ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

An overview of Information Accountability for Data sharing in Cloud computing

Vinutha K[1], Ashwini N[2]

Assistant professor, Dept. of ISE, BMSIT, Bangalore[1,2]

Abstract: Cloud computing provides many scalable services. Data of users are usually processed remotely in unknown machines which they do not own or operate. Lack of trust in clouds by potential customers is the key barrier to widespread usage of cloud computing. With the convenience brought by this new emerging technology, users' fear of losing control of their own data. To address this problem, cloud information accountability is proposed to keep track of the actual usage of the owners' data in the cloud. Data owners upload their data on authenticated cloud; authentication is done by generating certificates using SHA 256. For each access to that data by the registered users, the Java Archives will automatically generate a log record including information of the users. Log record includes the information about the users who are accessing the data enclosed in Java Archive, name of the file that is accessed by the users, its file id and duration of access. If any hacker tries to hack the data, hackers log will be generated and does not allow them to download the file. Hackers' details are sent to data owner from mobile cloud server for auditing purpose.

Keywords: SHA256, Auditing, Java archives

INTRODUCTION

Cloud computing is the construct that allows you to access applications that actually reside at a location other than your computer or other Internet-connected device, most often, this will be a distant datacentre. It is a subscription based service where you can obtain networks storage space and computer resources.

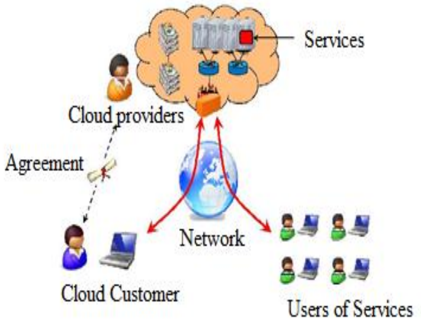


Fig1.1 Cloud Computing

Types of clouds

There are different types of clouds that you can subscribe to depending on your needs [12].

- Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

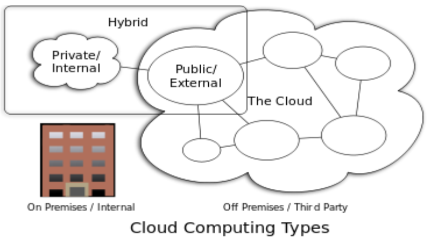


Fig 1.2 Types of Clouds

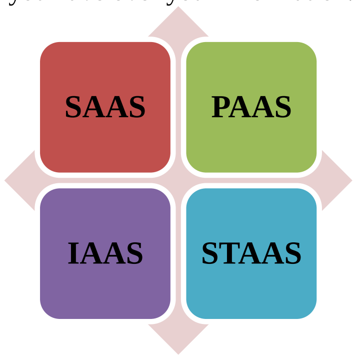
- Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
- Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.

Choosing a cloud provider

Each provider serves a specific function, giving users more or less control over their cloud depending on the type. When you choose a provider, compare your needs to the cloud services available. Your cloud needs will vary depending on how you intend to use the space and resources associated with the cloud. If it will be for personal home use, you will need a different cloud type and provider than if you will be using the cloud for business. Keep in mind that your cloud provider will be pay-as-you-go, meaning that if your technological needs change at any point you can purchase more storage space from your cloud provider.

Cloud service models

There are three types of cloud providers that you can subscribe to. These three types differ in the amount of control that you have over your information.



DOI 10.17148/IJARCCE.2015.4607

1.5 Cloud services

- Software as a Service - A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud.
- Platform as a Service - A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.
- Infrastructure as a Service - An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software that they need.
- Storage as a service (STaaS) - it is an architecture model in which a provider provides digital storage on their own infrastructure. Storage as a service can be implemented as a business model in which a large service provider rents space in their storage infrastructure on a subscription basis. The economy of scale in the service provider's infrastructure theoretically allows them to provide storage much more cost effectively than most individuals or corporations can provide their own storage, when total cost of ownership is considered.
- Storage as a Service is often used to solve offsite backup challenges. Critics of storage as a service point to the large amount of network bandwidth required to conduct their storage utilizing an internet-based service.

Trust in cloud computing
Trust is generally related to “level of confidence in something or someone” hence trust in cloud is as the customer’s level of confidence in using the cloud [10].

Barriers of cloud computing
Lack of consumer trust in CSPs
End users have increased expectations that companies with which they share their data will handle it responsibly
End users perceive a lack of transparency and less control over their data as it shifts to the cloud

- Fear that governments might get access to data in their countries

How to obtain redress in case of a problem?

Difficulty of Compliance for CSPs

- Data flows are global and dynamic

Trans border data flows–international agreements

- Which courts should preside in case of a problem?

Accountability in cloud
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.
Accountability is also defined as “the obligation and/ or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations”, accountability goes beyond responsibility by obligating an organization to be answerable for its actions.

In the context of cloud, accountability is a set of approaches to addresses two key problems:

- Lack of consumer trust in cloud service providers.
- Difficulty faced by cloud service providers with compliance across geographic boundaries.

Accountability life cycle
Having an awareness of the key accountability phases will not only simplify the problem, but also allow tool makers and their customersto gauge the comprehensiveness of tools (i.e. whether there are any phases not covered by a tool) [11].
A classification of the different phases may also help researchers to focus on specific research sub-problems of the large cloud accountability problem. These phases are collectively known as the Cloud Accountability Life Cycle (CALC), which consists of the following seven phases.

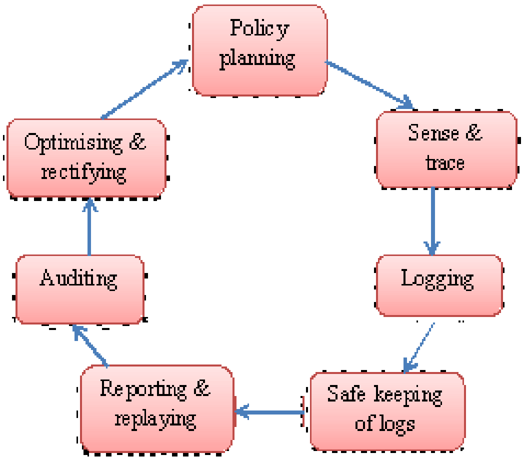


Fig 1.8 The cloud accountability life cycle

- Policy Planning - CSPs have to decide what information to log and which events to log on-the-fly. There are generally four important groups of data that must be logged: Event data – a sequence of activities and relevant information, Actor Data –the person or computer component (e.g. worm) which trigger the event,Timestamp Data –the time and date the event took place, Location Data – both virtual and physical (network, memory, etc.) server addresses at which the event took place.
- Sense and Trace- The main aim of this phase is to act as a sensor and to trigger logging whenever an expected phenomenon occurs in the CSP’s cloud (in real time).

DOI 10.17148/IJARCCE.2015.4607

- Accountability tools need to be able to track from the lowest-level system read/write calls all the way to the irregularities of high-level workflows hosted in virtual machines in disparate physical servers and locations. Also, there is a need to trace the routes of the network packets within the cloud.
- Logging -File-centric perspective logging is performed on both virtual and physical layers in the cloud. Considerations include the lifespan of the logs within the cloud, the detail of data to be logged and the location of storage of the logs. It may in some cases be necessary to pseudonymise or anonymize private data before it is recorded in logs.
- Safe-keeping of Logs -After logging is done, we need to protect the integrity of the logs to prevent unauthorized access and ensure that they are tamper-free. Encryption may be applied to protect the logs. There should also be mechanisms to ensure proper backing up of logs and prevent loss or corruption of logs. Pseudonymisation of sensitive data within the logs may in some cases be appropriate.
- Reporting and replaying -Reporting tools generate from logs file-centric summaries and reports of the audit trails, access history of files and the life cycle of files in the cloud. Suspected irregularities are also flagged to the end-user. Reports may cover a large scope, for example recording virtual and physical server histories within the cloud; from OS-level read/write operations of sensitive data, or high-level workflow audit trails.
- Auditing -Logs and reports are checked and potential irregularities highlighted. The checking can be performed by auditors or stakeholders. If automated, the process of auditing will become ‘enforcement’. Automated enforcement is very feasible for the massive cloud environment, enabling cloud system administrators to detect irregularities more efficiently.
- Optimising and Rectifying -Problem areas and security loopholes in the cloud are removed or rectified and control and governance of the cloud processes are improved.

SYSTEM DESIGN

The overall CIA framework, combining data, users, and logger are sketched in Fig.6. 1. At the beginning, each data owner selects the cloud on which he wants to upload his data, and then creates a pair of public and secret keys for each file using a RSA algorithm. Using the generated key, the data owner will create a JAR file, to store its data items. The JAR file includes a set of simple access control rules specifying whether and how the cloud servers and possibly other data stakeholders (users, companies) are authorized to access the content itself.The data owners can specify the users who can access his data, therefore only registered users will be allowed to access his data and he can also block the IP address of the system whom he don’t want to access his data. Then, he sends the JAR file to the cloud service provider that he subscribes to. To authenticate the CSP to the JAR, signatures are used; authentication signatures are generated by using SHA256 with RSA encryption. In the event that the access is requested by a user, authentication is employed, where in only registered users are authorised to access the data.

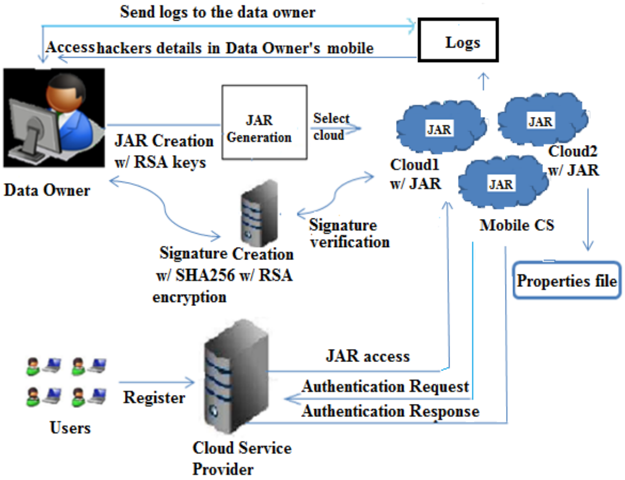


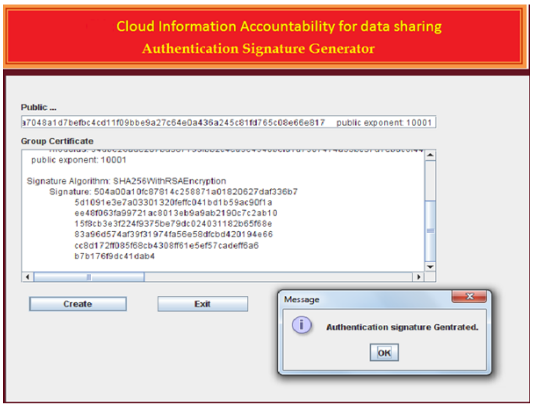
Fig 6.1 Overview of the cloud information accountability.

Once the authentication succeeds, the service provider (or the user) will be allowed to access the data enclosed in the JAR. As for the logging, each time when there is an access to the data, the JAR will automatically generate a log record. Log record includes the information about the users who are accessing the data enclosed in JAR, file name, file id, duration of access and date. Later logs can be accessed by the data owner or other authorized stakeholders by mobile cloud server at any time for auditing purposes.

Authentication signature Generator

Once the data owner creates the JAR file, he sends/uploads the JAR on to the cloud service provider that he subscribes to. To authenticate the CSP to the JAR, signatures are used, where signatures are generated by using SHA256 with RSA encryption.

Data owners can upload his file only when the signature on data owner and signature on cloud server matches, if it doesn’t match, he cannot upload the file and it generates a message as “signature mismatch”.


Cloud Information Accountability for data sharing
Authentication Signature Generator

Public ...

```
a7048a1d7befbc4cd11f09bbe9a27c64e0a436a245c81fd765c08e66e817   public exponent: 10001
```

Group Certificate

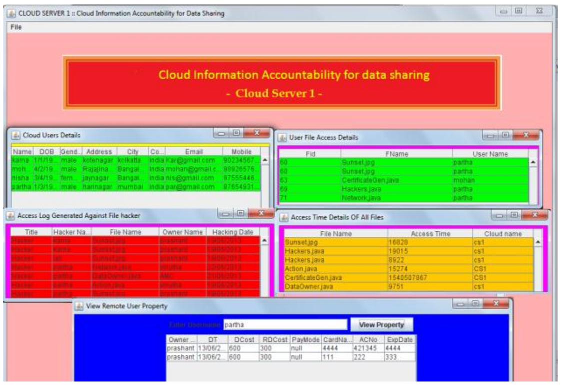
```
  public exponent: 10001

Signature Algorithm: SHA256WithRSAEncryption
      Signature: 504a00a10fc87814c258871a01820627daf336b7
            5d1091e3e7a03301320feffc041bd1b59ac90f1a
            ee48f063fa99721ac8013eb9a9ab2190c7c2ab10
            15f8cb3e3f224f9375be79dc024031182b65f68e
            83a96d574af39f31974fa56e58dfcbd420194e66
            cc8d172ff085f68cb4308ff61e5ef57cadeff6a6
            b7b176f9dc41dab4
```

Authentication signature Gentrated.

Authentication Signature generator

DOI 10.17148/IJARCCE.2015.4607



CLOUD SERVER 1 :: Cloud Information Accountability for Data Sharing

Cloud Information Accountability for data sharing
- Cloud Server 1 -

Cloud Users Details

Name	DOB	Gend...	Address	City	Co...	Email	Mobile
karna	1/1/19...	male	kotenagar	kolkatta	india	Kar@gmail.com	90234567...
moh...	4/2/19...	male	Rajajina...	Bangal...	India	mohan@gmail.c...	98926576...
nisha	3/4/19...	fem...	jaynagar	Bangal...	india	nis@gmail.com	97555446...
partha	1/3/19...	male	harinagar	mumbai	india	par@gmail.com	97654931...

User File Access Details

Fid	FName	User Name
60	Sunset.jpg	partha
60	Sunset.jpg	partha
63	CertificateGen.java	mohan
69	Hackers.java	partha
71	Network.java	partha

Access Log Generated Against File hacker

Title	Hacker Na...	File Name	Owner Name	Hacking Date
Hacker	karna	Sunset.jpg	prashant	19/06/2013
Hacker	karna	Sunset.jpg	prashant	19/06/2013
Hacker	lali	Sunset.jpg	prashant	19/06/2013
Hacker	partha	Network.java	vinutha	12/06/2013
Hacker	partha	DataOwner.java	AMC	21/06/2013
Hacker	partha	Action.java	vinutha	19/06/2013
Hacker	partha	Sunset.jpg	prashant	19/06/2013

Access Time Details OF All Files

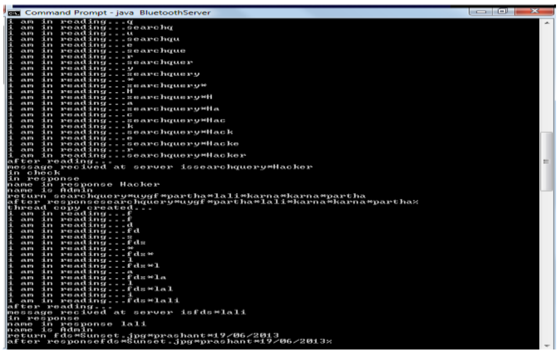
File Name	Access Time	Cloud name
Sunset.jpg	16828	cs1
Hackers.java	19015	cs1
Hackers.java	8922	cs1
Action.java	15274	CS1
CertificateGen.java	1540507867	CS1
DataOwner.java	9751	cs1

View Remote User Property

Enter Username: partha

Owner ...	DT	DCost	RDCost	PayMode	CardNa...	ACNo	ExpDate
prashant	13/06/2...	600	300	null	4444	421345	4444
prashant	13/06/2...	600	300	null	111	222	333

Accountability on CS1 i.e. User details, Access log, hackers' log, user access time details, and property file details on CS1.



Command Prompt - java BluetoothServer

```
i am in reading...q
i am in reading...searchq
i am in reading...u
i am in reading...searchqu
i am in reading...e
i am in reading...searchque
i am in reading...r
i am in reading...searchquer
i am in reading...y
i am in reading...searchquery
i am in reading...*
i am in reading...searchquery*
i am in reading...H
i am in reading...searchquery*H
i am in reading...a
i am in reading...searchquery*Ha
i am in reading...c
i am in reading...searchquery*Hac
i am in reading...k
i am in reading...searchquery*Hack
i am in reading...e
i am in reading...searchquery*Hacke
i am in reading...r
i am in reading...searchquery*Hacker
after reading...
message recived at server issearchquery*Hacker
in check
in response
name in response Hacker
name is Admin
return searchquery*uygf*partha*lali*karna*karna*partha
after responsesearchquery*uygf*partha*lali*karna*karna*partha%
thread copy created...
i am in reading...f
i am in reading...f
i am in reading...d
i am in reading...fd
i am in reading...s
i am in reading...fds
i am in reading...*
i am in reading...fds*
i am in reading...l
i am in reading...fds*l
i am in reading...a
i am in reading...fds*la
i am in reading...l
i am in reading...fds*lal
i am in reading...i
i am in reading...fds*lali
after reading...
message recived at server isfds*lali
in response
name in response lali
name is Admin
return fds*Sunset.jpg*prashant*19/06/2013
after responsefds*Sunset.jpg*prashant*19/06/2013%
```

Hacker's details on data owners mobile

CONCLUSION

By cloud services, users' data are processed remotely in unknown machines that users do not own or operate, hence users' fears of losing control of their own data. The actual usage of the user's data in the cloud is tracked in this approach by using novel cloud information accountability. It is an innovative approach for automatically logging any access to the data in the cloud. This log record consists of name of the user who is accessing file, file name and the data owner name. When any of the hacker tries to hack the file, then it generates log specifying the hacker's information like hackers name, file name, file owner name, hacking date. Hacker's information will be accessed by the respective data owner's in their mobile by mobile cloud server. The proposed approach allows the data owner to audit his data content.

For each of the features in the proposed system that were investigated, a solution that fulfilled the prescribed criteria was realised. In addition, the architectural and functional structure was discussed, in order that information accountability in cloud is better understood.

FUTURE ENHANCEMENT

This project has successfully demonstrated the concept of information accountability in the cloud i.e. each time when there is an access to the data; the JAR will automatically generate a log record. Log record includes the information about the users who are accessing the data enclosed in JAR, file name, time and date. There are number of extensions and improvements that could be carried out.
The future commendable improvements are:

- Privacy and security can be increased by accounting more information about users and hackers.
- In future this approach can be refined to verify the integrity of the JRE and the authentication of JARs.
- This approach can be made possible to support a variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance controls.

REFERENCES

[1] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE "Security and Privacy in Cloud Computing" 2012.

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

[3] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.

[4] W. Lee, A. CinziaSquicciarini, and E. Bertino, "The Design and Evaluation of Accountable Grid Computing System," Proc. 29th IEEE Int'l Conf. Distributed Computing Systems (ICDCS '09), pp. 145-154, 2009...

[5] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a Theory of Accountability and Audit," Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 152-167, 2009.

[6] R. Kailar, "Accountability in Electronic Commerce Protocols," IEEE Trans. Software Eng., vol. 22, no. 5, pp. 313-328, May 1996.

[7] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Proc.First Int'lConf.Cloud Computing, 2009.

[8] S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.

[9] A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing Information Leakage from Indexing in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2010.

[10] Markus Kirchberg, Qianhui Liang, Bu Sung Lee Trust Cloud: A Framework for Accountability and Trust in Cloud Computing, 2011.

[11] Ryan K L KO, Bu Sung Lee, Siani Pearson 2Towards Achieving Accountability, Auditability and Trust in Cloud Computing.

[12] The Basics of Cloud Computing, Alexa Huth and James Cebula © 2011 Carnegie Mellon University. Produced for US-CERT, a government organization.

[13] P. Mell and T. Grance.The NIST Definition of Cloud Computing (Draft). [Online] Available: www.nist.gov/itl/cloud/upload/cloud-defv15. pdf., Jan. 2011.

DOI 10.17148/IJARCCE.2015.4607