Open access Journal International Journal of Emerging Trends in Science and Technology

Preserving Consistency in Data Cloud Using Secure and Efficient Third Party Auditor

Authors
Greeshma M J[1], Jyothi Johnson[2]
[1]M.Tech in CSE, Marian Engineering College, Trivandrum
[2]Asst. Professor in CSE, Marian Engineering College, Trivandrum

Abstract
Cloud storage services have become very popular nowadays due to their immense advantages. To provide unique and updated always-on access, a cloud service provider (CSP) maintains multiple replicas for each piece of data on geographically distributed servers. The main problem of using the replication technique in clouds is that it is very expensive to maintain consistency among data. In this paper, a novel consistency as a service (CaaS) model is presented. It consists of a large data cloud and multiple small audit clouds. The audit cloud helps us to check whether consistency is maintained. In this model, a two-level auditing architecture is used, which only requires a loosely synchronized clock in the audit cloud. A heuristic auditing strategy is to be devised in order to reveal possible violations. In cloud, consistency influences the availability and performance of the system. To check the consistency, auditing is done where the data/report is evaluated to determine whether the cloud server safeguards the data, maintains consistency. The election of best suitable auditor for the auditing purpose will help improve in maintaining the consistency level of the data in the cloud.
Index Terms—*Cloud storage, consistency as a service (CaaS), two-level auditing, security, TPA.*

I. INTRODUCTION

Cloud computing has become more popular as it provides guaranteed services like data storage, virtualized infrastructure, simplicity, elasticity, high availability at low cost [1],[2] e.g. Amazon, SimpleDB etc. By using the cloud services, the customers or user can access data stored in a cloud anytime and at anywhere using any device, and customer ensure about less capital investment. To provide promised always on 24/7 access, the cloud service provider (CSP) stores data replicas on multiple geographically distributed servers. The main drawback of using the replication technique is it is very expensive to achieve strong consistency, and user is ensured to see the latest updates. Many CSPs (e.g., Amazon S3) provide only eventual i.e. updates are visible definitely but not immediately. E.g. Domain name system (DNS), but the eventual consistency is not interesting for all applications and which require strong consistency. Some applications like social networking sites require causal i.e. strong consistency. Thus the different applications require different level of consistency [3]. We propose novel consistency as a service (CAAS) model [6]. The CaaS model consists of, a large data cloud formed by CSP and multiple audit clouds formed by group of users worked on project or document that can check whether the data cloud provide a promised level of consistency or not. Two-level auditing structure which require only a loosely synchronized clock for ordering operation in an audit cloud then perform global auditing with a global trace of operations periodically an auditor is elected from an audit cloud. The problem with this work is that the auditor is elected with same probability from the cloud of audit. This does not provide the required level of efficiency in the auditing. The auditor is thus

elected based on the capability factor which measures the efficiency of the users with parameters like CPU utilization, memory and bandwidth. This will ensure that the auditor is elected efficiently based on the corresponding capability to maintain the consistency. Local auditing is concentrated on monotonic-read and read-your-write consistencies, which can be performed by an online light-weight algorithm while Global auditing focuses on causal consistency, in which construct a directed graph. If the constructed graph is a directed acyclic graph also called as precedence graph, we claim that causal consistency is preserved. In next sessions we will show how to preserve and attain consistency and security of cloud storage data.

II. CONSISTENCY OF CLOUD DATA THROUGH TWO LEVEL AUDITING

This section consist of three models i.e. consistency as a service (CaaS) model, user operation table (UOT) with which each user records his operations and two-level auditing structure.

2.1 Consistency as a Service (CAAS) Model

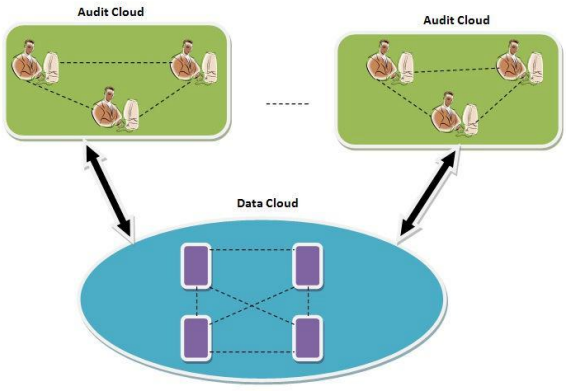

Figure 1: Consistency as a service model

An audit cloud consists of a group of users that work together on a job, e.g., a document or a program. We consider that each user in the audit cloud is identified by a unique ID. Before assigning job to the data cloud, an audit cloud and the data cloud will engage with a service level agreement (SLA), which demands the promised level of consistency should be provided by the data cloud. The audit cloud exists to verify whether the data cloud violates the SLA or not, and to analyze the severity of violations.

2.2 User Operation Table (UOT)

Each user maintains his own User Operation Table (UOT) for recording his trace of operations. Each record in the UOT is described by elements like Operation, logical vector, and physical vector. While issuing an operation, a user from an audit cloud will record his operation in UOT, as well as his current logical vector and physical vector. Each user will maintain a logical vector and a physical vector to track the logical and physical time when an operation happens, respectively.

2.3 Two-level auditing structure

Local Auditing: Each user independently performs local auditing with his UOT with two consistencies; Monotonic-read consistency, which requires that a user must read either a new value or same value Read-your-write consistency, which require a user, always read his latest update.

Global Auditing : Global auditing is performed by global trace of operations of all users operations with following consistency **Causal Consistency** Causal consistency writes that are causally related must be seen by all process in the same order and concurrent writes may be seen in a different order on different machine.

2.4 Heuristic Auditing Strategy

From the auditing process it is clear that only reads can display violations by their values. Therefore, the basic idea behind the heuristic auditing strategy (HAS) is to add exact reads for displaying as many violations as possible and call these additional reads as auditing reads. Under the CaaS model, consistency becomes a part of the Service Level Agreement and the users can get something from the CSP, by displaying consistency violations and determine the severity of the violations. The CaaS model will help both the CSP and the users adopt consistency as an important aspect of cloud services.

III. THIRD PARTY AUDITOR ELECTION

In the dual level auditing for checking the consistency of the cloud, an auditor is elected plainly from the cloud of auditors, where each and every user has the same probability to become an auditor. Whereas different users have a distinct ability with regards to availability of bandwidth, CPU utilization, storage. This auditor election can be done using the method of capability factor where each user has a unique ID. A table is constructed with ID number assigned to each and every user based on their efficiency. The user with least CPU utilization will be assigned the highest value and most utilization, the smallest. Based on this numbering the user with the most efficiency of all three factors will be elected as the auditor. For example, in the below table given (Table 1), user 3 has least CPU utilization, in the scenarios where users with least CPU utilization is required user 3 is elected as the auditor. Likewise, high band width scenario elects user 2 as the auditor and user 3 for high memory storage.

Table 1: Capability Factor

Parameters	Auditor		
	User 1	User 2	User 3
CPU Utilization	4.3	2.4	2
Bandwidth	2.5	4.4	2
Memory Storage	3.5	1.8	3

IV. SECURE STORAGE OF CLOUD DATA THROUGH THIRD PARTY AUDITOR

Cloud storage helps to store data remotely and it also provides the availability of the data 24/7 when it is demanded independent of hardware and software burdens. Organization use cloud as per their need for service like SaaS, Paas or IaaS and also use different deployment model as per the need like private, public, hybrid, community .When we store data in cloud the main issue we face is of security. The data should be secure so that it should not be accessible by any unauthorized parties and it should provide integrity for the data that are stored.

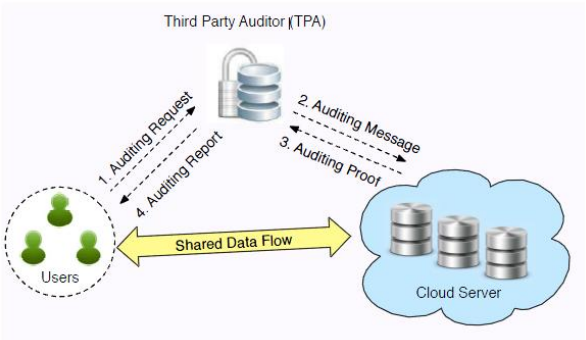

Figure 2: Cloud storage service architecture

Figure 2 shows the sample network architecture for cloud service architecture. In this

Users: Represent an entity that needs to store data in the cloud and it can be an enterprise or an organization.

Cloud Server (CS): The entity which is managed by the cloud service provider (CSP) for the data storage and future on demand accessing.

Third Party Auditor (TPA): On behalf of user request TPA will decide whether to trust the request or not. TPA will provide the blocking of unauthorized user access to the cloud storage.

The third party auditor is responsible for the security of the data stored in the cloud storage. The global auditor that provides consistency can also act as the TPA [4] for providing security for the data. TPA [5] will pass token to the cloud in encrypted form using RSA algorithm so that the token can't be decrypted by any other unauthorized users. Only authenticated user knows the key to decrypt the token and access the data. Data updating like deletion, appending and insertion of data can also be managed and controlled by TPA. It will help the server from intruder from attacking the server. It will also provide the consistency of the data. Third party doesn't know the secret binding key so there is no way the third party to read or analyze the data while auditing thus privacy preserving is TPA is achieved.

V. CONCLUSION

In this paper, we presented a consistency as a service (CaaS) model and a two-level auditing structure that helps users to verify whether the cloud service provider (CSP) is providing the promised consistency, and to quantify the severity of the violations, if any. With the CaaS model, the users can assess the quality of cloud services and choose a right CSP among various candidates, e.g., the least expensive one that still provides adequate consistency for the users' applications. Auditing is done, where the data/report is evaluated to determine whether the cloud server safeguards the data, maintains consistency. The election of best suitable audit for the auditing purpose will help to rectify the errors caused in the auditor procedure and thus indirectly helps in maintaining the consistency of the data in the cloud server. Security is achieved by implementing TPA to the same global auditor. Token passing method is also proposed to preserve the privacy of data from the TPA.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., "A view of cloud computing," Commun.ACM, vol. 53, no. 4, 2010.
2. P. Mell and T. Grance,"The NIST definition of cloud computing (draft)," NIST Special Publication 800-145 (Draft), 2011.
3. M.Ahamad, G. Neiger, J. Burns, P. Kohli, and P.Hutto, "Causal memory: definitions, implementation, and programming," Distributed Computing, vol. 9, no. 1, 1995.
4. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010.
5. C. 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.
6. in Liu, Guojun Wang, IEEE, Member, and Jie Wu, IEEE Fellow "Consistency as a service: Auditing cloud consistency", IEEE Vol 11 No.1, July 2014.