International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5 Issue: Special 4, pp: 790-991 20 May 2016

Distributed Accountability for cloud in Data Sharing

Thusha V
Mtech C.S.E,Citech, Visvesvaraya Technological University

Bhagavant Deshpande
Asso prof, Dept of ISE,Citech, Visvesvaraya Technological university

ABSTRACT:
Cloud computing can be consider as a source which are delivered over the network. Cloud computing can also be considered as a business model. It is an upcoming style of computing where applications, data, and resources are provided as services to the users over the network as on needed basis. The use of Cloud computing has widespread on different types of trusted scenario. Cloud systems can automatically control and optimize resource and the type of services, which are storage, processing, bandwidth and active user accounts. Resource usage are monitored, controlled and reported providing transparency for both the provider and consumer for service they have utilized. A major characteristic of cloud services are the user data are processed remotely in unknown machine where the user has no access. To overcome these few problems propose decentralised framework to track the user data actually being used in the cloud. In this existing, propose a novel distributed accountability and auditing mechanism.

KEYWORDS: Cloud computing, distributed accountability, Privacy, auditing, data sharing, security.

1. INTRODUCTION:

Cloud computing has enabled much highly scalable services which become easily available over the internet as per our needs. There are major features of cloud that provides services for user's data. Which are processed remotely by an unknown machine which a user do not own or operated upon. As enjoying all these easy of convenience brought by this new emerging technology, thus user fear of losing control over their own data it could be anything like personal particulars, financial, or health care. The data which is outsourced on clouds could lead to number of issues related to accountability including handling things of personal information of the identification. This shall become a significant barrier to the wide adoption of cloud and its services. Here require a novel decentralized information accountability framework that could keep track of actual data that is being used in the cloud. Kind of propose an object-centered approach that could enable enclosing our logging in mechanism together with the user data and its policies.

One can use the maximum advantage of the JAR programmable capabilities to create both dynamic and traveling objects and it shall ensure that any access to user's data shall trigger authentication and automated logging locally to the JARs. Also provided distributed auditing mechanisms to strengthen the user's control over data. Extensive experimental studies have been demonstrated to show the efficiency and effectiveness of the proposed system approach.

The architecture of the proposed system is platform independent and highly decentralized, it does not require any kind of dedicated authentication throughout or any place for storage system.

The delivery models in cloud can be classified as three types: Public, Private, Hybrid. In public cloud capability demands on what business they rent and pay for what they actually use. Examples for public clouds are Amazon, Google, IBM. In private clouds a business eventually turns into cloud its IT environment and is used to deliver its services to its users. Hybrid clouds are a combination element of public and private clouds.

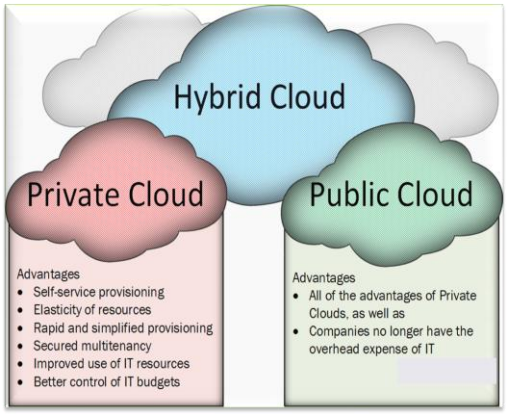

Fig 1: Cloud Computing Architecture

2. EXISTING SYSTEM:

To consider user concerns it is quite essential to provide an effective mechanism for users to view and monitor the usage of their data in the cloud. For an instance should ensure that

their data are handled as service level agreements which are made at the time they sign on for service in the cloud. For closed domains (i.e. databases and operating system) conventional access control approaches are developed. One can also use centralized server in distributed environments in the existing framework data are directly outsourced by cloud service provider to other entities in cloud, these providers can also delegate the task to others and so on, as entities can join and leave the cloud in flexible manner thus data handling in cloud goes through a very complex and kind of dynamic hierarchical service chain which does not exist in conventional environment.

3. PROBLEMS ON EXISTING SYSTEM:

First of all, data can be sent or outsourced by the direct cloud service provider (CSP) to other entities in the cloud and these entities can also delegate the task to others and so on.

Second one is, as entities are allowed to join and leave the cloud in a very flexible manner as this is a result that data handling in clouds goes through a complex and dynamic hierarchical service chain which is not there in conventional environments.

4. PROPOSED SYSTEM:

To overcome the above mentioned problems, proposed novel approach called as cloud Information Accountability (CIA) framework, which is based on the notion of information accountability

As Privacy protection technologies that are built on the perspective to hide-it or lose-it, same way the information accountability keeps track of data usage transparent and it is track able. Proposed CIA framework shall provide end to end accountability in highly distributed fashion. The main innovative features of the CIA framework is its ability to maintain lightweight and powerful accountability which also the combines the aspect of usage control, access control and authentication. With the help of CIA framework data owners can track not only if service-level agreements are dishonoured, but also impose access control and usage control rules as needed. To this accountability feature there are two modes for auditing one is push and other is pop mode.

5. IMPLEMENTATION:

Implementation of project is a stage when theoretical design is turned out into a well developed working system. Thus this is considered as the most critical stage in reaching a successful level for a new system and giving the user a confident stage to enhance the new system would work effective.

Implement stage includes few stages to evolve a complete new system these are careful planning, investigating about all the details of the existing system and its constraints, faced difficulties during implementation, designing few methods to achieve change over in new system and evaluation of the methods considered during the changeover.

6. MAIN MODULES THAT WE CONSIDER:-

1. Cloud Information Accountability (CIA) Framework:

Cloud Information Accountability (CIA) framework Algorithm, it maintains light weighted and strong accountability that combines all the aspects for access control, usage control and authentication. With the help of this CIA the owner of the data can track both service-level agreements being honored or dishonored along with enforcement of usage control, access control rules.

2. Owner or user

Data owner can upload data to the cloud server; to get an access to the cloud server the owner needs to register with cloud server in order to upload the required data. After the owner has registered with the cloud server, the owner will be assigned with some space to upload the data.

User is a person who can download the needed data from the cloud server or just can view the data from the cloud server. To download any data from cloud server, the user has to register first with the cloud server the details like username and password and set of other details. All these information's will be stored in the data base for future use and authentication.

3. Push and pull

Push can be referred to the logs that are being sent to the data owner at regular intervals. Pull refers to the other way approach where these logs can be retrieved when ever needed.

4. Logging and auditing Techniques

1. Log files should couple with the corresponding data and should maintain minimum infrastructure to support from any server.

2. Access to the user data should be automatically and correctly logged in terms to know who accessed the data, who verified the data, what operations on data being performed and the time that data was accessed.

3. All Log files must be reliable and tamper proof in order to prevent illegal insertion, modification and deletion by other

malicious parties. Recovery mechanisms are very much necessary to restore the damaged log files.

4. Log files should be sent to the users at regular intervals as to inform them the current usage of their data.

5. Random number set

Whenever the users request to download a data from the cloud server, the users need to enter random number set. If it matches the user can download the data. Random number is given to the owner during registration phase only. Remember each time the random number will vary thus this will ensure security for downloading through right mode.

7. SECURITY REASONS:

Let us see what could be possible attacks on this framework.

1) Authorized users verses unauthorized user:

If an unauthorised user try to view actual data, then it is not possible to access as the integrity is checked by the authenticated system.

2) Jar files attacked

What if the data in the JAR is being accessed without anyone noticing? Then this type of attack can easily be found by auditing. Actions are recorded by the logger and log reports are sent to user at regular time intervals. Hence data owner will be aware of files being downloaded.

CONCLUSION AND FUTURE RESEARCH

Our system run online thus it can be improved further and will be hosted on mobile apps. This is platform independent. Purpose of this paper is to provide distributed accountability in cloud. This framework will guarantee the user by protecting their data with the help of JAR files and limited number of consumer access policies. The most important aspect of the framework is owner can monitor their data usage. It Should be capable to support variety of security policies. In future aim is to free licenses on Amazon cloud and to implement in Big Data for cloud optimization.

REFERENCES:

[1] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T. Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[2] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM*. , pp. 441–445, 2010.

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography Workshops*, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[4] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[5] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[6] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in *TRUST*, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.

[7] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability andtrust in cloud computing," HP Technical Report HPL-2011-38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in *ACM ASIACCS*, pp. 282–292, 2010.

[9] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in *15th National Computer Security Conference*, 1992.

[10] 2014 IEEE transaction paper "CIA BASED ON THE CLOUD STORAGES".

[11] 2013 IEEE COMPLETE REFERENCE ONLINE CLOUD". [12] 2012 IEEE LIVE "study on science DOUBLE AUTHENTICATION CLOUD detection used for ONLINE CLOUD"