Shakti Arora et al. International Journal of Institutional & Industrial Research ISSN: 2456-1274,
Vol. 1, Issue 1, Jan-April 2016, pp.15-17

Study of Integrity Based Algorithm in Decentralized Cloud Computing Environment

Shakti Arora, Surjeet Dalal

Department of CSE, SRM University, Haryana, India

***Abstract*- Cloud computing is getting popularity day by day especially in business people. Many of the people are getting attracted towards cloud computing services. It's very easy to mange and independent in terms of location and device. Mostly the business people are seeking the high security model keeping their information more secured and risk protected. Data availability is also an important aspect because our all operations will be performed online data that is placed on the cloud. Data is stored in distributed manner on the server and client does n't maintains the local copy of data so integrity of data becomes a more challenging factor. In this paper we will try to identify the issues and solutions to overcome the problem. This paper also contains find the latest techniques that are used to check the integrity of data with various different algorithms.**

Keywords— Cloud service provider, homomorphic integrity, Proof of knowledge, TPA

1. Introduction

From Several years cloud computing is gaining popularity. It's an Web based development and use of all computer resources over the web. Cloud computing provides a pool of computing services on a cheaper rate with powerful processor and data centres. Due to the dynamically increasing the network bandwidth and reliable flexible network connections user is getting a most convenient environment to subscribe high quality services of data and software that resides exclusively on data centres. Having the data on the cloud reduces the burden of direct hardware management and storing data directly on the cloud provides major benefits:

Relief of storage management

Universal data access with independent geographical locations

1) Avoidance of capital expenditure on hardware, software and personal maintenance

While we are having unarguable advantages of cloud computing, Dealing with cloud is separate administrative entity, the internal operational working of cloud service provider is totally hidden by the cloud users. The Distance between the user and provider put the correctness of the data at great risk due to the following reasons:

1) There is larger risk of internal and external threats in cloud computing due to larger infrastructure and computing resource than personal computing.
2) Cloud computing technology is totally adopted in terms of business and provider are dealing all the resources in terms of assets it could be hardware, software, storage or any type of services . So keeping your crucial data to that Cloud Service Provider could be challenging
3) Some of the CSP are selling their user information to marketing agencies for making their customer so it's also a great threat to our privacy.

Cloud Service provider may discard the storage which has not been or rarely accessed by the users without their knowledge just because of monetary benefits and reputations.

4) User is not aware about the location and sharing of data, his data is shared with which particular customer and stored inside which database.

5) For checking the audit ability of data on the cloud different integrated aspects need to be considered.

1) Integrity
2) Computation Integrity w.r.t. Time

The proposed work is going to examine the computation integrity of data that is outsourced from the local storage to decentralize servers on the clouds. In the reality the user no longer have physical access large size of outsourced data which makes the integrity protection in the cloud computing a very challenging and difficult task.

A trust is hard factor in cloud computing and when the distance between two parties increases chances of risk also increases proportionally. Cloud computing is critical due to the merging of different computing services and task on single point. All the assurances of users come in the form of availability and consistency of data every time. How much time is taken for retrieving the data as well as if any the damage occurs during operation with data over the cloud then what action has been taken to recover it. All these factors make the Trust factor high and increase the reliability over cloud.

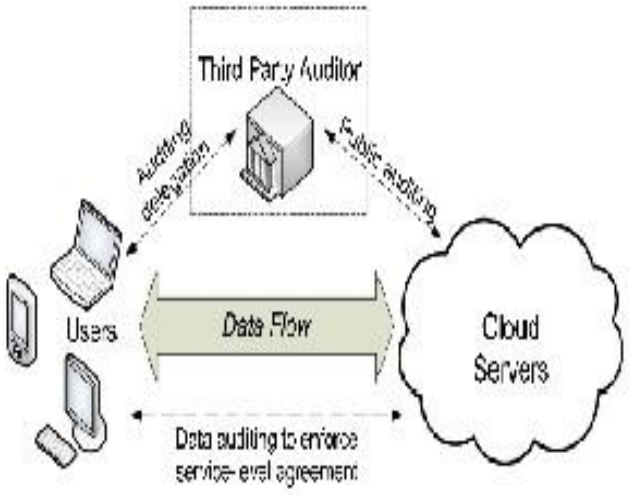

Fig 1 (Shows the location of TPA in cloud environment).

To fully ensure the data security and save the cloud computations, a concept of third part auditing was introduced. Different researchers have introduced different algorithms and techniques for implementing third party auditing more secure and reliable. With the TPA more functionality are added to outsourced data. TPA supports an external auditing of outsourced data on the cloud without having any knowledge about the data. TPA works an intermediate between the client and CSP over the cloud and check the security and availability of data at regular interval of times without making a burden over the Cloud Servers

2. Related Work

Initially, simple cryptographic algorithms and techniques were used to find the availability and integrity of data. These techniques were purely based on the hashing techniques and private signature. But the problem behind the older techniques was that it always requires the local copy of data for auditing. It was an unrealistic approach of auditing because we have to move the data from cloud server to client machine for verification and every time loading the data increases the computation cost and time.

To enable data integrity on a cloud the approach designed was TPA (third party auditor). TPA was aware about the SLA between the CSP and user. The main benefit of TPA was security was data because all of the auditing was done by the TPA without having any information about the data.

In [7] and [11] few special techniques for cryptography applied to keep the data secure were Homomorphic encryption and proof of reterivability as well as Provable data possession approaches.

In [4] Researchers found a way to cover the gap between the CSP and data owner more secured and authentic way of audit the data over the cloud by introduction of third party auditing schemes, it requires along bond of time ld be maintained by the user, CSP, and TPA. To keep the connection active for several years requires a lot of monitoring cost and complexity. Advantages of this scheme was that TPA can audit the without keeping a local copy of data. But the main problem was that TPA can collect the knowledge of the data and this could lead to data leakage problem.

In [3] introduced a privacy preserving technique for auditing the sourced data with less computation time. This technique works with less storage overhead and decreases the time of computation as well.

In [5] introduced the new models which can work with large file and can check the data integrity verification. This model generates the proof of the integrity in database and applies algorithms to check consistency every time. The main advantage that was found in this model was that it works for dynamic updations on the cloud.

For considering the public auditibility in [12], RSA based security algorithm was applied on the chunks of data for checking the authentication of outsourced data. Random sampling is done with sampling techniques for making a linear combination of data which could be passed to external auditor for verification. The basic problem with this technique was data leakage due to various samples data could be distributed and passed to any sample and no record of content was maintained and auditor could get the information of data.

Cloud architecture is based on distributed storage and computing so if we apply some technique at one place than at all of the places should be affected with same

In [8] explored the problem of data security in the distributed storage system over the cloud. In this paper an effective approach was found which was dynamically updating all of the instances of the data over the cloud as well as decreasing some computation time accordingly proposed an effective and competent distributed scheme with a precise dynamic support, counting block update, delete and append. All this was done to bring about the cloud assurance data integrity and availability

3. Proposed Model

We will try to focus the public auditing mechanism over the cloud and discuss the important issues which we generally face regarding the security of data on the cloud. A lot of algorithms with different security parameters are designed to check verification and availability of data .Our main goal is to design the algorithm that will provide the third party verification of data with dynamic nature often content and user needs. It will check the integrity after a short interval of time overall the virtual servers which are keeping the content and without having a knowledge about the content .This algorithm will run parallel on all the virtual servers as well as we will try to minimize the computation time of algorithm on all the servers

4. Conclusion

In this article, we analysed a different approaches to deal with the verification of data on the cloud. We studied a number of techniques to audit the data .previously few algorithms were designed to handle the data and maintain a local copy of the data which was on the cloud. We also faced storage over burden and computation costing by dealing with third party auditing algorithms. And finally we find out the latest problem which is handling all the auditing with Third party auditing mechanism in Dynamic updations of data on the cloud.

References

[1]. Subashini S, Kavitha V. "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*; Vol. 34, No.1, pp. 1-11,2011.

[2]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and dependable Storage Services in Cloud Computing, "*IEEE Transactions on Services computing*, Vol. 5, No. 2, pp.220-232, April-June 2012.

[3]. Wang. C, Chow. S, Wang, Q Ren, and Lou, W. " Privacy preserving public auditing for secure cloud storage*", IEEE Transaction*, Vol. 62,No.2, pp. 362-375 ,2013.

[4]. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest", *Proc. 11th USENIX Workshop Hot Topics in Operating Systems* , pp. 1-6,2007.

[5]. A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files", *Proc. 14th ACM Conf. Computer and Comm. Security, pp*. 584-597, 2007

[6]. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" This paper was presented as part of the main Technical Program at *IEEE INFOCOM*. vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[7]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of *ESORICS'09, Saint Malo, France*, Sep. 2009.

[8]. Ms. T .J. SALMA " A Flexible distributed storage integrity auditing mechanism in cloud computing, Information communication and embedded system,pp283-287 feb(2013)

[9]. M. Venkatesh. M. R. Sumalatha, Mr. C. Selvakumar "improving public audit ability, Data Possession in Data Storage for Cloud Computing", *ICITISF, pp* 463-467(2012).

[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/.

[11]. Patel Himani Atulkumar and Patel Srushti Hasmukhbha "Cloud Model-with TPA" , *IJREAT*, vol 1, ISSN: 2320 – 8791, 2013.

[12]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession", in Proc. of Secure Comm'08.NewYork, NY, USA: ACM, 2008, pp. 1–10.

.

