International Journal of Engineering & Technology, 7 (4.39) (2018) 640-644

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Issues of Accountability in Cloud Computing Environment

Surjya Kanta Mohanty*, Samaresh Mishra, Prasant Kumar Pattnaik,

School of Computer Engineering, KIIT Deemed to Be University, India
**Corresponding Author Email: coo@kiss.ac.in*

Abstract

In an accountable Cloud Computing Environment the system able to handle even the smallest action being performed by any entity in the environment and trace the entity that performed such as action to hold same accountable for mishap/risk if any. It is very essential that evidence of all the activity stored and processed may be maintained and stored for recovery in the future if required. This stored/maintained data are required to have enough information so that a particular activity can be properly scrutinized. This process should be an iterative process in order to achieve excellence in the system of the Cloud. This paper addresses the issues of accountability in a cloud computing environment.

Key words: *Accountability, Cloud computing environment, Steer Whee of Accountability, Trust, Security.*

1. Introduction

The Cloud Computing Environment (CCE) mentions to the freedom of use computing infrastructure over the internet. Information may be kept on the hard drive or change the applications the users use a service through the internet as to his needs, at anywhere. It offers flexible, dynamic, confidential and accountable infrastructures, Quality of Service guaranteed computing environment. It is characterized by providing hardware and Software resources as virtualized services as a result of which the users are free from the burden of thinking about the low level administration.

In **[1]** it describes Cloud Computing as the use of a set of services, applications, data, and platform in order to compute, storage of resources, and network. These mechanisms may be instantaneously provided in pay for use basis and it can be scalable as for requirements.

In the CCE, users take risks with regard to the privacy and security of their data, however, follows are certain features of cloud such as (i) No upfront hardware costs, time, resources (ii) Per-usage pricing (iii) Scalability (iv) convenience of remote access, the possibility of the capability on the basis demand, which have some obvious causes to take the risk associated.

The important consideration here is to look into what problems users are facing and identify the methods to reduce such problems/issues. When users put their data /information in the cloud they tend to lose their control over their data/information. There is a major concern/challenge with this issue, i.e. whether the information stored by the user in the cloud is secure and protected as it would have been if the user would have stored the same data/ information in its own network or computer. When working with Cloud users are required to have a clear knowledge of the actual meaning of security **[2],** which in general may have three components for consideration, i.e. security attacks, mechanism and services and subsequent goals as confidentiality, integrity and availability. However, while moving with Cloud Computing our attention is required to be towards transparency and accountability.

2. Over View of Accountability for CCE

The privacy professionals define accountability as "*Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information*".

There are basically two entities in a CCE, one is the user who shares its personal data in the cloud and the other is the service of cloud provider who manages the information in the CCE. The Scenario is such that neither of them (User and service provider of the cloud) can be held accountable for any kind of mishap in the cloud environment. To create a secure and trustworthy environment one of the entities (User or Cloud service provider) is required to be held responsible in order to solve any dispute that may arise in future. The entity that can be held responsible in required to have a strong identity with necessary provision for storing all transactions **[3,4]** and whenever required the same may be audited. For this it is required that a set of policies may be formed/defined that would govern the transaction and when required, the record of the stored/maintained transaction may be verified against the policies framed. Here we may cite an example to replicate the above scenario as follows, suppose that an entity X does some action in the Cloud Computing environment then that action may be verified with the defined/framed policies to ensure/check that whether the entity X has performed some wrong action. If anything wrong is found then the entity X may be held responsible for the same. Further When CCE is implemented with proper accountability aspects which are also the threats that need to be taken care are **[5]** Malicious insiders, abuse and nefarious usage, Shared technology vulnerabilities, iformation leakages or loss, Unknown risk profile, Insecure application programming interfaces, Account, service and traffic hijacking.

Many researchers focuses on issues of account, provision and

interchange, *say example:* Stolen identification may includes regulation and privacy policy that will be differ in place of country to country. However, the application in CCE must be restricted to laws of the nation.

Based on the definition of Accountability Stack l is explained **[6]** in Fig-1.

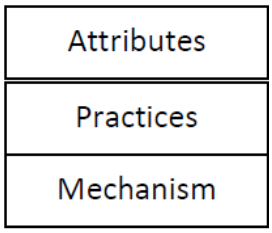

Fig. -1: (Accountability Stack)

This Stack of Accountability Consists of three parameters, first parameter being accountability attributes: this are the elements of accountability such as verifiability, observability, responsibility, transparency, attributability, remediability and liability, then second parameter being accountable practices: this are the practices by which accountable attributes are operationalised and then the third parameter accountability mechanism: this are the mechanism which are used to implement accountable practices.

2.1. Challenges of accountability in cloud computing environment:

Some challenges faced by the cloud computing environment **[7]** during the deployment of accountability are discussed below:

- Loss of data on the CCE or failure of the cloud to provide information when needed.
- Improper or poor customer service due to allocation of insufficient resources to the user.
- Destruction of data in the CCE due to virus or certain malafide actions of a third party.
- A wrong calculation result which may be due to misconfigured systems.

2.2. Needs of accountability in cloud computing environment:

Accountability is the aggregation of procedures to make the environment responsible and trustable. Considering that all entities within the Cloud Computing environment are semi trusted an accountable system is required to bind every action taking place to identify the user associated with a particular action . In other words, we can say that each acknowledged user may lie according to its own interest so by imposing predefined policies the culprit user may be held accountable for the mishap in the system. In **[8]** the need of accountability is outlined as follows:

Logging: The past record of dispute free operation may be logged in real-time. This recorded logs is required to be t enough to resolve any subsequent disputes in associated processes.

Monitoring and Auditing: The organization status may be constantly monitored and audited. Once an immunity or destruction is identified , the reason behind it should be found out and actions are required to be taken to minimize its effects.

Dispute declaration: When the source of malfunction cannot be detected and a particular entity can not be held accountable, will be take awayt to decide the violating entity(s). In such circumstances effort should be made that the system is required to suffer minimal delay due to dispute declaratio**n**.

3. Requirement of accountability in cloud computing environment:

The technical requirements of cloud accountability are described here referring to **[9]:**

A. **Availability:** Accountability of the cloud clarification and process should fit the basic needs of stability and competence.

B. **Access Control:** Access control mechanism held responsible for authenticity enabling a property of access scheme that includes authentication process and limited to user grants to access the information in the cloud.

C. **Integrity and Data Confidentiality:** Cloud accountability management process should not negotiate with the actual data confidentiality and integrity.

D. **Logging and Real-time Data Monitoring:** In this process user data should be logged and notify in the real time.

E. **Trust management:** In CCE, the associated service may have precedence permission to store the information in the cloud.

F. **Auditability:** A Cloud Log must be auditable and verifiable.

G. **Management:** The handheld devices may be connected to access the cloud, it is needed to ensure the devices are full proof. The user seeking an effective mechanism to control their data in the cloud environment; however, these users may interested to know about how, when and who is managing their cloud environment infrastructures during data access. The cloud accountability method focuses on proper transparency.

4. Deployment of accountability in cloud computing environment:

Accountability can promote execution of mechanisms by which the legal needs and guidance in a CCE can be well translated into organised data protection. In General the policies framed may be applied only at data level whereas accountability mechanism can exist at different levels including data and system level. Developers can offer data controllers with a pool of methods that may enable the creation of built in solutions in which the controllers can tailor measure to their context while considering into account the involved systems , the type of data /information , its flow and so on.

With this approach users may co-design various mechanism, measures and procedures **[10].** Design element may be integrated by the users to support retrospective accountability using detective control and prospective accountability using preventive control. In order t find out the privacy and security risk that goes against procedure / policies, detective control is used. Tracking, auditing, monitoring and reporting are included in detective control. Similarly, to find out whether an action continues or takes place at all preventive control may be used. Risk analysis and decision making tools and techniques, policy , trust appraisal and identity management are included in anticipatory control.

Further whenever an undesired outcome has already occurred in Cloud Computing Environment, in order to fix such undesired outcome corrective control may be used. All the above i.e. Preventive control, detective control & corrective control complement with each other and a combination of all these control

is ideal for accountability. In a cloud which is highly dynamic and automated environment the provision of accountability may not occur only through procedural means. It is by enforcing policies, providing decision support , assurance , security and so on , the technology may play a crucial role in enhancing solutions. Procedural measures for accountability include finding cloud service provider ability before selecting , negotiate service level agreements, limiting the communication of confidential data, and purchasing insurance and technical way for accountability includes privacy informediaries, mitigation & encryption for data security. The Infrastructure should be such that users must also be able to depend on it to report information correctly, enforce policies and preserve appropriate separations.

5. Popular mechanism of accountability in cloud computing environment:

Having recognized that accountability is essential; in this section, is defined three services that make service providers accountable to users, three accountability targets, and data elements for validating accountability as follows:

A. Three Services for Incorporating Accountability:
In providing accountability to the users it essentially involves the expertise to replicate transaction events that have already taken place based on consistent data. In order to achieve this there are three services that would make cloud service providers accountable to users**:** an event trace service (acquire, consolidate, store), an event visualize service (retrieve, relate, display), and an event prove service (validate, show event is unaltered and not expired).

B. Three Accountability Targets
There exits three types of events that providers are required to be capable of replicating in order to be fully accountable to users and provide users with dependable cloud-based services: Process accountability (proof that a service process has truly been performed): Process accountability find out the timing, the sequencing, and if necessary the location of the sites of processing a user's request, Content accountability (history and lifecycle of content movement): Content accountability is the ability to outline the movement of specific content (files, data) outside the cloud, when it enters the cloud, when it exits the cloud, and on which storage devices the information are stored in the cloud. Content accountability is able to track content through the entire life cycle from creation to destruction of the content and Operation accountability (history of the operator's actions): Operation accountability is the ability to map out operation events of cloud system providers.

C. Data Elements and Security for Accountability: The Data Elements and Security for Accountability focuses on Data Elements that deals with location of a service based on uncertainty. Data Element: In a CCE the location of information or data is not clear, and it is hard to specify the user. Simultaneously it is extremely essential to maintain information showing timing, places, and parties involved. This information should be kept together with information revealing how data is processed (method) and what became to the data (result) and Data Security: It is like employing a scheme that endows cloud service provisioning systems with a way to reserve the confidentiality, the completeness, and the availability of the above information structure elements which will enables users to guarantee the validity of accountability content.

6 Some cloud acountabiity framework availiable

Some frameworks and their corresponding approaches proposed by researcher's literature are discussed below:

A. Cloud Information Accountability Framework:
The Cloud Information Accountability (CIA) framework focuses on audit and accountability mechanisms in the cloud computing environment**[11]**, CIA ensures data is visible and noticeable under any situation. It helps in end-to-end accountability such as data authentication, data access, and data control.
There are mainly three components of the CIA:
***1) Programmable* Java Archives.** In this Java Archives (JARs) have the ability to trace the transaction of a particular users in the cloud computing environment.
2) Logger. *A* user's data storage and the related log files and nested Java archive file is used that is known as Logger.
3) Log harmonizer. The component that is responsible to make replications of the logger process that contain the same data items is termed as Log harmoniser. It is Java archive file that contains class files for server and client side. It is responsible for the auditing. However, there are two modes for auditing: push mode and pull mode**[11].**
***a) Push mode*.** The push mode is an operation used in cloud computing environment that at regular intervals sends subsequent logs to the user.
b) Pull mode. The pull mode is an operation used in cloud computing environment to recover data logs at anytime as for user's need.

B. A4Cloud
The A4Cloud is a environment that intended provide accountability system in the cloud service assessment chain **[12].** It has been concluded in this framework that it is a challenge to attain cloud accountability only through the functioning of only technical assess. In this cloud accountability model to achive accountability three element have been defined as follows: Tiers, Rules, and Process.
1) Accountability* Tiers*:
Accountability consists of three basic tier : workflow, data, and system . The **workflow tier** is the top most , which focus on audit The **system layer** is the lowest tier which includes file - logging, file system and network;. The **data tier** supports the data abstraction and maintains consistency among the logger.
2) Accountability Rule:
Accountability rule ensures data security particularly, when the applications that are executed by a trusted third party instead of the cloud service provider itself. user are permitted to participate in the process
3) Accountability Process:
A4cloud provides anticipatory risk, identifying risk and managing incidents process, with each individual handling many types of applications in many situations. these process are capable of providing CSPs transparency for the third party data access.

C. Access control augmentation based Cloud Accountability:
The CSP is accountable for defensive the data in the cloud computing Environment by recommending an access control framework for cloud accountability with followings **[13].**
1) XML based document representation of user data
2) Policy scheme
3) Access scheme relies on access role and corresponding certificate.
4) Certificate could be hierarchical structure.
5) Encryption, decryption and integrity over the data to be achieved with public and private key

7. Phases of cloud accountability:

In a CCE the users store its data in a file within a virtual machine (VM) launched by a Cloud service provider. When the data in uploaded to the Cloud environment, service provider's domain performs load balancing by creating many virtual servers and physical servers started with file creation in the backup process, includes data transfers , read/write operations. Moreover, it would be likely to trace the file record and log record, thereby achieving cloud accountability and auditability.

By tracing the transactions it would be possible to know when, where, how and what was being leaked/accessed, and by whom. This helps both user and CSP to take for granted a Cloud environment. Based on above, in this context is proposed a Cloud Accountability Steering Wheel **[14]** which focuses to achieve an accountable and trustworthy environment that is secure and protected. In Fig.-2 seven processes have been described to implement accountable Cloud Steer Wheel.

7.1. Policy planning

The Cloud Service provided needs to decide that which data to be logged. In **[14]**, focus is on four important groups of data that must be logged: (1) Event data – a series of actions and related data, (2) Actor Data – the entity which fired the event, (3) Timestamp Data – date and time when the event occurs and (4) Location Data –Network, server detail where event initiated.

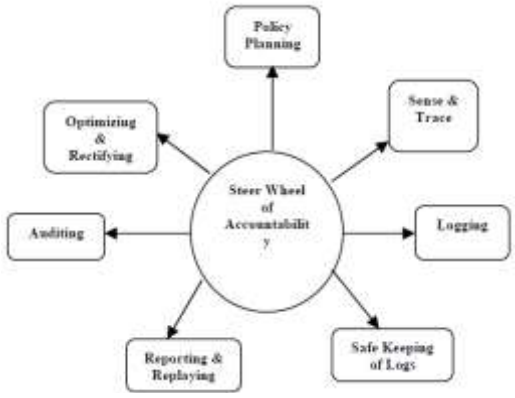

Fig.2:- Steer Wheel of Accountability

7.2. Sense and trace

This phase would act as a feeler and logging in real time when the expected event executed in the cloud environment. In this situation, tools are expected to monitor the system read/write operations that hosted in virtual machines in cloud servers and locations. The routes of network packets in the cloud are also needed to be traced.

7.3. Logging

Logging should be performed in the Cloud in physical as well as virtual layers. The important facts to be taken into consideration here in the lifespan of the logs, the logged data details and the exact location where the logs would be stored.

7.4. Safe-keeping of logs

Once the logging has been completed it quite important that the integrity of the logs is protected and prevented against unauthorized access. It is also required to be ensured that the logs are not tempered and for this the logs may be encrypted. Proper backing of logs, prevention of logs from being corrupted is also required t be ensured by applying appropriate mechanisms.

7.5. Reporting and replaying

In this phase the predefined reporting tools would generate summaries and reports of the audit trails, the access history of files and the life cycle of files in the cloud. Suspected irregularities would also be flagged to the end-user. Reports would cover a wide scope ranging from the physical and virtual server histories within the cloud to high-level workflow audit trails.

7.6. Auditing

In this phase the logs and reports would be checked and potential fraud-causing loopholes would be brought infront. The necessary auditing would be carried out by the stakeholders and auditors.

7.7. Optimising and rectifying

In this phase the specific problem areas and loopholes would be removed and rectified. An iterative process would bring an excellent environment to work upon.

8. Conclusion:

Cloud Computing has emerged as an important technology for outsourcing various IT needs of organizations. Now days there are various Cloud Service providers that provide different Cloud services with price difference and varied performance attributes. With the increase in the number of Cloud service offerings there opens the chance of infinite computing resources of the Cloud available to the users, simultaneously, it has become a challenge for the Cloud customers to find the best Cloud services which can satisfy their Quality of Service requirements in terms of parameters such as performance and security, privacy and accountability. In order to choose correctly between different Cloud services, the users/customers are required to have a method to identify and measure key performance criteria that are important to their applications. Focus should be on accountability in Cloud Environment that will bring the basic trust among the users to use and work in Cloud Environment. It is felt the users major concern in on their personal information security and privacy. To increase the popularity of Cloud Computing a sense of trust is required to be brought in the mind of users, which can be met by defining and implementing accountability measures in the Cloud Computing Environment.

References

[1] Parul Chachra / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, P(1066-1068).
[2] Rajeev Kanday/International Conference on Computing Resources/2012/P(302-308)
[3] Pearson, S. , "Toward Accountability in the Cloud" Internet Computing.IEEE 2011.
[4] Nakahara, S.; Ishimoto, H. "A study on the requirements of accountable cloud services and log management" Information and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium, 2010.
[5] Ryan K L Ko , Peter Jagadpramana , Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang , Bu Sung Lee/ Trust Cloud: A Framework for Accountability and Trust in Cloud Computing /IEEE /2011/P(584 - 588)
[6] Massimo Felici and Siani Pearson/ Accountability, Risk and Trust in Cloud Services/ 2014 IEEE 10th World Congress on Services/P(105-112)
[7] Zhifeng Xiao and Yang Xiao/ Security and Privacy in Cloud Computing /IEEE communications surveys & tutorials, vol. 15, no. 2, second quarter 2013/P/843-859)
[8] Jinhui Yao, Shiping Chen, Chen Wang, David Levy, John Zic/ Accountability as a Service for the Cloud/ 2010/IEEE International Conference on Services Computing/P(81-88)

[9] Xianghan Zheng, Hui Ye, Chunming Tang, Chunming Rong, Guolong Chen/ International Conference on Cloud Computing and Big Data/2013/P(627-632)
[10] Siani Pearson/Towards Accountability in the Cloud/IEEE/2011/1089-1801/II
[11] 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, P. 82-87, 2008.
[12] Chunming Rong, and Javier Lopez, " Accountability for Cloud and Other Future Internet Services, " IEEE 4th International Conference on Cloud Computing Technology and Science. 2012.
[13] Shi Jun, Li Hui, Zhou Lidong. "Research of security data storage based on cloud computing, " Journal of Nanjing Normal University (Natural Science Edition). vol. 35, No. 3, 2012
[14] Ryan K L Ko , Bu Sung Lee, Siani Pearson/ Towards Achieving Accountability, Auditability and Trust in Cloud Computing/ First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV/ Springer Berlin Heidelberg/P(432-444)