Distributed Accountability for Data Sharing in Cloud

LAKSHMIPRIYA R
S7 CS B

Guided By:
Mrs. ANITHA M
Department of Computer Science and Engineering

20 OCTOBER 2020

Overview

1. INTRODUCTION
2. PROBLEMS FEARED BY USERS
3. PROBLEM STATEMENT
4. EXISTING SOLUTION:
5. ACCOUNTABILITY SOLUTIONS:
6. PROPOSED SYSTEM
7. CLOUD DATA ACCOUNTABILITY FRAMEWORK:
8. FLOW OF DATA
9. POSSIBLE ATTACKS
10. CONCLUSION
11. REFERENCES

INTRODUCTION

- CLOUD COMPUTING: A technology which uses internet and remote servers to store data and application.
- In cloud there is no need to install particular hardware, software on user machine, and is able to use various resources with less effort and cheap rates.
- User can access the data from any machine or any where in the world on demand
- They are cost efficient, increased storage capacity, backup and recovery, continuous resource availability and location independence and scalable

INTRODUCTION (Contd.)

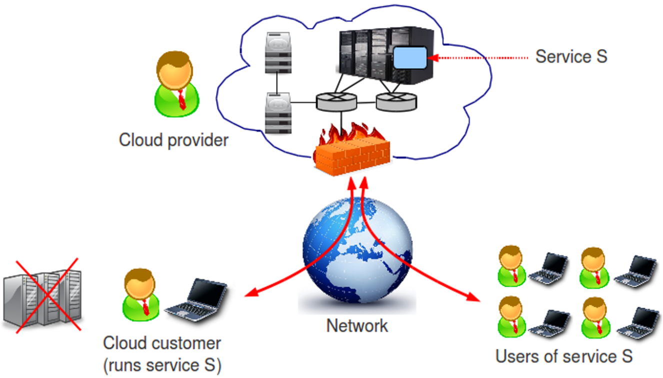


Figure 1: cloud computing

Models For cloud storage:

- Infrastructure As A Service (IAAS): provides virtualized computing resources over the internet. In an IAAS model, a third party provider hosts hardware, software, servers, storage and other infrastructure components on the behalf of its users.
- Platform as a Service (PAAS): a cloud computing model that delivers applications over the internet. In a PAAS model, a cloud provider delivers hardware and software tools, usually those needed for application development, to its users as a service.
- Software as a Service(SAAS) : a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Problems

- Data security in cloud is very important issue to solve
- Worry about unauthorized access of their data and manipulation of data which leads to accountability issues
- Users may not know the machines which actually process and host their data, thus worry losing control of data
- No specific mechanisms to check if the service level agreements made between are preserved or not

Virtualisation problems

- Virtualisation:a pillar technology in cloud computing for multiplexing computing resources on a single cloud platform for multiple cloud tenants
- Existing monitoring mechanisms on virtualized platforms either takes a complete VM as the monitoring granularity, such that they cannot capture the malicious behaviours within individual VMs,
- they focus on specific monitoring functions that cannot be used for heterogeneous VMs concurrently running on a single cloud node
- assumes that the privileged domain is trusted to act as expected
- which contradicts users concern

Problem statement

- Cloud user send his/her data access control policies to the service provider
- The service provider will have granted access rights
- the rights are granted using conventional access control mechanisms, data will be fully available at the service provider
- We use new logging and auditing techniques to track the actual usage of data

EXISTING SOLUTION

- PRIVACY MANAGER MECHANISM:Here user's data is in encrypted form in cloud and evaluating is done on encrypted data, thus forms readable data from result of evaluation manager to get the correct result. In obfuscation data is not present on Service provider's machine so data is safe on cloud.
- this not suitable for all cloud application, when input data is large this method can still require a large amount of memory

Existing soln (Contd.)

- Second Mechanism: policies are decided by the parties that use, store or share that data irrespective of the jurisdiction in which information is processed.data owner attach Policies with data, which contain a description of which actions are allowed with which data, but there is the problem of Continuous auditing of agent
- soln: a three layer architecture which protect information leakage from cloud, it provides three layer toprotect data, in first layer the service provider should not view confidential data in second layer service provider should not do the indexing of data, in third layer user specify use of his data and indexing in policies, so policies always travel with data.

Conventional controls in cloud

- Conventional access control approaches developed for closed domains and approaches using a centralized server in distributed environments, are not suitable.
- * data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the Cloud and these entities can also delegate the tasks to others
- *entities are allowed to join and leave the cloud in a flexible manner
- the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments

Accountability

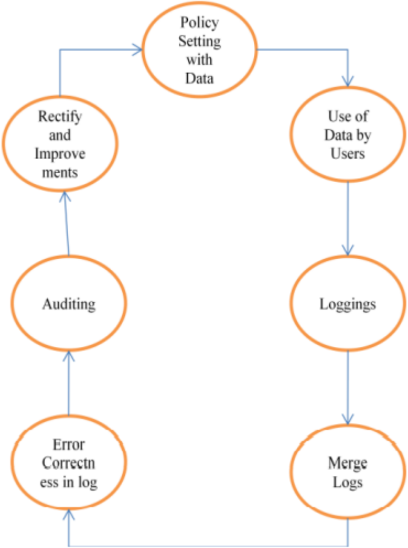
Accountability helps to

- Trace the user's data
- Protect sensitive confidential information
- Enhance user's trust in cloud computing

A cloud is accountable if:

- Faults can be reliably detected
- Each fault can be linked to one party (customer or provider)

Phases of accountability



Proposed system

- information accountability focuses on keeping the data usage transparent and track able and supports distributed environment.
- built on the hide-it-orlose-it perspective-framework provides end-to end accountability in a highly distributed fashion
- accountability is for verification of authentication and authorization
- Data owner will decide the access rules and policies and user will handle data using this rule and logs of each data access have been created.
- 1.Toward Publicly Auditable Secure Cloud Data Storage Services
- 2.. Online data storage using implicit security

Major components:

LOGGER:

- Have logging access to a particular instance of user data Encrypt log record using the public key of the content owner Periodically send the log record to log harmonizer Ensure access usage control policies associated with data are honored

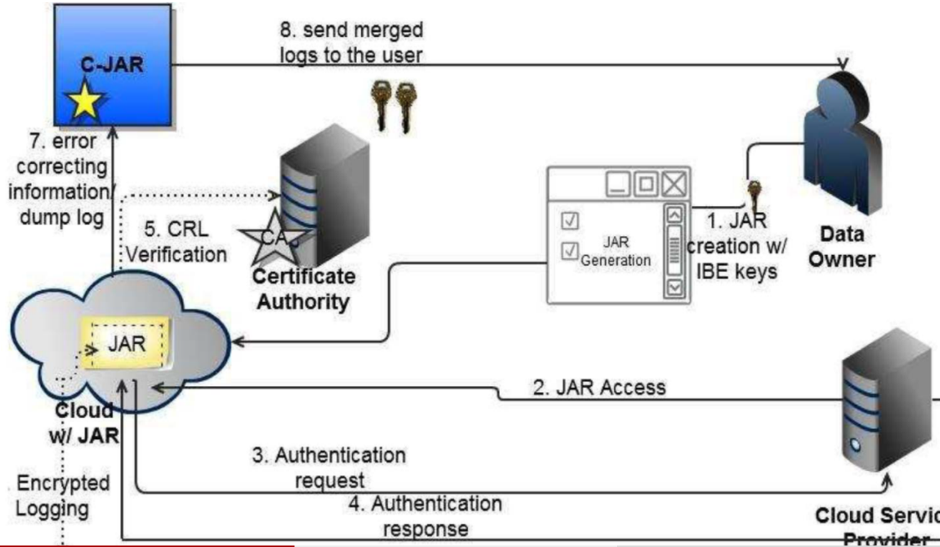
LOG HARMONIZER:

- performs monitoring and rectifying decrypting logs using the master key for integrity verification of logs and error correction, merges and send data to data owner

contd..

- The data owner creates a JAR file that encloses the original encrypted data, the access control policies and the logging policies.
- . Authentication of cloud service provider has been done using open SSL based certificates ,after authentication CSP grants authorised form of access data in JAR based on the previously specified access control rights based on user's role
- The automated logging mechanism is initiated for every data access and the log generator begins to generate log records for every data access in the cloud
- These access control policies are fixed by the data owners based on the user's role to be played in accessing the cloud data.

Accountability mechanism:


C-JAR
8. send merged logs to the user
7. error correcting information/ dump log
5. CRL Verification
CA
Certificate Authority
JAR Generation
1. JAR creation w/ IBE keys
Data Owner
JAR
Cloud w/ JAR
2. JAR Access
3. Authentication request
4. Authentication response
Encrypted Logging
Cloud Servic
Provider

MODES:

PUSH MODE

- In push mode logs are automatically send to data owner
- Here the size of the log record and the maximum time that should elapse before dumping of log files are sent to data owner if violates the fixed value

PULL MODE

- owner can demand logs, so he can see access of his data at anytime, anywhere and he can do monitoring of his data
- used if owner suspects of data being misused

Accountability mechanism:

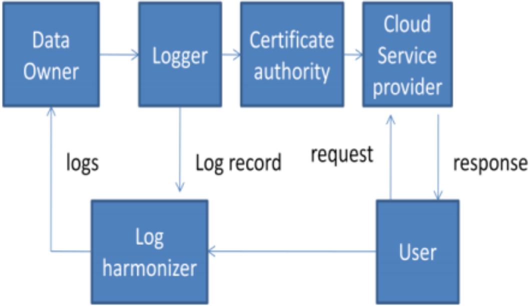


Fig 2: Accountability Mechanism in cloud

Figure 4: Accountability mechanism

cloud data accountability framework

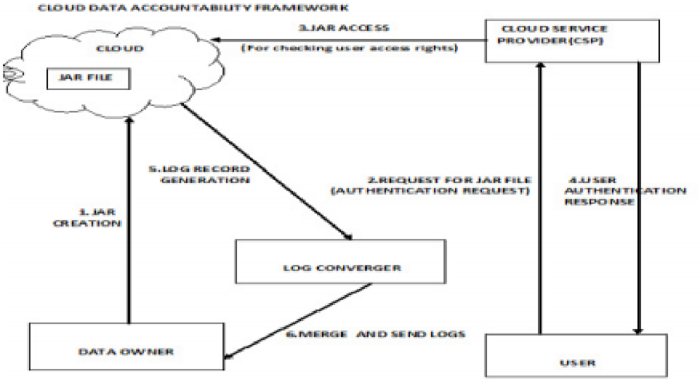

CLOUD DATA ACCOUNTABILITY FRAMEWORK
CLOUD
JAR FILE
3.JAR ACCESS
(For checking user access rights)
CLOUD SERVICE PROVIDER(CSP)
5.LOG RECORD GENERATION
2.REQUEST FOR JAR FILE (AUTHENTICATION REQUEST)
4.USER AUTHENTICATION RESPONSE
1. JAR CREATION
LOG CONVERGER
6.MERGE AND SEND LOGS
DATA OWNER
USER

Fig 1 Cloud data accountability framework

Figure 5: Cloud data framework

Logger structure

outer JAR

- Contains access control policies for each user based on their role
- responsible for user authentication for a particular JAR file based on the specified access rights.
- Contain more than one inner JARs and selects correct inner JAR based on request
- Checking the JVM's validity
- Managing the Graphical User interface

Inner JAR

- consists of the data in encrypted form, class files initiating log generation, displaying data in required format
- Generation of log file for each encrypted data

Structure of JAR File

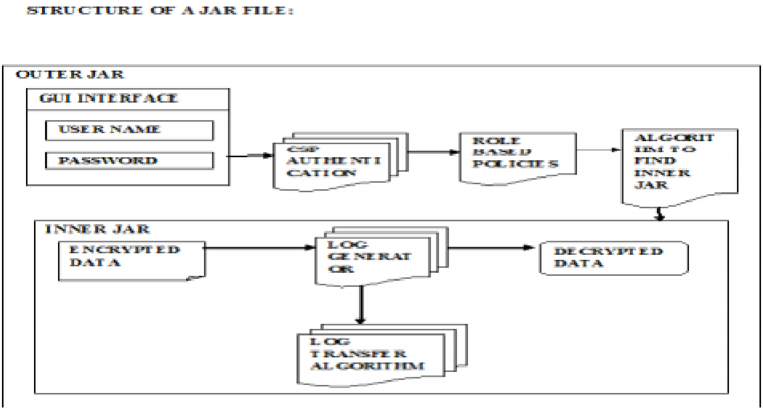


Fig 2 Structure of the JAR File

Techniques proposed with Logging and Auditing

- The logging should be decentralized in order to adapt to the dynamic nature of the cloud
- Every access to the user's data should be correctly and automatically logged.
- Log files should be reliable and tamper proof to avoid illegal insertion, deletion, and modification by malicious parties.
- Log files should be sent back to their data owners periodically to inform them of the current usage of their data.
- The proposed technique should not intrusively monitor data recipients' systems.

Data proprietor in cloud

- The new users can register with the service provider and create a new account and so they can securely upload the files and store it.
- For the security purpose the data owner encrypts the data file and then store in the cloud.
- The Data proprietor can have capable of manipulating the encrypted data file.

JAR File

- JAR file includes a set of simple access control rules specifying whether and how the cloud servers and possibly other data stakeholder's are authorized to access the content itself
- Any access to the data will trigger an automated and authenticated logging mechanism local to the JARs.
- this leads to "strong binding" since the policies and the logging mechanism travel with the data. This strong binding exists even when copies of the JARs are created; thus, the user will have control over his data at any location.

Transition diagram

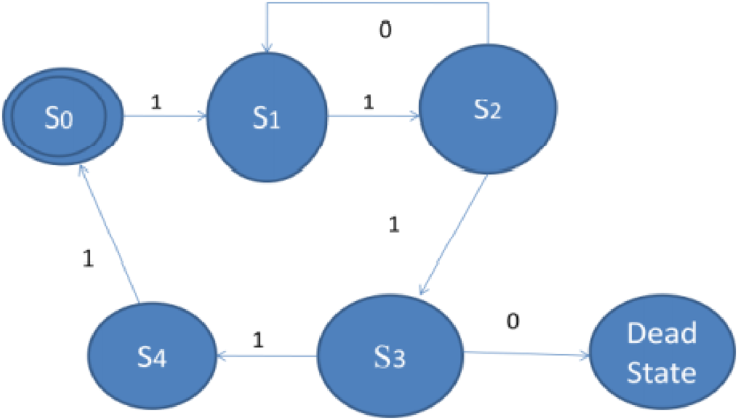


Fig 3: State Transition Diagram

Figure 7: Transition dgm

Transition dgm(contd...)

- Where,
- 0 : Unsuccessful
- 1 : Successful Transition are :
- S0 : Data Owner will send data to logger.
- S1: Data Owner will create logger which is a jar file to store data and policies .
- S2 : Authentication of CSP to JAR file.
- S3 : Authentication of user.
- S4 : owner can see merge log Input: = 0, 1
- Representation of A= (S0, S1 , S2 , S3 , S4, 0, 1, , S0 , S4)
- Input given 11011011
- Expected output (S0,1) = S1 (S1,1) = S2 (S2,1) = S3 (S3,1) = S4 (S4,1) = S0

Transition dgm(contd...)

In accountability mechanisms the log records are generated as access of data in jar happened then it create log record log rec (Lr).

- Lr = r1, r2, r3, r4... rk.
- Parameters uses for log record are rk = (id, action, T, loc, h((id, action, T, loc)ri-1. . . r1), sig)
- Where, rk = log record, id = user identification , action = perform on user's data, T = Time at location loc, loc = Location h((id, action, T, loc)ri-1. . . r1) = checksum component, sig = Signature of record by server,
- Checksum of each record is calculated and it is stored with data
- Checksum is computed using hash function H[i] = f(H[i 1] ,m[i]), Where, Compression function is f = 0, 1 n x 0, 1b 0,1n H[i] = hash value of ith log record [10], [11].

POSSIBLE ATTACKS:

- COPYING ATTACK: The Jar copy attack copies the JAR files and assumes that it will allow him to access the JAR file data without being noticed by the data owner
- DIASSEMBLING ATTACK:Disassemble the JAR file attempt to extract useful information
- MAN IN THE MIDDLE ATTACK: Attacker intercept messages during authentication of service provider with certificate authority, and reply messages
- COMPROMISED JVM ATTACK: Attacker try to compromise the JVM

CONCLUSION

- This paper presents effective mechanism, which performs automatic authentication of users and create log records of each data access by the user.
- Data owner can audit his content on cloud, and he can get the confirmation that his data is safe on the cloud.
- Data owner also able to know the duplication of data made without his knowledge.
- Data owner should not worry about his data on cloud using this mechanism and data usage is transparent, using this mechanism.

REFERENCES

1. Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud,", IEEE Transaction on dependable a secure computing, VOL. 9, NO. 4, pg 556-568, 2012.

2. S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud, " Proc First Int'l conf. Cloud Computing, 2009

3. Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" HP Laboratories, pp 1 – 7, HPL-2011

4. R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud Information Accountability (CIA) Framework Ensuring Accountability of Data in Cloud and Security in End to End Process in Cloud Terminology, International Journal of Civil Engineering and Technology, 8(4), 2017

5. S. Nanda, T. Chiueh, A survey on virtualization technologies, Technical Report, ECSL-TR-129, SUNY at Stony Brook, 2005

6. S. Nanda, T. Chiueh, A survey on virtualization technologies, Technical Report, ECSL-TR-129, SUNY at Stony Brook, 2005

7. http://www.bic-trust.eu/files/2013/01/Papanikolaou$_{A}ccountabilityInCloudComputing_{J}une2012.pdf$

THANK YOU....