Secure Data Sharing In Cloud with Distributed Accountability

Shaikh Ajhar, Dr. J Sasi Kiran

***Abstract*— In this world every computer or web user is using the cloud services to accomplish his work. Cloud computing provides the ease in using the application or services provided by him. Using cloud computing now user can access his data from anywhere anytime. In this users' data are usually processed remotely in unknown machines that users do not operate. On the one hand we are using this services but another side is that user don't have control over his own data due to wide range of cloud service users and may fear of losing its own data. To handle the stated problem with the cloud computing in this paper we provide approach to handle the user's data in that we are keeping the accountability of data. In this method the user's data is binded with the logging mechanism means every usage of that data will be informed to user or we can say that handled by user. Accountability checks for transparent access and authorization of data. With using JAR programming which provide privacy and security for data. We provide experimental result that demonstrates the efficiency of our proposed approach.**

***Index Terms*— cloud computing, accountability, logging, data sharing, auditing mechanism.**

I. INTRODUCTION

Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities.

Cloud computing is at an early stage, with a motley crew of providers large and small delivering a slew of cloud based services, from full-blown applications to storage services to spam filtering.

There are various services provided by the Cloud are as follows:

- Infrastrucure-as-a-service(IaaS)
- Platform-as-a-Service(PaaS)
- Software-as-a-Service(SaaS)

Infrastructure as a Service(IaaS):

Infrastructure-as-a-Service like Amazon web services provides the customer with virtual server instances and storage as well as application program interfaces(API) that allows the customer to start, stop, access and configure their virtual servers and storage.

Platform-as-a-Service(PaaS):

Platform-as-a-Service incloud is defined as set of software development tools hosted on the provider's infrastructure. Developers create application on the provider's platform over Internet.

Software-as-a-Service(SaaS):

Software-as-a-Service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front end portal.

Traditional access control approaches developed for closed domains such as databases and operating systems, using a centralized server in distributed environments, are not suitable, due to the inlisted features characterizing cloud environments. First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also represent the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments. To overcome the above problems, we propose a new approach, namely Cloud Information Accountability (CIA) framework, based on the idea of information accountability [3]. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and track able. Our proposed CIA framework provides end-to-end accountability in a highly distributed fashion. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed.

II. EXISTING SYSTEM

To allay user's concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed

Manuscript received October 29, 2014.

Shaikh Ajhar, Department of Computer Science and Engineering, Vidya Vikas Institute of Technology, Hyderabad,India.

Dr. J Sasi Kiran, Department of Computer Science and Engineering, Vidya Vikas Institute of Technology, Hyderabad,India.

environments, are not suitable, due to the following features characterizing cloud environments.

A. *Problems on existing system*

First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

B. *Proposed System*

We propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and tractable. Our proposed CIA framework provides end-to end accountability in a highly distributed fashion. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed.

Our main contributions are as follows:

We propose a novel automatic and enforceable logging mechanism in the cloud. Our proposed architecture is platform independent and highly decentralized, in that it does not require any dedicated authentication or storage system in place.

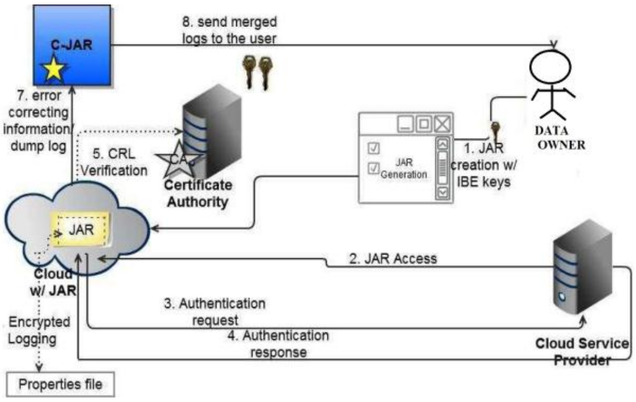

Fig 1.Overview of CIA framework

We go beyond traditional access control in that we provide a certain degree of usage control for the protected data after these are delivered to the receiver.

We conduct experiments on a real cloud testbed. The results demonstrate the efficiency, scalability, and granularity of our approach. We also provide a detailed security analysis and discuss the reliability and strength of our architecture.

III. Modules

Following are the important module used in our project,
Module 1: DATA OWNER
Module 2: JAR CREATION
Module 3: CLOUD SERVICE PROVIDER

A. *DATA OWNER*

In this module, the data owner can upload their data in the cloud server. The new user has to register with the service provider by creating new account because of that security is maintained and he can upload or store his files. Data owner encrypt data for security purpose.

The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file. To allay users’ concerns, it is essential to provide an effective way for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud.

B. *JAR CREATION*

In this module Jar file is created for file uploading.The user should have the same jar file to download the file. This way the data is going to be secured. The logging should be decentralized in order to adapt to the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled, and require minimal infrastructural support from any server. Every access to the user’s data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity who accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed. Log files should be reliable and tamper proof to avoid illegal insertion, deletion, and modification by malicious parties. Recovery mechanisms are also desirable to restore damaged log files caused by technical problems. The proposed technique should not intrusively monitor data recipients’ systems, nor it should introduce heavy communication and computation overhead, which otherwise will hinder its feasibility and adoption in practice.

C. *CLOUD SERVICE PROVIDER*

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud with the jar file created for each file for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them

IV. SECURITY DISCUSSION

We now analyze possible attacks to our framework. We assume that attackers may have sufficient Java programmingskills to disassemble a JAR file and prior knowledge of our CIA architecture. We first assume that the JVM is not corrupted, followed by a discussion on how to ensure that this assumption holds true.

A. Attacks on JAR files

The common attack that we can assume is accessing the data in JAR file without being noticed. But such attack can befound out by auditing. However if someone tries to download the JAR files, the actions are recorded by the logger and the log record is sent to the user. By this the data owner will be aware of his JAR file download.

B. Unauthorized user

If some unauthorized person tries to access the data, first of all it is impossible as his/her integrity is checked by the authentication system before giving the access to actual data.

V. Conclusion

In this paper we see innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism is proposed. The approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge.

In the future, planned to refine our approach to verify the integrity and the authentication of JARs

ACKNOWLEDGMENT

Good Teachers are worth more than thousand books, we have them in Our Department.

REFERENCES

[1] SmithaSundareswaran, Anna C. Squicciarini and Dan Lin, "EnsuringDistributed Accountability for Data Sharing in the Cloud,", IEEETransaction on dependable a secure computing, VOL. 9, NO. 4, pg 556-568, 2012.

[2]Hsio Ying Lin,Tzeng.W.G, “A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding“,IEEE transactions on parallel and distributed systems,2012.

[3] Yan Zhu, Hongxin Hu, Gail JoonAhn, Mengyang Yu, “Cooperative Provable Data Possession for IntegrityVerification in MultiCloud Storage” , IEEE transactions on parallel and distributed systems,2012.

[4]http://www.a4cloud.eu/cloud-accountability

[5]http://www.hpl.hp.com/techreports/2011/HPL-2011-38.pdf.