Enhanced Security Framework for Data Integrity Using Third-party Auditing in the Cloud System

Balamurugan Balusamy, P. Venkatakrishna, Abinaya Vaidhyanathan, Meenakshi Ravikumar and Nirmala Devi Munisamy

Abstract Cloud computing is an evolving paradigm that has been resulted as an adoption of available technologies. Although cloud technology allows users to take more benefits from available infrastructures, and virtualization, which is an enabling technology provided by the cloud allows users to manage and use the resources in an efficient and easiest manner, it does not guarantee data integrity and security over the resources stored in the cloud. Though many security frameworks have been developed for the cloud, still there may be loss of data or loss of control over data uploaded into the cloud. And also, many solutions for data integrity by third-party auditor are available but they are semi-trustable, if third-party auditors (TPA) compromise unauthorized access over the resource in the cloud. Hence, our proposed scheme focuses on extended framework that guarantees data integrity by involving data owner to perform auditing on the outsourced data in the cloud. And so, our proposed scheme achieves data integrity and guarantees security to the data owners for their resource in the cloud to major extent. Therefore, this type of TPA approach creates awareness to the data owner of their resource and thereby guarantees data integrity for every resources stored in the cloud.

Keywords Cloud service provider · Data integrity · Third-party auditor

B. Balusamy (✉) · P. Venkatakrishna · A. Vaidhyanathan · M. Ravikumar
N. Devi Munisamy
VIT University, Vellore, India
e-mail: balamuruganb@vit.ac.in

P. Venkatakrishna
e-mail: pvenkakrishna@vit.ac.in

A. Vaidhyanathan
e-mail: abinaya.v2010@vit.ac.in

M. Ravikumar
e-mail: meenakshi.r2010@vit.ac.in

N. Devi Munisamy
e-mail: nirmaladevi.m2010@vit.ac.in

L.P. Suresh et al. (eds.), *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, Advances in Intelligent Systems and Computing 325,
DOI 10.1007/978-81-322-2135-7_4

1 Introduction

Cloud computing is a technology that is growing tremendously in our competitive world. Cloud computing generally provides easy way in tracking the data's of users whenever and wherever possible. Mostly people think the security of the cloud is not as secure as possible because of this reason [1]. Therefore, auditing of the data's stored in the cloud is done by the third-party auditors (TPA) [2] who are assigned confidentially by the cloud service providers (CSPs). Many insecure actions or incidents make cloud users to think more in auditing the cloud data storage [3]. The TPA may turn out to be a malicious user and can hack the cloud data or some critical applications stored in the cloud at the time of auditing.

The TPA are the persons who are extravagant in all process and have the skill of auditing process. These people generally checks out each and every process the user does and maintains a log that represents date, time and name of the files, the user accessed, and mode of the file that has been provided to the users. The TPA make many levels of auditing that ensures the current progress of the users of the cloud and the data owner of the files are in correct stage. Not only other malicious users but also the TPA [4] who are actually tied up with the CSP may also be induced by some malicious thoughts that make them to do unwanted auditing process and produce always good results. These reasons are made as the stepping stone for introducing the verification technique of the auditing process done by TPA. The verification technique is implemented by notifying the data owners about the file access information and makes sure the correctness of the auditing log. Hence, the need for the involvement of the data owners is inevitable (Table 1).

If the user does not opens his/her account frequently, then the files uploaded by them may be insecure. The auditing process [5] will be carried out generally, and the notifications are sent. In case if the notification is not appropriate to the user's expectation, then he/she does not accept the auditing process done by the TPA and verifies the auditing process. He/she may verify the whole process or the part of the process that needs verification. User can ask them to redo the auditing process (rare occasions). If the data owner needs to know the progress or present status of his account suddenly when they are in need, then he/she can request for an audit. The network problem is another issue that makes the user feel uncomfortable and insecure in using the cloud.

Table 1 Verification technique

Period of time (time interval)	T
Files	F
Medium of data storage	M
Log	L

2 Related Works

In Marshal [6], "Secure Audit Service By Using TPA for Data Integrity in Cloud System," they explained their proposed scheme through four major modules such as audit service system. This explains about security that is designed with cryptographic method and also proves the soundness property and zero knowledge property. Second module is about data storage [7] service system, and they considered four entities to store the data. Third module is an audit-outsourcing service system uses the secret key to process the file. And the last module is about secure and performance analysis which verifies the correctness of cloud data on demand hence in such a way they are allocating the security requirements to the file [8]. This scheme involves minimum overhead with correctness of the system. In Vinaya and Sumathi [9], "Implementation of Effective Third Party Auditing for Data Security in Cloud," they proposed a scheme that is an enhancement of data integrity concept [10]. Here, integrity is guaranteed by measuring correctness of the system. This work verifies correctness of the data on the cloud without retrieving complete copy of the file, and it is proven with the help of service-level agreement (SLA). In this paper, integrity is verified by developing hash code by the server and sends back the file name and a signature from the hash code. TPA in return takes an old signature back from TPA database and checks the equality between the two signatures. And this is again assured by SLA. In Xu [11], "Auditing the Auditor: Secure Delegation of auditing operation over cloud storage," they defined about the audit protocol that explains with three phases such as release plan, execute plan, and review plan. And, in release plan data owner selects an audit plan. In the execute plan, TPA sends the request to CSP and reply to the request in the specified time interval. Review plan verifies whether the request has been executed in particular time interval. And other module known as time secured that involves two processes are backward-timed secure and forward-timed secure. In backward process, TPA performs audit within a time interval; if exists, it will reject in the review plan. In forward process, TPA performs audit process and checks the request after the time interval; this will take place in review plan. This whole work goes in such a way that all above plan will be performed sequentially. First phase is a set up in which it produces the secret key pair of (pk,sk) which is used to divide the files into block and encrypt the file. Next phase is the release plan phase that chooses the time for audit plan. And, in the execute plan phase, message is decrypted using the secret key. Review plan phase finally retrieves the message from receiver (Fig. 1).

3 Proposed Work

Usage of TPA scheme guarantees the data integrity, which allows data owner to audit the resource in the cloud. Framework includes auditing by data owner/client, notifications for the resource access, and validating time complexity for resource.

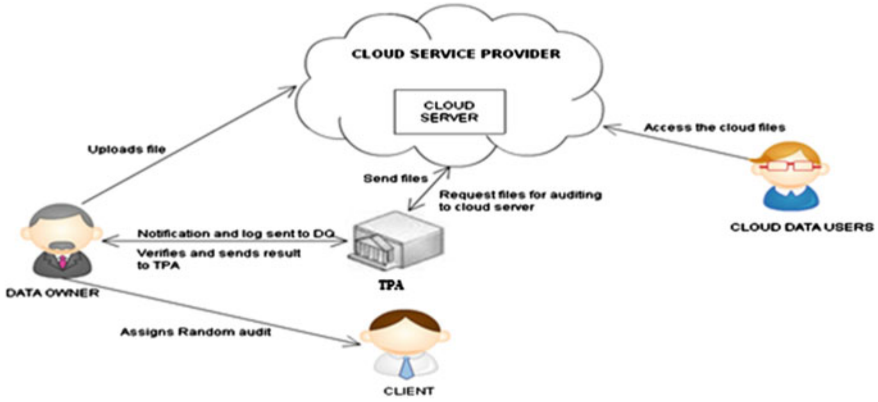

Fig. 1 Architecture of third-party auditing

3.1 Auditing by Data Owner/Client

Data integrity has been achieved by the usage of TPA scheme, in which allowing TPA to audit the outsourced data in the cloud. Auditing process is done on the resource by TPA using resource information provided by the CSP. Data owners are provided with notifications that when his/her resource has been accessed by users, and hence, data owners are aware of the resource and thus provides resource integrity. Thereby, data owners validate the notifications and log report generated by the normal auditing process with the resource list available with the data owners, and hence, data integrity is achieved. If data owner found that the notifications have some error with his/her resource status database, then "surprise auditing" is performed by the data owner or client employed by the data owner to audit the resource in the cloud. Hence, data owner can able to track an unauthorized access to the resource by notification provided with him.

3.2 Notifications for the Resource Access

Notification scheme involves issuing notifications to the data owner when his/her resource has been accessed by cloud users. This methodology is used to create awareness to the data owner with the status of his/her resource. Hence, this technique is used to inform data owner with resource status information that helps him to verify integrity of that particular resource in the cloud. This helps data owner to track an unauthorized access over the resource with the user details and system information (Fig. 2).

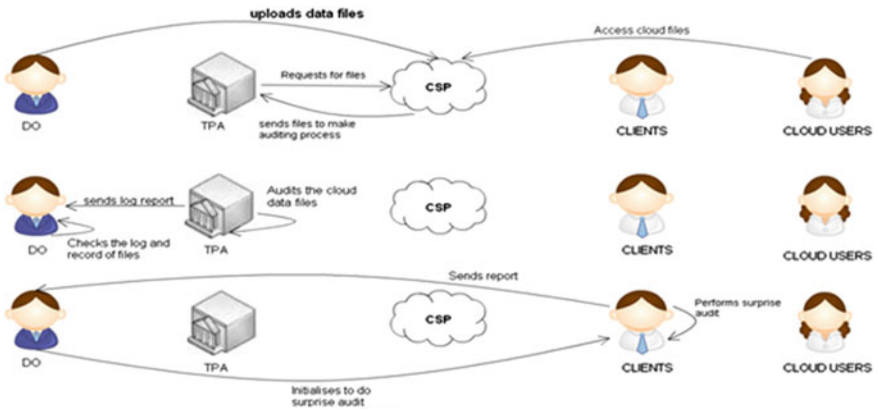

Fig. 2 Overall system architecture

3.3 *Validating Time Complexity for Resource*

For every critical resources in the cloud, “threshold value” is assumed or calculated by the data owner based on the random time generation technique and every critical resource has been validated by verifying response time with the time lesser than threshold value assigned to the resource. If response time to the data owner exceeds, then threshold value helps data owner to perform surprise auditing over the resource in the cloud. Hence, integrity has been achieved by validating the time complexity and medium of storage complexity [12] over that resource. Since response time to the users depends upon the storage medium by which the resource has been stored in the CSP, thereby, data owners are able to find the storage medium of his/her critical resources in the cloud.

4 Validation

Validating audit process models include the following steps:

Step 1: **Request initialization and response verification**

This step is to ensure that TPA sends request to CSP to get an essential information needed to perform auditing by appropriate period. And to ensure that the response given by CSP matches with the resource details available with the data owner.

Step 2: **Report examination**

To inspect an audit report or audit log generated by CSP and compare with the notifications provided with data owner to validate the exact status of the resource.

Step 3: **Resource scheduling**

To check the response time and storage medium of any critical resource by finalizing time and resource scheduling with an employed client or data owner.

Step 4: **Follow-up**

Employing third-party cloud users for managing and verifying closure audit verification.

Audit process is validated by,

$$\text{Val\_Flag} = \sum_{(i=1)}^{n} \left(\left(\text{TPA}_{\text{log}_{\text{report}}}\right)\right).\left(\text{DO}_{\text{notifications}}\right).\left(\text{surprise}_{\text{audit}_{\text{report}}}\right)$$

where

n number of resources of data owner.

i ‘i’th number of resource that goes for auditing

DO data owner.

Case 1 *Val_Flag is true, if*

(i) Log report generated by TPA matches with the resource status database of data owner (DO).

(ii) Notifications provided to data owner matches with the list of resource access list.

(iii) Surprise audit report generated by client or data owner matches with the available resource database contents.

Case 2 *Val_Flag is false, if*

(i) Log report generated by TPA does not match with the resource status database of data owner (DO).

(ii) Notifications provided to data owner does not match with the list of resource access list.

(iii) Surprise audit report generated by client or data owner does not match with the available resource database contents.

5 Conclusion and Future Work

This paper focuses on auditing process of the resource in the cloud. Our proposed scheme also involves data owner/client to audit the resource. This helps to reduce the problem that occurs in the auditing process. This technique also helps us to make data owner to feel secured about their resources. Thus, security is achieved through this activity. Also, this process promises data owner that their resources are stored in safer place. Thus, reduces misplace of file that are stored in a particular location. Finally, our work has some extravagant properties like proving the security, reduces the overhead through the client, and also achieves the integrity.

References

1. G. Roopa, S. Manjunath, Secure way of storing data in cloud using third party auditor. IOSR J. Comput. Eng. (IOSR-JCE) **12**(4), 69–74 (2013)
2. L. Li, L. Xu, J. Li, C. Zhang, Study on the third-party audit in cloud storage service, in *International Conference on Cloud and Service Computing* (2011)
3. C. Wang, S.S.M. Chow, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for secure cloud storage. IEEE Trans. Comput. **62**(2), 362–375 (2013)
4. G. Delong, Use of Third Party Audit to Verify Sources from Farm to Supplier
5. U. Vijayaraghavan, R.M. Arieth, K. Geethanjali, Proof of retrievability: a third party auditor using cloud computing. Int. J. Emerg. Technol. Adv. Eng. ISO 9001:2008 Certified J. **3**(7) (2013)
6. S.V. Marshal, Secure audit service by using TPA for data integrity in cloud system. Int. J. Innovative Technol. Exploring Eng. (IJITEE) **3**(4) (2013)
7. S. Han, J. Xing, Ensuring data storage security through a novel third party auditor scheme in cloud computing, in *Proceedings of IEEE CCIS* (2011)
8. M. Hussain, H. Abdulsalam, SECaaS: security as a service for cloud-based applications
9. V. Vinaya, P. Sumathi, Implementation of effective third party auditing for data security in cloud. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **3**(5) (2013)
10. T.J. Salma, A flexible distributed storage integrity auditing mechanism in cloud computing
11. J. Xu, *Auditing the Auditor: Secure Delegation of Auditing Operation Over Cloud Storage* (National University of Singapore, Singapore)
12. L.D. Dhinesh Babu, P. Venkata Krishna, Versatile time-cost algorithm (VTCA) for scheduling non-preemptive tasks of time critical workflows in cloud computing systems. Int. J. Commun. Netw. Distrib. Syst. **11**(4), 390–411 (2013)