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 today's 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.

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],
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. Conclusion

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


