International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 3 (May-June, 2016), PP. 101-105

CLOUD INFORMATION ACCOUNTABILITY IN CLOUD COMPUTING

[1]Sailendra S L, [2]Arun Kumar Sangaiah
School of Computing Science and Engineering, VIT University, Vellore, India
slsailendra@gmail.com

Abstract— **Cloud computing has accomplished success by providing services whenever required and its cost is according to the use of service. Denial of service attacks are a critical threat to the internet. These attacks mainly lead to the improper functioning and degrading of quality of service. This shows more effect on online services and web applications. These attacks may cause failure for several services and it directly effects the service cost. To avoid the extra service cost caused by these attacks, care should be taken to identify these attacks as early as possible. In this paper a framework is proposed which is called "Cloud Information Accountability (CIA)". The main component of the CIA framework is logger component. Lightweight maintenance and strong accountability are the characteristics of CIA framework.**

Index terms- **cloud computing, Denial of service, CIA framework, logger.**

I. INTRODUCTION

Cloud computing becomes very popular over the internet these days. It refers to the access to the computers and all their functionalities with the help of local area network or internet. Resources are present in the cloud, whenever a user wants to access these resources he can utilize them with the help of web services. Initially the user has to request for the service he wanted. When it is granted, the resource is committed to the user as long as he uses the service. Users have no idea about the physical location of the machines which process their requests and stores their data. As users enjoying this convenience with the cloud technology, they are also worrying about privacy of the data. The data which is present on the cloud is not so safe, thus causes so many issues regarding the authentication, privacy and accountability.

There are various type of attacks which causes in the degradation of quality of service and performance. One of these attacks is Denial of service (DoS), which aim at reducing the availability of the service and consumes the resources of host system to degrade the performance. Denial of service is a type attack where the user is unaware of the ongoing damage. The user normally waits for the resource service provided by the cloud service provider, but this service is actually consuming by the unauthorized user. This attack doesn't causes any information loss whereas by the unwanted resource consumption there may be an extra service cost. As cloud is adopted with pay-per-use business model, DoS attacks may cause effects on service costs.

Therefore, in order to avoid extra service costs, certain countermeasures have to be implemented. Till now, various attempts have been made to discover these attacks.

A new kind of approach has been made, which is called Cloud Information Accountability. This framework works on the concept of information accountability, which offers end-to-end accountability in distributed manner. Some fundamental revolutionary characteristics of the CIA framework are lightweight maintenance and strong accountability that associates features of entry and usage manage along with authentication. Admin publishes the data along with some access privileges. The end user will access the data according to their access privileges specified by the admin. Whenever the data is accessed by the user a log file is generated. This log file can be retrieved by the admin. Auditing and accountability plays a major role in the CIA framework by keeping track of the ongoing process in the cloud. Data owner can retrieve log file either by one of the two auditing modes: *Push mode* and the other is *Pull mode.* In push mode logs are being sent on a constant tie basis to the data owner at the same time. In pull mode, contrary to push mode, logs can be retrieved by the authorized user.

II. RELATED WORK

DoS attacks are intended to target the weak points on the cloud and attacks them to decrease the performance. All these process is hidden that it can't be seen by the user. Even the detection mechanisms can't identify these type of attacks. When compared to the old-fashioned attacks these are difficult to find and causes severe damage in terms quality of service and service cost.

These type of attacks can be divided into two classes:

- ✓ *job-content-based*
- ✓ *Jobs arrival pattern based.*

Job-based-content attacks have been deigned to accomplish the worst case complexity. Whereas the latter exploits the worst case traffic arrival pattern of requests that can applied to the target system.

Cloud computing deals with various type of issues regarding the security and privacy. These issues depends upon the following five attributes, they are *confidentiality, accountability, availability, integrity* and *privacy.* Confidentiality and privacy are concerned with data safety. Availability refers to the time in which data is available to the customers for the service processing. Integrity refers to the detection of data violation stored on the cloud server. Finally, the accountability is responsible to maintain the relationship with trust among the cloud service providers and cloud users.

A new approach which depends on the entity for accountability of sharing data in cloud has been presented in which logging is performed on every access to the data in the cloud. The generated logs helps the data owner in finding out that the data is accessed by the authorized users only. The data owner has the idea who are the users that are accessing the data i.e., either they are the authenticated or potential users.

III. PROPOSED SYSTEM

In this paper a new kind of strategy namely cloud information accountability has been implemented. Most of the privacy concerned technologies are built on the perspective of hide-it-or-lose-it, but the proposed CIA framework concentrates mainly on making the data clear and can be tractable. The proposed CIA framework provides end-to-end accountability in a highly distributed manner. CIA framework has some special characteristics such as lightweight maintenance and accountability control which combines the features like authentication and access control. With the help of CIA, data owners are capable to track service level agreements and also implement access rules according to their wish. There are two kinds of modes regarding the accountability feature. They are:

- ✓ Push mode and
- ✓ Pull mode.

In push mode logs are sent to data owner or stakeholder on a constant time basis. Whereas in pull mode logs can be retrieved by the user as per his requirement.

IV. METHODOLGY

The main component of CIA framework is Logger component. The architecture of the framework can be shown below. Data owner publishes the data in the cloud server. Data publishing is done only after the authentication of owner is checked with the help of Certification Authority, which is an entity responsible for providing authentication to all users.

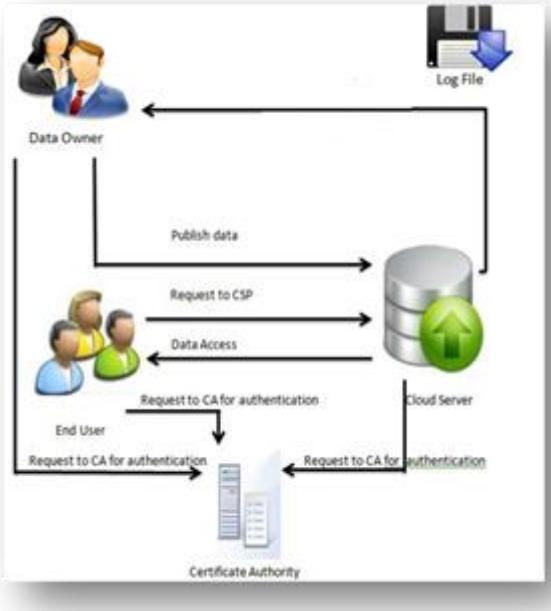

Fig.1: architecture of CIA framework

Data owner will publish the data on cloud server. This data will be accessed by the end users. Users should check their authentication by using Certificate Authority before requesting for accessing the data. When the user access the data in the cloud server, a log file is generated which contains user basic information details like user id, user's location etc. This log file can be retrieved by the data owner either once in a while or as per the requirement.

V. MODULES:

The following are the modules for the proposed framework.

- ➢ *Log file*:

Log file contains the basic information about the user and time of the data access such as User ID, location, Date, Time, etc. This log file is created with the logger component. Whenever there is a data access by the user this log file is generated and it is sent to the data owner.

- ➢ *Auditing mechanism:*

With the help of auditing the data owner can monitor the actual usage of his data. This can be done with help of log file. This log can be retrieved by the data owner by either of the following two methods:

*Push mode***:**

In this mode the log file can be received by the owner on a constant time basis. The data owner has to wait to get the log file for a period of time.

*Pull mode***:**

Unlike push mode, here the data owner doesn't need to wait for the log file. Here, the data owner can retrieve the log file according to his requirement.

- *Access privileges:*

The data owner while publishing the data will give some access privileges. The data owner decides which user is allowed to download the file and which user is not eligible. The access privileges are of different types such as view, download, location based etc. with the help of access privileges data owner will restrict the data access

VI. CLOUD INFORMATION ACCOUNTABILITY FRAMEWORK

The proposed CIA framework has some characteristics like lightweight maintenance and accountability controlling. With the help of CIA data publishing owners are capable of tracing the Service level agreements and can implement access rules.

A. Auditing Modes:

Push mode:

In push mode, logs are retrieved by the data owner on a constant time basis.

Pull mode:

In Pull mode, contrary to the push mode, only the authorized can get the log files according to their requirement.

B. Logging and auditing Techniques:

1. The logging ought to be decentralized keeping in mind that the end goal to adjust to the dynamic way of the cloud. More particularly, log files ought to be firmly limited with the equivalent information being controlled, and require negligible infrastructural support from any server.

2. Whenever there is an access to the user's data, it should be correctly and repeatedly logged. For this to happen some integrated techniques are necessary, which can monitor data access, verification, and record the actual operations on the data along with time at which data is accessed.

3. Log files should avoid illegal insertion, deletion, and modification by third parties and should be reliable. There may be a chance of losing log files due to technical failure, so recovery mechanisms should be incurred.

4. Data owner should get the log files, which contains the information of data access, periodically. The data owner should also be capable of retrieving log files whenever necessary irrespective of the location of log files stored.

5. The proposed technique doesn't leads to communication or computation overhead, thus it provides feasibility and reliability in data access.

C. Cloud Information Accountability (CIA):

A summary of the Cloud Information Accountability framework has been introduced here and how the CIA framework meets design requirements has been explained. The flowchart for the CIA is also given below. The main components of the framework are data owner, cloud service provider, and user.

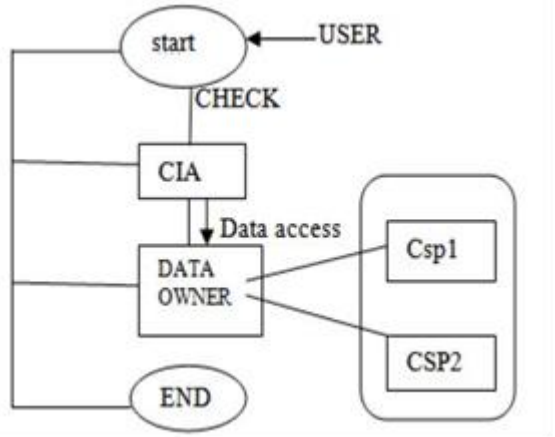

Fig.2: overall architecture

The cloud accountability feature has seven phases in its life cycle. This can be shown in the following figure:

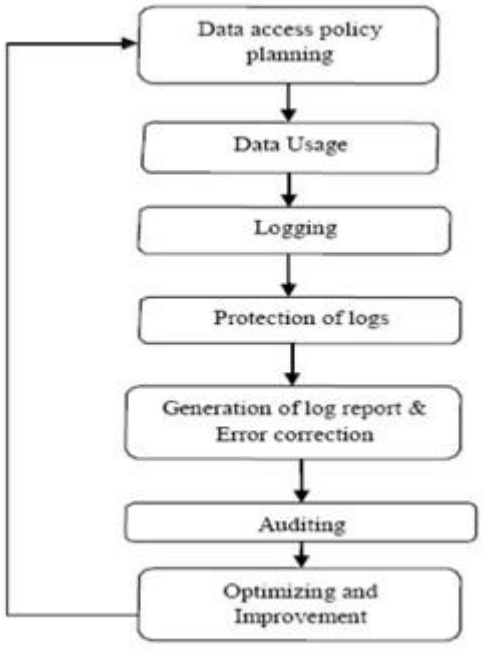

Fig.3: life cycle of Cloud Accountability

- In data access policy planning phase the data owners will decide what events have to be logged
- In data usage phase, if there is any misuse of data is occurred in cloud service provider then the accountability tools need to be able to trace.
- In logging phase, data usage details have to be logged and also the location where the logs are stored.

- These generated are to be kept safe which means providing integrity from unauthorized users. This is done in protection of logs phase.
- If there is any log corruption occurred then the error correction can be done by restoring the last backed up data.
- In auditing phase, the logs and records are being monitored by the trustworthy third parties.
- If there are any loopholes present in the cloud then it should be removed which is done in the final phase.

The accountability mechanism consists of the following components:

- ✓ Data owner
- ✓ Logger
- ✓ Cloud service provider
- ✓ User
- ✓ Log harmonizer

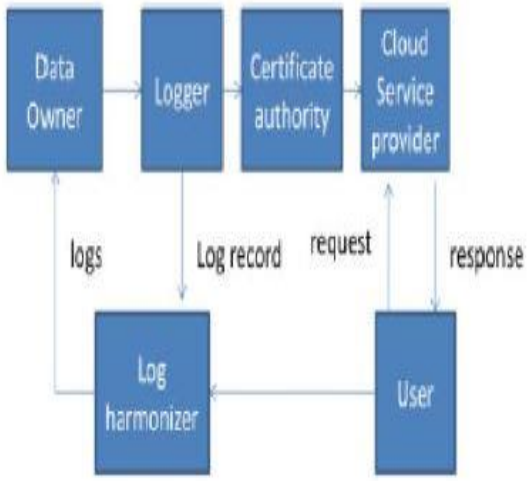

Fig.4: Accountability mechanism in cloud

Algorithm for handling server load:

In general there are more number of operations are performed by the users with the cloud service provider. When more number of requests came for the same content then there comes a problem. The following algorithm will handle the server load.

1. Start
2. When request meet to the CSP and that will be already registered user then
3. Cloud Subscriber :=Pull
4. Else
5. If CSP load< Moderated load
6. Client:=Push
7. Else
8. If CSP Load>moderated Load then
9. Repeat
10. Reduced Server load()
11. Until CSP load, timed out
12. Else divert some Push Subscriber to pull.
13. End if
14. End if
15. End if
16. Stop

VII. RESULTS AND COMPARISONS

Creation of log file and overhead measurement of the system are considered for the results. Overhead takes place mainly during the merging of log data, and authentication.

Log creation Time:

When the data is accessing continuously the log file is also created constantly. The time to generate a log file depends upon the size of the accessing data. As expected that the time taken to generate a log file is increasing linearly with the increase of the file size. The graph below shows various file sizes which are varied with the time to generate.

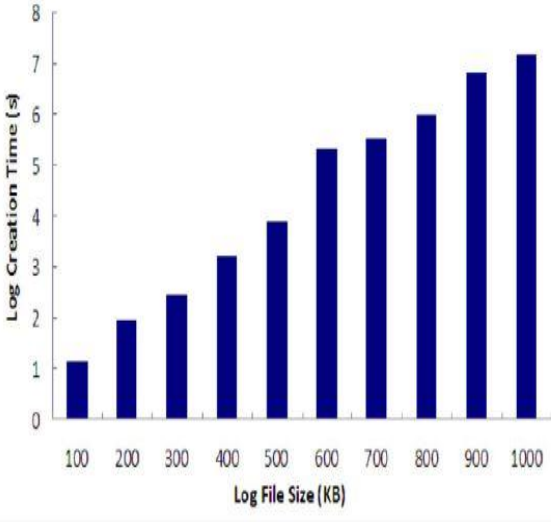

Fig.5: time to generate log file

Authentication time:

At the time of authentication there is a possible occurrence of overhead. If the time took for authentication is long then there will be more delay in accessing the data. As authentication happens each time the data is accessed by the user, the performance can be increased by adding a cache of certificates.

Log Merging Time:

From the following figure we can observe that there is an increase in the time as the number of files and their sizes increases.

The obtained graph is similar to a linear graph.

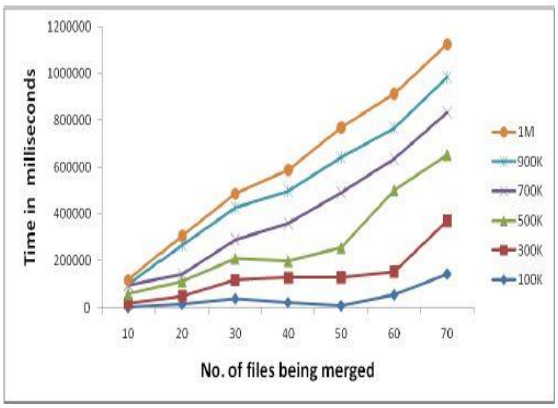

Fig.6: time to merging log files

Comparisons are made based on some metrics. These can be shown in below:

Parameters used for comparison	Existing framework	Proposed CIA framework
Response time	280 ms	250 ms
Service cost	Will be more than actual cost	Doesn't exceeds actual service cost
Scalability	Comparatively low	High
Overhead	Heavy at the server side	Slightly less than the existing
CPU utilization	High	Comparatively low
Availability	99%	99.50%
Throughput	130 ms	130 ms
Latency	User will get the access to data in minimum time	Takes minimum time for the data access

Table 1: Comparison of the existing and proposed framework

VIII. CONCLUSION

The CIA approach of automatically creating a log file allows data owners to check the actual usage of their data. Due to this the data owner will not have to worry about losing the control of his own data. Based on the log tracking, admin is aware of the potential users and authenticated users and hence can avoid the denial of service attacks in cloud computing. Also the owner can audit those copies of data that were created unknowingly.

REFERENCES

[1] M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson. Security and Privacy Governance in Cloud Computing via SLAs and a Policy Orchestration Service. In Proc. of the 2th Int. Conf. on Cloud Computing and Services Science, 2012, pp. 670-674.

[2] "A case for Accountable Cloud" Max Planck Institute for software System (MPI-SWS)

[3] Review on Techniques to Ensure Distributed Accountability for Data Sharing in the Cloud" H.Arun, R.Nilam, S.Purva, International Journal of Advanced Research in Computer and Communication Engineering, volume 2.,October 2013

[4] C. Metz. DDoS attack rains down on Amazon Cloud. Available at: http://www.theregister.co.uk/2009/10/05/amazon bitbucket outage/S, 26 Oct. 2009

[5] S. Sundareswaran, A. Squicciarini, D. Lin. "Distributed Accountability for Data Sharing in the Cloud" Proc. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No.4, Aug. 2012

[6] "Distributed Accountability for Data Sharing in Cloud" International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012.

[7] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 4, July/August 2012.

[8] D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigen-baum, J. Hendler, and G.J. Sussman, "Information Accountability," Comm. ACM, vol. 51, no. 6, pp. 82-87, 2008.

[9] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.