Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.84 – 87

RESEARCH ARTICLE

Verifying Integrity and Availability in Multi-Cloud Using PDP

Chandrasekaran Anand [1], Prabu.P [2], Roopan Prasath.V [3], Sasikumar.P [4], Silambarasan.P [5], Mr.P.Sivakumar [6]

[1, 2, 3, 4,5]Department of Computer Science and Engineering, Anna University Chennai, India
[6]Assistant Professor, Department Of Computer Science and Engineering, K.S.R. College Of Engineering, Tiruchengode, India

[1]callmeanand1991@gmail.com; [2]pan199004@gmail.com; [3]roopanprasath@gmail.com; [4]psasikumar14892@yahoo.com; [5]simbucse222@gmail.com; [6]sivakumarphd2013@gmail.com

Abstract— In this paper we are going to say an efficient technique that describes how integrity is maintained in storage of the data. We provide this by using the concept of Provable data possession which supports a good service and migration of data in a distributed cloud environment, where we take into account of multiple cloud service to store and also to maintain the data of the clients. We hereby deliver a new concept called cooperative provable data possession (CPDP) using hash index hierarchy and homomorphic verifiable response. Security of the system is proved based on a scheme zero-knowledge proof system. We use optimal parameters to improve the system performance efficiently and cost of computation for the client and cloud storage providers.

Key Terms: - Provable data possession; Multi- cloud; Cooperative; Parallel; Distributed

I. INTRODUCTION

In recent years parallel computing has emerged to solve the problems with a greater computational speed. It's operation is based upon the principle that larger problems can be reduced to a number of smaller ones, then which are solved concurrently("In Parallel").Parallel computing can be implemented in several ways of computing like instruction level, bit level, task and data parallelism. Based on the level at which hardware supports parallelism, it can be classified as multi-core and multi-processor.

Generally in a computer system a problem can be solved serially with a stream of instructions. Only one instruction is executed at a time, and then the other instructions are executed. On the other hand in parallel computing, uses multi-processing elements to solve a problem. This is accomplished by breaking the problem into independent parts so that each processing element can execute its part of the algorithm simultaneously with others. There is another important concept which is responsible for effective and efficient computation of our problem is, distributed system. Using high performance computers connected by equally high-speed communication links, it is possible to build a single system consisting of multiple computers and using it as a single consolidated system.

In a distributed system, the computers are not independent but interconnected by a high-speed network. Here are a few requirements for a distributed system;

Like security and reliability, consistency of replicated data, concurrent transactions, fault tolerance. The major aim of constructing a distributed system is that its behaviour should be transparent to the user. In a

distributed memory architecture if we take into account each processor has its own local memory and all the processing is done locally. All systems are interconnected through a LAN.

In any kind of system which involves data storage and retrieval, availability is one of the major security issues to be concerned. Provable Data Possession is such a technique which ensures data availability or proof of retrievability (POR); it's the proof which is provided for storage provider, in order to prove the ownership and integrity of client's data without being downloading it. The proof-checking of the data without being downloading is very important, especially when it comes to large sized data blocks. It is necessary because it is to be ensured that the data is not altered or deleted. PDP schemes are very useful when it comes to these kind of issues. However, this scheme will be effective only for single cloud storage, but not for the multi-cloud storage environment.

II. STRUCTURE AND TECHNIQUE

In a world that sees new technological trends bloom and fade on almost a daily basis, one new trend promises for a long time. This trend is called cloud computing. Cloud is a collection of computers and servers that are publically accessible via the internet. This hardware is typically owned and operated by a third party on a consolidated basis in one or more data center locations. There are many advantages of using cloud technology, for both developers and end users.

For developers, cloud computing provides increased amounts of storage and processing power to run the application they develop. Cloud computing also enables new ways to access the information, process and analyse data, and connect people and resources from any location anywhere in the world.

For end users, cloud computing offers more benefits. A person using a web-based application is not physically bound to a single PC, location, or network. His applications and documents can be accessed wherever he is and wherever he wants. Documents hosted in the cloud always exist, no matter what happens to the user's machine. And another benefit is group collaboration. Users from around the world can collaborate on the same documents, applications and projects, in real time.

Data protection technology was launched by cipher cloud in which tokenization and encryption of data is provided by a web proxy before sending the data to the cloud application. This technology does not have much effect on the application.

Another technology has been adopted known as okta that was designed to speed up the cloud applications by the integrating the cloud applications with that of the previous ones and this helps the users to quickly access the cross platforms.

A) Verification of Multi-Cloud Framework

Multi-cloud technique is the use of two or more cloud services to minimize the risk of large amount of data loss or temporary fault in the computers due to a localized component failure in a cloud computing environment. Such a failure may occur in hardware, software, or infrastructure.

A multi-cloud approach is also used to control the traffic from different customer bases or partners through the fastest possible parts of the network. Some clouds are better suited than others for a particular task.

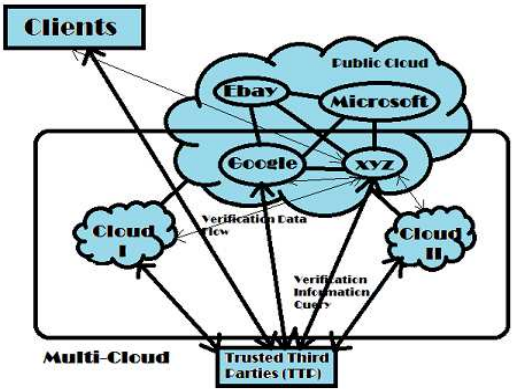

Figure I An illustration for multi-cloud working

B) Cooperative PDP

Based on zero knowledge proof system and interactive proof system we prove the integrity of data stored in a multi cloud. A CPDP is a collection of two algorithms (Key Gen, Tag Gen) and interactive proof system Proof.

- Key Gen: It takes a security parameter as an input and returns a secret key as output.
- Tag Gen: It takes a secret key, file and set of cloud storage providers as input and returns triples.
- |Proof: It is a protocol of proof of data possession between the CSP's and verifier.

Let H = { Hk } be a family of hash functions where Hk : $\{0,1\}^n \longrightarrow \{0,1\}^*$ index by k ε K. This algorithm has a benefit in breaking the collision resistance of H.

Collision-Resistance H: In this a hash family H(t, ε) collision resistant if no t-Time adversary has advantage atleast ε in breaking collision of H.

First the KeyGen algorithm is run in this scheme to obtain the public or the private key for users. Then TagGen is generated by the clients for the outsourced data.

C) Hash Index Hierarchy for CPDP

Three layers are used to illustrate the relationships among the blocks for stored resources .They are as follows:

1. Express Layer: it shows representation of stored resources.
2. Service Layer : it offers and manages cloud storage and services and
3. Storage Layer : realizes data storage on physical devices

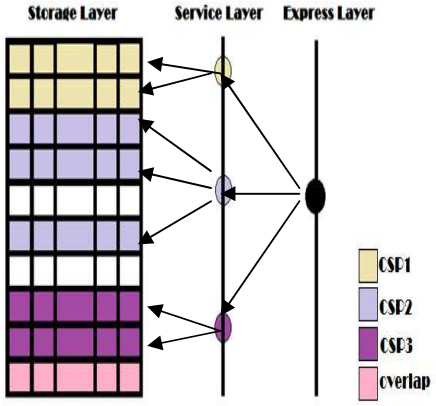

Figure II Representation of hash index hierarchy working

D) Homomorphic Verifiable Response for CPDP

A homomorphism is a map f : P $\longrightarrow$ Q between two groups such that f (g1+ g2) = f(g1) x f(g2) for all g1,g2 ε P, where + denotes the operation in P and x denotes the operation in Q.

Homomorphic verifiable response is the key technique of CPDP because it not only reduces the communication bandwidth, but also conceals the location of outsourced data in the distributed cloud storage environment.

III. CONCLUSIONS

With the techniques such as hash index hierarchy and homomorphism verifiable response, cooperative provable data possession concept has been achieved and hence integrity and availability is verified .The zero-knowledge proof system is used and hence increases the security so it can be used widely in public cloud services thereby increasing their performance. By this approach the computation time and cost is reduced. Our system can be used as a new method for data integrity verification in out sourcing data storage on multi-cloud environment.

In Future we would like to improve the performance of the cooperative provable data possession scheme for larger files since many complex operations take place at the same time. RSA based schemes have to be used to overcome these issues and we have to rectify the ones that are present in the existing systems so as to increase security.

REFERENCES

[1] YanZhu,Hongxin Hu,Gail-Joon Ahn,Senior Member,IEEE,Mengyang Yu "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage" IEEE Transactions on parallel and distributed systems.10.1109/TPDS.2012.66,PP 1-13.

[2] B. Sotomayor, R. S. Montero, I. M. Llorente, and 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," in 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., "Pors: proofs of retrievability for large files," in 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, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1–10.

[6] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, 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," in ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[8] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in 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," in 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. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in 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," in TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109–127.

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

[13] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, "Collaborative integrity verification in hybrid clouds," in IEEE Conference on the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom, Orlando, Florida, USA, October 15-18, 2011, pp. 197–206.

