International Journal of Engineering Research and General Science Volume 4, Issue 4, July-August, 2016
ISSN 2091-2730

Consistency and Integrity as a Service in Auditing Cloud

Shwetha J, Prof. (Dr.) D. Nageswara Rao

[1]KVM College of Engineering and IT,CUSAT University,
Cherthala-688583, Alapppuzha, Kerala
Shwethajayachandran81@gmail.com

[2]KVM College of Engineering and IT,CUSAT University,
Cherthala-688583, Alapppuzha, Kerala
dronamraju8@gmail.com

Abstract— For enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources can be rapidly provisioned and released with very minimum effort, cloud computing is just a model for it. Cloud service provider maintains a multiple copies of each data in different geographical area, but this replication technique is highly expensive to achieve consistency and integrity on a worldwide. In this paper, we present a model which consist of data cloud and audit cloud. Cloud service provider maintains the data cloud and huge group of users constitute an audit cloud. Users are of two types, global and local users. The consistency is provided to the audit cloud using global auditing and local auditing algorithm. Integrity checking is allowed only for global users for checking whether the local users try to access any unauthorized data or not by using SHA algorithm.

Keywords— Data storage, Service model, local and global auditing algorithm, AES, SHA algorithm.

INTRODUCTION

Cloud computing is a term used to describe a new class of network based computing that takes place over the internet, basically a step on from utility Computing. The platform provides on demand services on rental basis that are always on, anywhere, anytime and anyplace. . e.g., Amazon is the best example for cloud storage; here all that we need is a Credit card. And also should be a registered member. Like every storage (laptops, mobile phone etc.) has a capacity, cloud used to provide a server according to the storage needs. Hardware and software services are available to general public, enterprises, corporations and business markets. Cloud service provider maintains a multiple replicas of each piece of data on geographically distributed servers. But it is very expensive to achieve consistency and integrity on a worldwide. For eliminating the limitation, we present a paper about a service model which consist of data cloud and audit cloud. Data cloud is maintained by cloud service provider and audit cloud contains a group of users, who can verify whether the data cloud provides a surety in consistency and integrity. To decrease the threat of data, integrity is a major issue. The purpose of data security protection cannot be adopted only due to the user's loss control of data under cloud computing. We need authentication of correct data storage in a cloud without explicit knowledge of whole data by considering various kinds of data for each user that are registered in the cloud. The verification of data in a cloud is a more challenging factor

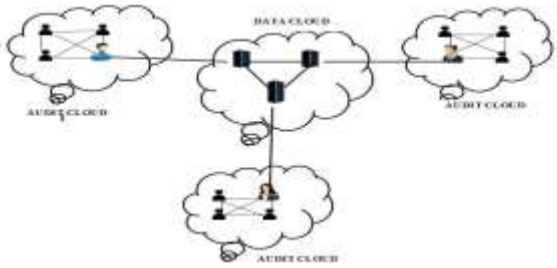


Figure 1: Service model in cloud

Fig.1. shows the service model in cloud, contains group of audit clouds and group of data clouds. Each server is maintained by an administrator by checking the integrity. Admin can create two types of account, global users and local users. Global user will get equal power like admin. Every user has a unique ID.

If suppose consider a company X have different branches in different places. Each group of users assigned a job. For the co-operation, they need to interact with different users and to access different data in other severs. Then in this cloud computing model, consistency and integrity is a key factor**.**

1. SERVICE MODELS IN CLOUD COMPUTING:

Cloud storage services become commercially popular due to its various advantages such as scalability, elasticity and high availability at low cost. The cloud service provider (CSP) offered various kinds of services and tools which are given below:

A. SOFTWARE AS A SERVICE:

By All users are geographically distributed by using cloud infrastructure and cloud platforms to the various customers with software applications.

B. INFRASTRUCTURE AS A SERVICE:

Registered member is allowed to access the physical computing hardware such as data storage, CPU, memory and network connectivity of the service provider etc. Server itself acts as virtual server. Any type of system i.e., Windows, Linux etc. should be compatible. The user gain greater flexibility in access to basic infrastructure.

C. PLATFORM AS A SERVICE:

It enables customers to use the cloud infrastructure as a service. Development of web application and others software can be controlled by users. Cloud SIM is a best example.

D. CONSISTENCY AS A SERVICE MODEL:

Distributed server maintains replicas of data of improve response time and avoid data loss in case of failures. The performance and the availability of data in the case of network partitioning are enabled by ensuring data consistency eventually but it won't work out all the times. Suppose for example, Alice, Bob and Clarks are global users working in different branches (different locations). If Alice updates a new version of a project and upload it to the cloud server. Then Alice calls the Bob and Clarks to download the latest version that she updated. But if the casual consistency is not there, then Bob and Clark try to download the project will get only the old version. Then the consistency is a major factor. Basically different applications need different consistency requirements. We are here to present model consisting of group of data cloud and audit cloud. In this virtualization technique, it is very hard for the user to find whether the data in a data cloud is latest one or not. For the solution, we need to trace the interaction among users. For the tracing operation, local auditing algorithm is used for local users and global auditing is used for the global users.

E. INTEGRITY AS SERVICE MODEL:

User interaction is a vital factor for an every organisation. For the completion of a particular work, sometimes employees need to send file or any project to other employee who is working in same company but different location in a cloud. Such a cases the company head need to check whether the user are sharing correct file or not. Otherwise it will affect the growth of the organisation. So admin need to trace the file the users are sharing. So we are providing a integrity checking with the help of SHA algorithm. Auditing cloud consist of two types of users, Global and Local users. Global users check the file that shared by local users.

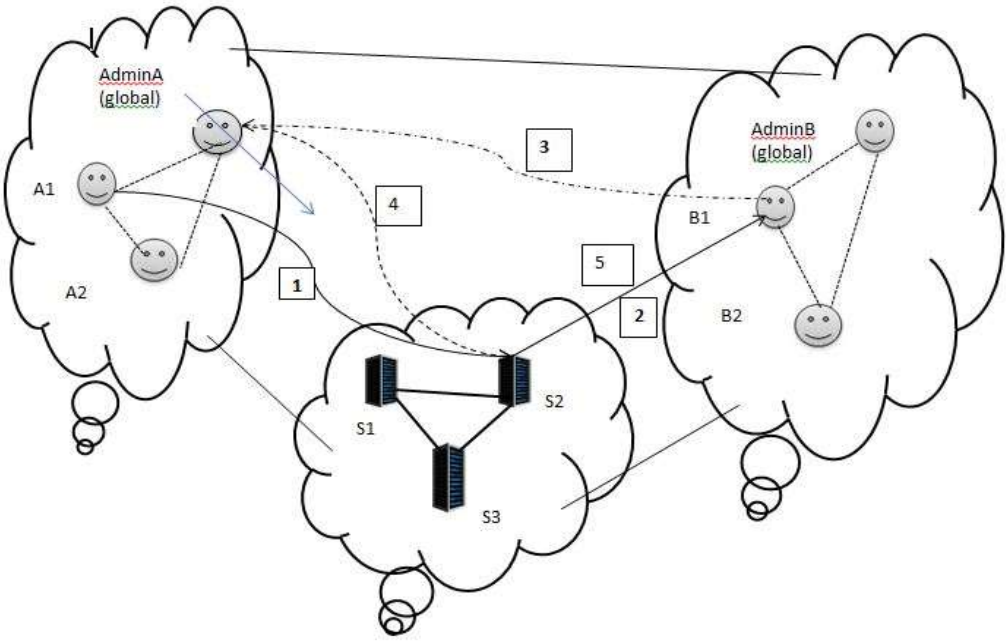


Fig2: Integrity Checking

Fig 2 shows the diagrammatic representation of integrity checking. The models contain group of audit cloud and data cloud. Admin A is a global user of one audit cloud and Admin B is the global user of other audit cloud. Each audit cloud contain local users (A1, A2, B1, B2). The expansion of above fig 2 as follows:

1. A1, local user of an audit cloud who located in S1 send file to the B1, local user of audit cloud located in S2.
2. B1 who located in S2 received the file.
3. AdminA, global user of sender side can view the confidential file sent to the B1
4. AdminA delete/ view/ update the same file.
5. B1 ‘s file should be replaced by AdminA’s action.

Algorithms used are:

1. AES - For Data Encryption and Decryption.

2. Sha1 - Secure Hash Algorithm

3. Local consistency auditing - For auditing local consistency - attackers while accessing file and checking read or write.

The Secure Hash Algorithm (SHA) developed by the National Institute of Standards and Technology (NIST) . This algorithm takes as input message with maximum length of less than 2^128 bits and produces as output a 512-bit message digest. It is used for secure exchange of data and messages.

2. IMPLEMENTATION:

In this section, we first illustrate the consistency as a service model. Then, we describe the structure of the user operation table (UOT), with which each user records his operations. Then we apply auditing algorithms.

A. USER OPERATION TABLE:

User operation table is used to maintain a UOT for the operation to record all the local operation in a systematic manner. Each present record in UOT will be shown by three components. First is an operation which consists of sender and receiver id, next is the current logical vector means the number of message received by receiver’s inbox and finally the current physical vector which means the total number of message received in a complete table. Consider ‘op’ be the operation, where W(K,a) be the writing the value a to data which is identified by key K and R(K,a) stands for reading data which is identified by K. Let us consider W(K,a) as R(K,a)’s dictating write and R(k,a) as W(k,a)’s detected read. Following are the properties:

a. A read must have unique dictating write.
b. A write must have either zero or more detected reads.

When an each operation happens each user will track logical and physical time to maintain logical vector and physical vector respectively. Suppose that there are N users in the audit cloud. A logical/physical vector is a vector of N logical/physical clocks, one clock per user, sorted in ascending order of user ID. For a user with IDi where $1 \leq i \leq N$, his logical vector is < L1,L2,...,LN >, where Li is his logical clock, and Lj is the latest logical clock of user j and his physical vector is <P1,P2,...,PN >, where Pi is his physical clock, and Pj is the latest physical clock of user j.

B. LOCAL AUDITING TECHNIQUE:

Local consistency auditing technique is an online algorithm. The operation in this module or unit, in which each user is going to record all his complete activities and store in his UOT. During the read operation, the authorized user is going to perform local consistency operation in an independent manner.

Algorithm:

Step 1: initially user operation table with null while issue an operation op do

Step 2: if op = w(a) then record w(a) in user operation table

Step 3: if op = r(a) then w(b) Belongs to user operation table is the last write

Step 4: if w(a) -> w(b) then read your write consistency is violated r(c) belongs to user operation table is the last read

Step 5: if w(a) -> w(c) then monotonic consistency is violated

Step 6: record r(a) in user operation table

C. GLOBAL AUDITING TECHNIQUE:

Global consistency auditing technique is going be considered as an offline algorithm. Next to consider is that an auditor periodically will be selected from the audit cloud system to perform the special operation like global consistency auditing technique. Hence in this case the auditor is going to collect all users' UOTs for obtaining a special global trace of all activities. Then later executing global auditing technique, selected auditor is going to send results of auditing operation as well as its vectors values to all other authorized users. Now given the auditor's vector values, then each user will come to know other users' new clocks up to next global auditing**.**

Algorithm:

Step 1: for every operation in the global trace is represent by a vertex

Step 2: for operation op1 and op2 do

Step 3: if op1->op2 Then time edge is added between op1 and op2

Step 4: if op1=w(a),op2=r(a) op1 and op2 comes from different user then data edge is inserted between op1 and op2

Step 5: if op1=w(a) and op=(b) and op1 and op2 comes from different users and w(a)->w(b)->r(b) then causal edge is inserted between op1 and op2

Step 6: verify whether the graph is directed acyclic graph using topological sorting method .

D. INTEGRITY CHECKING:

The steps are:

Step 1: The sender first encrypts the data using encryption using shared key.

Step 2: Then the message digest is created using SHA-1 algorithm, D=h (M').

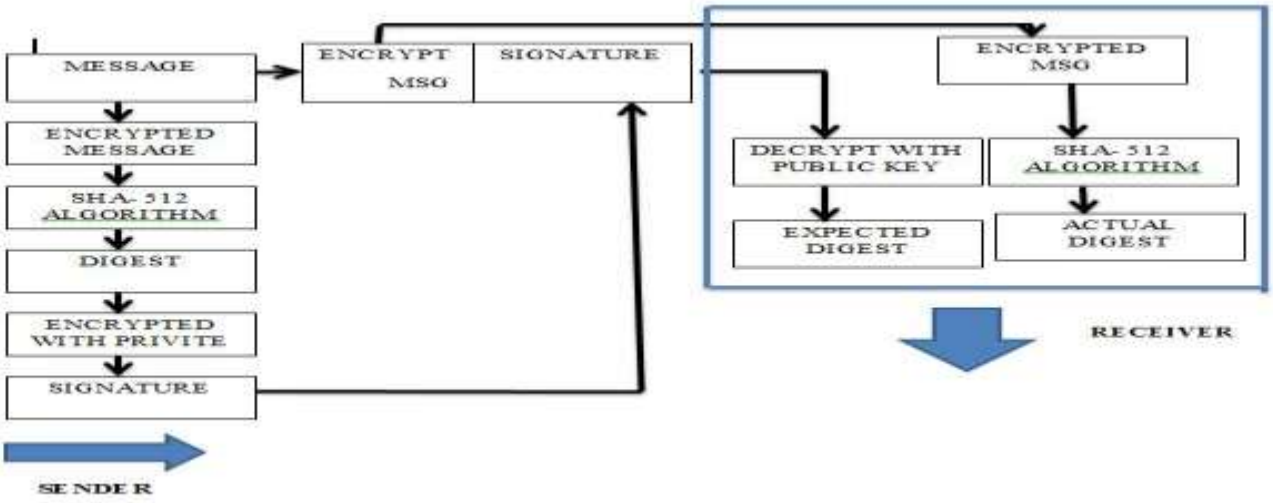
Step 3: Then the message is signed=D^d mod n.

Step 4: Then the encrypted message and signature is sent to the cloud service provider.

Step 5: Then CSP uses the receiver's private key on the signature to retrieve the digest, D'=S^e mod n.

Step 6: It applies the hash algorithm on the encrypted data to get the digest D.

Step 7: CSP now compares the two digests D and D'. If they are not equal, it posts the user that the data in the cloud is modified. Otherwise the message is accepted.



3. SAMPLE RESULTS:

STORAGE 1		
User Id	**User**	**Privilege**
1	Alice	Global
2	X	Local

Table1: User table of storage1

STORAGE 2		
User Id	**User**	**Privilege**
14	Bob	Global
15	Y	Local

Table2: User table of storage2

STORAGE 3		
User Id	**User**	**Privilege**
25	Clark	Global
26	Z	Local

Table3: User table of storage3

ALICE'S CONSISTENCY TABLE			
Sender	**Receiver**	**Logical Vector**	**Physical Vector**
1	14	5	10

Table4: Consistency table of Alice

BOB'S CONSISTENCY TABLE			
Sender	**Receiver**	**Logical Vector**	**Physical Vector**
14	25	6	9

Table4: Consistency table of Bob

CLARK'S CONSISTENCY TABLE			
Sender	**Receiver**	**Logical Vector**	**Physical Vector**
25	1	3	4

Table5: Consistency table of Clark

Above table1, table2, and table3 are the users table in three different storages. Table3 shows Consistency table of storage1 which means Alice be the sender and Bob be the receiver, and which contains corresponding logical vector and physical vector. Logical vector is the total number of message received for the receiver in his message table and total number of message received in message table of receiver's storage is its Physical vector. From table1 Alice sends message to Bob, Its logical vector is 5 and its physical vector is 10. Similarly table4 and table5 are defined.

CONCLUSION

The consistency is provided to the audit cloud using global auditing and local auditing algorithm. From this study we can conclude that the consistency service model is going to maintained by the system, and also we have come across a two levels of auditing structure technique. This technique helps the user to checks whether cloud service provider also called as CSP is going to provide a valid consistency operation or not. And in this system the user also can understand which Cloud Service Provider genuine service provider from the other different Cloud service provider. . Integrity checking is allowed only for global users for checking whether the local users try to access any unauthorized data or not by using SHA algorithm.

REFERENCES:

[1] E. Brewer, "Towards robust distributed systems," in Proc. 2000 ACM PODC.

[2] Garima, "Ensuring data storage security in cloud using two way integrity check algorithm" ,International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 11, November-2013

[3] Kapila Sharma, Kavita Kanwar, Chanderjeet Yadav, "Data Storage Security in Cloud Computing", International Journal of Computer Science and Management Research, Volume 2 Issue 1 January 2013

[4] M. Ahamad, G. Neiger, J. Burns, P. Kohli, and P. Hutto, "Causal memory: definitions, implementation, and programming," Distributed Computing, vol. 9, no. 1, 1995

[5] 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.

[6] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST Special Publication 800-145 (Draft), 2011.

[7] "Pushing the CAP: strategies for consistency and availability," Computer, vol. 45, no. 2, 2012.

[8] Qin Liu, Guojun Wang, IEEE, Member, and Jie Wu, IEEE Fellow "Consistency as a Service: Auditing Cloud Consistency", IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT VOL:11 NO:1 YEAR 2014

[9] Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo Yan, "Mona: secure multi-owner data sharing for dynamic groups in the cloud" , IEEE transactions on parallel and distributed system, Volume 24, NO. 6, June- 2013