Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.181 – 186

SURVEY ARTICLE

Survey on Distributed Accountability for Data Sharing in the Cloud

K.S.Khadke[1], Prof. Umesh.B.Chavan[2]

[1]Department of Information Technology, Walchand College of Engineering, Sangli, India

[2]Department of Information Technology, Walchand College of Engineering, Sangli, India

[1]Email: kunal18689@gmail.com; [2]Email: umesh.chavan@walchandsangli.ac.in

Abstract ---Cloud computing makes highly scalable services to be used over Internet on as per need basis. In cloud the user data is processed remotely on unknown machines. Cloud computing has some risks for both the customer and the cloud provider. Usually cloud computing services are offered by a third party provider who owns the infrastructure. It moves the application software (services) and databases (financial, health) to the data centers of CSP, where the controller of the data and services may not be fully trustworthy which have not been well understood. This paper presents a review on new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable framework and often virtualized resources as a service over the Internet.

In cloud whenever a problem occurs it is hard to know mistake is from user or cloud service provider. In this technology user fears of loss of his own personal data. How to provide appropriate privacy protection for cloud computing is important. To solve this problem we propose data accountability approach to keep track of usage of user's data in the cloud. We create JAR programmable files to ensure user's data authentication and automated log in JARs.

Index Terms---Cloud computing; accountability; data sharing; privacy.

I. INTRODUCTION

Cloud computing is new technology which is used by many companies nowadays. User stores his personal data on cloud server and access it through internet. The actual location of data server is unknown to the user. They fears of loss of data, unauthorized access to data. The cloud computing is, simply, that computing resources which are remain unused during mean time that we give on rent to other organization. Cloud computing is the new evolution of on demand computing power, services and products. Cloud computing is a means by which highly scalable and fully technology based services can be easily consumed over the internet on an as-needed basis. Cloud computing is the technology of visualization of resources .This technology leads security risks and data privacy. A significant barrier to the adoption of cloud services is thus user

fear of confidential data leakage and loss of privacy in the cloud. Privacy is an important and fundamental human right that encompasses the right to be left alone, many techniques is proposed under different systems and security models. The user cannot trust on the cloud service provider, so make trust between both the parties they need some mediator between them that is the trusted third party auditor TPA.

In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public audit ability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. Moreover, for efficiency consideration, the out-sourced data should not be required by the verifier for the verification purpose The other important concern among previous designs is that of supporting dynamic data operation for cloud data transfer and security applications. In Cloud Computing, the remotely stored private and personal data might not only be accessed but also updated by the clients such as through block modification, deletion and insertion, The user (customer) uses cloud to provide his service to its customer. Service S is stored on CSP server but it is unknown to user. Hence there should be mechanism by which user can track his data or service.

To solve user's problem we need a mechanism which monitor the usage of user's data in the cloud. The solution to this is Cloud Information Accountability (CIA). Accountability is a set of approaches to addresses two key problems lack of consumer trust on CSP and difficulty faced by CSP with compliance across geographic boundaries. Information accountability is keep the data usage transparent and tractable [2].CIA provides usage control, access control and authentication.JAR (Java Archives) files are used in the CIA framework. User can set any access policy for their data in the JAR files and automatically log the usage of user data. This framework is platform independent is more advanced than traditional access control.

II. **CLOUD TRUST**

Trust means the user have confidence about privacy, security, accountability, and auditability mechanism provided by the CSP [3]. The CSP should provide more security mechanism so that unauthorized user can't access data. Privacy stands for protection of data over leakage of data. Accountability means obligation of the service policies defined by the user is followed or not, that is only allowed users of service can use the service. Auditability means how the system maintained records and systems that enable efficient auditing of processes within the cloud.

III. **ACCOUNTABILITY**

Cloud computing is technology where massively scaled IT related capabilities are provided as a service across the internet to multiple external customers and are billed and there is a considerable growth in the usage of this service. Amazon is the pioneer in this field. It is important to define what is mean by 'accountability' as the term is susceptible to a variety of different meanings within and across disciplines. For example, the term has used for a number of years in computer science to refer to an imprecise requirement that is met by reporting and auditing mechanisms.

A. WHAT IS ACCOUNTABILITY?

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

Accountability is corporate data governance (the management of the usability, availability, integrity and security of the data used, stored, or processed within an organization). Protection approaches have heavily influenced by public law, rules and regulations and premised upon command and control over the regulatory strategies. However, such legislative and regulatory mechanisms have declined in effectiveness as technological developments render the underlying regulatory techniques obsolete.

Accountability in our sense will be achieved via a combination of private and public accountability [4] [5].

B. BENEFITS OF ACCOUNTABILITY

Individuals should be adequately informed about how their data is handled within the cloud and the responsibilities of people and organizations. Transparency in cloud computing is important not only for legal and regulatory reasons, but also to avoid violation of social norms.

The corporate user provides assurance and transparency to the customer/client through its privacy policy, while requiring similar assurances from the SP through contractual measures and audits.

Accountability helps user trust. When it is not clear to individual why their secure private information is requested, or how and by whom it will be processed, this lack of control will lead to distrust. There are also security-related concerns about whether data in the cloud will be adequately protected.

Most data protection regimes require a clear allocation of responsibility for the processing of PII, as existing regulatory mechanisms rely heavily upon user and regulator intervention with responsible parties. Such as mobile e-commerce and cloud computing, can hinder determination of that responsibility. As information is shared and processed within the cloud, pre-empts perceptions of regulatory failure, which is also permits companies to assess their trading risks in terms of potential financial losses and data privacy data. This knowledge can be used to establish organizational and group privacy data and the available security standards, and to implement due diligence/compliance measures

Which conform to regulatory parameters, but which are otherwise negotiable between contracting organizations, Based on relevant operational criteria.

Accountability helps ensure that the cloud service complies with laws, and also the mechanisms proposed in this paper help compliance with cloud provider organizational policies and auditing [5] [6].

C. PROBLEM STATEMENT

A customer is interested in running serviceS on the cloud, which can be accessed by its customers. For this customer makes agreement A with cloud service provider how to run and who are the stakeholders. The customer has no control on physical server where its service application is stored and he cannot check status.

As the above scenario we noticed some observations a user who wants to use the service sends its information to cloud service provider, then CSP check the access permissions for that user (if he subscribed that service) then access is given.

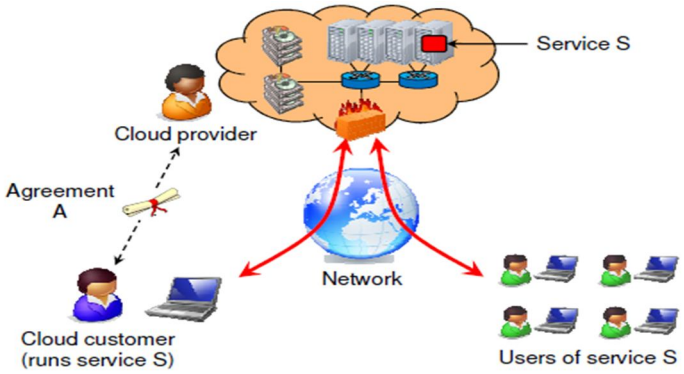

Fig. 1.Cloud computing scenario with Cloud customer, Cloud provider and User

To maintain the track of usage of data we develop logging and auditing. This satisfy following requirements

1. The logging must be decentralized as the cloud is distributed in nature.
2. Each access to the user's data must be correctly logged.
3. Log files must reliable and tamper proof.
4. Log files must send back to data owner.

IV. CLOUD INFORMATION ACCOUNTABILITY

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

A. MAJOR COMPONENTS

There are two major components of the CIA, first is the logger, and second is the log harmonizer. The logger is gets downloaded with the data when customer access the data, and it get copied whenever the data are copied. Logger keeps track of each copy of user's data and maintains logging access to that copy. The log harmonizer is the component which helps the user to access the log files created by logger. All logger are centrally connected to log harmonizer.

B. DATA FLOW

First, each user creates a pair of public and private keys based on Encryption algorithm. Using these keys, the user will create a logger which is a JAR file, to store its data items. The JAR files contain rules for the access control of the data. It is responsible for handling the user's data by the stakeholders in the cloud. Only authorized users can access the data.

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.

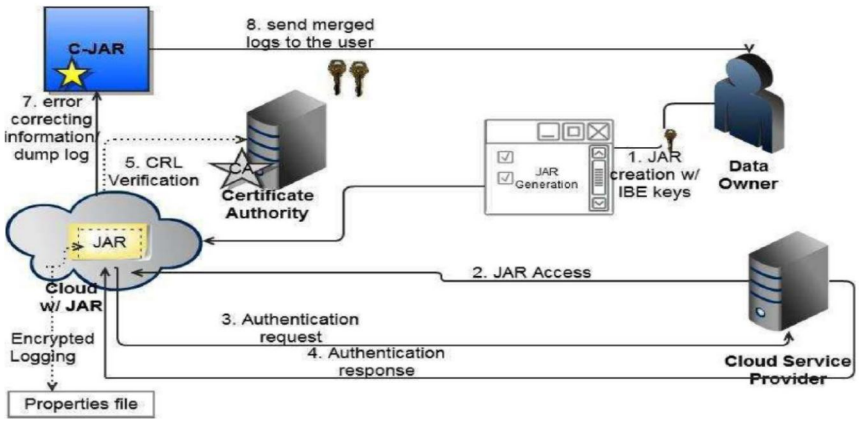

Fig. 2.Overview of the CIA framework

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

The logs are stored along JAR and encrypted using public key to avoid unauthorized access to the log. User can give same pair of key to all JAR files, also can use different pair of keys. The log harmonizer will make correction if any error is occur during log creation. The logs are verified by the user by decrypting the JAR by his private key, also auditing is done by using log harmonizer[2].

V. CONCLUSION

It is more and more important to defend and preserve people's privacy on the Internet, against unwanted and unauthorized disclosure of their confidential data. Despite laws, legislations and technical attempts to solve this problem, at the moment there are no solutions to address. Throughout this paper, the authors have systematically studied and review the security and privacy issues in cloud computing. We have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-pre servability). Cloud computing is a new term that is introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the consumers. Some security issues and their counter measures are discussed in this paper. It has several models to protect its data for the business users. An organization used private clouds within its organization to prevent from loss of data. Security in cloud computing consist of security abilities of web browsers and web service structure. We also discussed the cloud information accountability framework for data sharing in the cloud.

ACKNOWLEDGMENT

We express our sincere thanks to all the authors, whose papers in the area of Cloud accountability are published in various conference proceedings and journals.

REFERENCES

[1] Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin,"Ensuring Distributed Accountability for Data Sharing in the Cloud," *IEEE trans on dependable and secure computing*, vol. 9,no. 4,JULY 2012.
[2] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," *Proc. IEEE Int'l Conf. Cloud Computing*, 2011.
[3] Ryan K L Ko et al. "TrustCloud: A Framework for Accountability and Trust in Cloud computing," *HPL*-2011-38.
[4] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," *Proc. Ann. Hawaii Int'l Conf.System Sciences (HICSS)*, 2004.
[5] 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.
[6] S. Pearson and A. Charlesworth," Accountability as a way forward for privacy protection in the cloud," *Hewlett-Packard Development Company* (HPL-2009-178), 2009.

