ISSN:0975-9646

Effective Distributed Accountability for Data Shearing In cloud

Rahul H. Bhole, Ganesh K. Pakle

Department of Information Technology,
SGGS IE & T, Nanded,
Maharashtra, India-431606

***Abstract*—In the Internet world Cloud computing is the next development stage which will provide the services that are required for everything from computational power to computational infrastructure, business processes, applications to personal collaboration can be delivered to you whenever and wherever you want. Privacy protection techniques only focusing on controlling the cloud environment, that's why research is needed in the area of accountability and auditing. This paper represents a framework for distributed accountability and auditing which is used to protect user's data as well as monitor the actual usage of data provided through cloud services. In order to control the usage of data distributed auditing mechanism is followed and information of the user is collected simultaneously.**

Keywords *Cloud computing, auditing, data sharing, accountability*

I. Introduction

Cloud computing is the software application which will provide data storage capability and access over the internet. Cloud computing is the next generation technology which will dynamically delivers information, resources, capabilities and resources as a services over the Internet. There are three building blocks of cloud computing, software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a service (Iaas). All these allow user to run applications and to store data online. Each offers different levels of user flexibility and control.

SaaS allows user to run existing online applications, PaaS allows to create their own cloud applications using tools and languages, and Iaas allows to run any application they please on cloud hardware of their own choice. Cloud computing has following attributes:

1. Service-based
2. Scalable
3. Shared
4. Metered by use
5. Virtualized resources

As per todays use of computer and internet this cloud will provide the access to low-cost, ultra lightweight devices and inexpensive, handheld devices which are built based on Google's Chrome Operating System or on Google's Android. While some introductory books about Cloud Computing have been describing how to use the cloud computing services provided by several sites such as Google and Amazon, there are few books which will concentrate on the vendors, enterprises and services they provide.

There are three key benefits of cloud computing:

1. Speed and Time to market.
2. Free up your IT staff to do more valuable work.
3. Lower your costs.

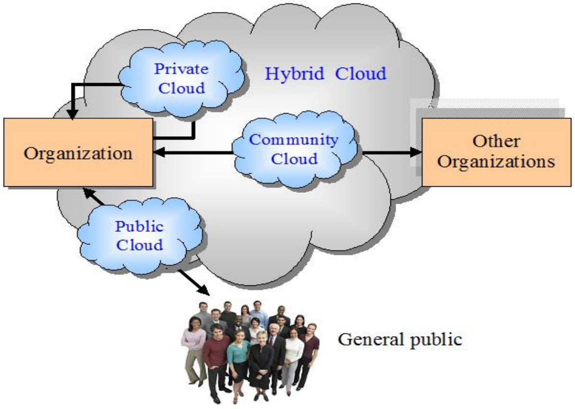

Figure 1: Cloud Computing Architecture

Privacy plays an important role to provide rights through many techniques which are proposed under different systems and security models. Data can be outsourced by the direct cloud service provider (CSP) to other systems in the cloud and these systems can also allocate the task of data management to others, and so on. Being flexible in nature users are allowed to join and leave cloud on their wish. So the data handling takes place through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

II. Related Work

Security plays a vital role in cloud computing, there are many techniques are available for applying the security policy:

i. Deny from the storing of sensitive information in the cloud.
ii. Carefully read out the user agreement policy to find out how your cloud service storage will work.
iii. Encryption
iv. Use an encrypted cloud service.

In paper [1], the authors have proposed an agent-based system which is related to grid computing. The software agent follows distributed jobs, along with the resource consumption at local machines. Accountability policy is related to ours, but it is focused on resource consumption and on tracking of sub jobs processed at multiple computing nodes, rather than access control. In paper [2], the authors propose automatic logging mechanism in the cloud system. As per our knowledge, this is the first time a systematic approach to data accountability through the novel usage of JAR files is proposed. Their proposed architecture is platform independent and highly decentralized, which does not require any dedicated authentication or storage system in place but here multiple jar files takes lot of time to execute. In [3], the authors explain their scheme of auditing and support the batch auditing for multiple owners. Due to the large number of data tags, their auditing protocols may incur a bulky storage overhead on the server. The notion of ABE was first introduced by Sahai and Waters [4] as a new method for fuzzy identity-based encryption. The primary drawback of the scheme in [4] is that lacks of expressibility. Some of the efforts followed in the literature to try to solve the expressibility problem. In the ABE scheme, cipher texts are not encrypted to one particular user as in traditional way of public key cryptography. Rather, both cipher texts & users decryption keys are associated with a set of attributes or a policy over attributes. User is able to decrypt a cipher text only if there is a match between his decryption key and the cipher text. ABE schemes are classified into key-policy attribute based encryption (KP-ABE) and cipher text-policy attribute- based encryption (CP-ABE), depending how attributes and policy are associated with cipher texts and users' decryption keys [5].

III. Distributed Accountability And Auditing

Cloud computing over the internet will provide the services to multiple external customers by means of resources are stored, scaled IT related capabilities and are billed and there is a considerable growth in the usage of this service. Amazon is the leader in the field of cloud computing. It must need to define what is mean by accountability.

A. What is accountability?

Accountability is the term having variety of different meanings within and across the disciplines. For example, in computer science, the term accountability has been used for to refer to an imprecise requirement that i met by reporting and auditing mechanisms.

Accountability is the management of usability, integrity, availability and security of the data used, stored, or processed within the organization. Protection access have affected by public law, regulations and rules and premised upon command and control over the regulatory strategies. Accountability is in our sense, which will be achieved via a combination of private and public accountability [6] [7].

B. Benefits of accountability

Transparency in cloud computing is important for legal and regulatory reasons, and also to avoid violation of social norms. The corporate user provides transparency and assurance to the client by their privacy policy, while requiring the similar assurances from the Service Providers through contractual measures and audits.

Accountability helps to user's trustworthiness. When it is not clear to individual, so why their secure private information is requested and by whom it will be processed, this lack of control will lead to wariness. There are also some security-related concerns about whether data in the cloud will be protected.

IV. Cloud Information Accountability

CIA framework represented in this paper solves above problems and fulfill all requirement.

A. Major components

There are two major components of CIA are present, first is logger, and second is log harmonizer. The data can be downloaded by using logger, when customer requires the data and it will be provided by cloud service provider. Logger keeps track of each copy of all user data and maintains logging access to that copy. Log harmonizers responsibility is to allow users to access the log files created by logger. Log harmonizer is the central system which connects all loggers together.

B. Data flow

Based on Encryption algorithm, each user creates a pair of public and private keys. By using these keys, the user will create a logger which is a JAR file which stores its data items. Rules governing access control of the data is kept in JAR file. It manipulates the user's data by the stakeholders in the cloud. Only recognized users can have access to the data.

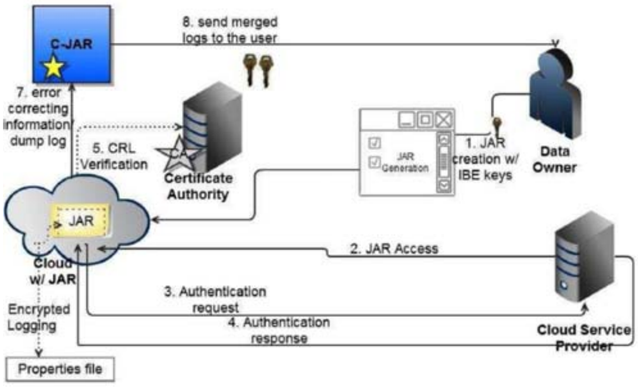

Figure 2: CIA Framework

Then, the JAR file is given to CSP according to which he has to work. To authenticate this JAR files CSP uses the certificates from the trusted third party.

When authentication is done cloud service provider will give access to customer of the user after the completing subscription of the user's service. JAR gets downloaded at customers place. According to the access control rules which are set during creation of JAR it keeps track of usage and maintain logging. JAR will generate a log record automatically when there is access to user's data.

The logs are stored along JAR and encrypted using public key to avoid unauthorized access to the log. For all JAR files user can give same pair of key, and also can use different pair of keys. Correction can be done by the log harmonizer if any error is occurred during log creation. A user can verify the log by decrypting the JAR by his private key, and also auditing is done by the log harmonizer.

V. Future Scope

In the future, we plan to refine my approach to verify the integrity of the JRE and the authentication of JARs. For example, we will investigate whether it is possible to leverage the notion of a security. This research is aimed at providing software tamper resistance to Java applications. In the long term, we plan to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of traveling content. We would like to support a variety of security policies, like indexing policies for text files, usage control for executable, and generic accountability and provenance controls.

VI. Conculsion

In future we would like to enhance a cloud, on which we will install JRE and JVM, to do the validation of JAR. Refine to enhance the protection of accumulated data and to reduce log record generation time.

References

[1] W. Lee, A. Cinzia Squicciarini, and E. Bertino, “The Design and Evaluation of Accountable Grid Computing System”.

[2] 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.

[3] C.Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in INFOCOM. IEEE, 2010, pp. 525–533.

[4] As A. Sahai and B. Waters, “Fuzzy identity based encryption,” in Proc. Acvances in Cryptology—Eurocrypt, 2005.

[5] ZhiguoWan, Jun’e Liu,Robert H. Deng, ”HASBE: A Hierarchical Attribute-Based Solution for flexible and Scalable Access Control in Cloud Computing”

[6] B. Chun and A.C. Bavier, “Decentralized Trust Management and Accountability in Federated Systems,” *Proc.Ann. Hawaii Int’l Conf.System Sciences (HICSS)*, 2004.

[7] P.T. Jaeger, J. Lin, and J.M. Grimes, “Cloud Computing and Information Policy: Computing in a Policy Cloud?”*J. Information Technology and Politics*, vol. 5, no. 3, pp. 269-283, 2009