrell, M. Burrows and M. Isard, 2003. A Cooperative Internet Backup Scheme," Proc. of the 2003. USENIXAnnual Technical Conference (General Track), pp: 29-41.
10. Bowers, K. D., A. Juels and A. Oprea, 2008. "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, http://eprint.iacr.org/.
11. Carter, L. and M.Wegman, 1979. Universal Hash Functions," Journal of Computer and System Sciences, 18(2): 143-154.
12. Hendricks, J., G. Ganger and M. Reiter, 2007. Verifying Distributed Erasure coded Data," Proc. 26th ACM Symposium on Principles of Distributed Computing, pp: 139-146.
13. Abou-Deif, M.H., M.A. Rashed, M.A.A.Sallam, E.A.H. Mostafa and W.A. Ramadan, 2013, Characterization of Twenty Wheat Varieties by ISSR Markers, Middle-East Journal of Scientific Research, 15(2): 168-175.
14. Kabiru Jinjiri Ringim, 2013. Understanding of Account Holder in Conventional Bank Toward Islamic Banking Products, Middle-East Journal of Scientific Research, 15(2): 176-183.
15. Muhammad Azam, Sallahuddin Hassan and Khairuzzaman, 2013. Corruption, Workers Remittances, Fdi and Economic Growth in Five South and South East Asian Countries: A Panel Data Approach Middle-East Journal of Scientific Research, 15(2): 184-190.
16. Sibghatullah Nasir, 2013. Microfinance in India: Contemporary Issues and Challenges, Middle-East Journal of Scientific Research, 15(2): 191-199.
17. Mueen Uddin, Asadullah Shah, Raed Alsaqour and Jamshed Memon, 2013. Measuring Efficiency of Tier Level Data Centers to Implement Green Energy Efficient Data Centers, Middle-East Journal of Scientific Research, 15(2): 200-207.