A Survey on Accountability of Data usage in Cloud Computing

Nitin P. Doiphode, Prof. H. P. Channe

Abstract— **Cloud computing is an emerging technology which is running on a distributed network. Cloud computing provides many services to the users over internet like computing and storage. These services are on demand services to the customers and customers need to pay as they use these services. Many users use storage services to store their large amount data to the cloud. These outsourced data can be private, so that it should not be disclose to unauthorized cloud users. Users should have the control over their data in cloud, but when user uploads his data to the cloud, he does not know that who is going to use his data over the cloud. All accesses to the user's data should be transparent to the data owner then trust between the cloud users and cloud service providers will increase.**

Accountability can help to increase the trust among the cloud users and cloud service providers. In this paper, we have done survey on the accountability of data usage in cloud. The accountability can ensure the integrity of data and can help cloud users to monitor their outsourced data and helps to check whether their data is handled according to the service level agreements. Accountability consists of logging of actions and auditing of these actions performed.

Index Terms— **Accountability, audit, privacy, security.**

I. Introduction

Cloud computing is an emerging technology which runs on a distributed network. Cloud computing provides many services to the users over the internet like computing and storage. These services are on demand services to the customers and customers need to pay as they use these services like no. of CPU cycles, storage capacity and network bandwidth. In this paper, we are focusing on cloud storage used for data storage by individuals and organizations. The data stored on cloud can be sensitive and private; hence it should not be open to unauthorized access. Data owner needs to ensure the integrity and security of his outsourced data. In this scenario, accountability may help to cloud users to trust more on cloud service providers.

Now days, many people are using cloud storage as their storage solutions or for the backup. These increasing numbers of users have a question about the security of their outsourced data in cloud storage. Any access to the outsourced data needs to be made transparent to the data owner; this can be achieved by accountability in cloud. Accountability can assure to cloud user that his data on cloud storage is safe and he should not worry about the security of the data.

This paper mainly focuses on cloud storage and accountability of data usage in cloud. Initially we have discussed cloud storage and its types, then accountability in cloud computing and finally some issues and problems in cloud computing related to security and privacy. Further we discussed how accountability can help to improve the relationship among the cloud service provider and cloud users.

II. Cloud Storage

Cloud storage provides online storage of data in cloud, from where an individual or an organization can store and access their data in distributed manner. Cloud storage stores data in logical pools which spans over multiple physical storage servers. Cloud users take this physical storage on lease from service providers. Cloud storage can be used as secondary storage for mid-size and small organizations.

Basically, cloud storage is of three types: public, private and hybrid. As per the needs of the storage, customer can choose which cloud storage to be use.

A. Public cloud storage

As the name suggests, this cloud storage is public to all authorized users such as an organization or any individual. There can be some security problems in public cloud storage as it open to all. A small and mid-size organization uses public cloud storage as archival or backup disaster recovery.

B. Private cloud storage

This cloud storage is limited to single person or company. Private cloud storage can be hosted by two ways such as outsourced and on-premise. In outsourced, host manages administrative tasks of storage; still this cloud storage remains private to the customer. On-premise hosted cloud storage is fully managed by customers only.

C. Hybrid cloud storage

This is the combination of public and private cloud storage. As per the customer's requirement, we can customize the cloud storage to get the benefits from both the public and private cloud storage. If the data is more sensitive then we will use private storage for this and the data which is not much important, then we can place this data into the public storage.

Cloud storage manages the cloud data in objects form with the help of cloud storage gateway. Every object consists of the metadata and unique identifier. Object storage used for

Manuscript received Feb 28, 2014.

***Nitin P. Doiphode**, Computer Engineering Department, Pune Institute of Computer Technology, Savitribai Phule Pune University., Pune, India.*

***Prof. H. P. Channe**, Computer Engineering Department, Pune Institute of Computer Technology, Savitribai Phule Pune University, Pune, India.*

All Rights Reserved © 2015 IJSETR

storing unstructured data sets over cloud and it can be accessible easily using internet.

The advantage of the cloud storage is that user can easily access his files stored on cloud storage any time by using internet connection. One more benefit is that, cloud storage can provide backup to the small and mid-size organizations which will be useful at disaster recovery. Limitation of cloud storage is limited bandwidth, if an available bandwidth is not sufficient i.e. if internet connection is slow then we can get the problem while accessing the files stored on the cloud storage.

III. Accountability in Cloud

Accountability is a mechanism which makes the system accountable and helps to increase the trust among the cloud users and the cloud service providers. A4Cloud project defines the accountability on the basis of three aspects such as accountability attributes, practices, mechanism and tools. Accountability defines governance which responsible for storing, accessing, sharing and processing of the data in cloud according to the service level agreement. Accountability also monitors for SLA violation, loss of physical control over the data and service.

Accountability consists of logging of events in cloud and auditing of these actions. Logging can be performed on services and applications running on virtual machines and also on data usage in cloud storage. Analysis of these generated logs can be called as auditing.

In [8], Smitha Sundareswaran et al presented an object oriented approach for accountability and in [12]-[18] accountability is discussed more in detail. Also

IV. Literature Survey

In this section, we have explained accountability in cloud, auditing and cloud data storage in detail. Now days, cloud computing has many issues related to the security and privacy in cloud.

In [1], Zhifeng Xiao and Yang Xiao discussed many issues related to security and privacy in cloud computing. These issues are based on the five main attributes, which are confidentiality, privacy, availability, integrity and accountability. Confidentiality and privacy are deals with keeping the data confidential from unauthorized users. The more the service is confidential, the more the privacy is provided to the customers. Availability specifies that how much time the data is available for the processing or the services are available to the customers. If the service is no longer available to the customers or quality of service is not meeting the service level agreement, then customers may lose the faith in the cloud service provider. Integrity refers as detection of the any violation to the data stored on the cloud server i.e. any unauthorized changes to the data like read, write and download needs to be visible to the data owners. Finally, the accountability responsible for building the trust relationships among the cloud service provider and cloud users.

Similar to the [1], Ramgovind S. et al presented current challenges and issues in cloud computing [2]. Here, author presented some security requirements to the cloud at each service model and delivery model, which are authentication, authorization, non-repudiation, confidentiality, availability and integrity.

Daniele Catteddu et al defined accountability and presented a model of accountability [3]. This model is based on three aspects, which are accountability attributes, practices, mechanisms and tools. Accountability attributes are the elements which are responsible for the building of accountability; it includes transparency, liability, observability, responsibility, assurance, obligations and sanctions. Accountability practices are set of functions required to make the system accountable. Finally, accountability tool and mechanism are the softwares which help to implement accountability practice sets.

Ryan K L Ko et al presented how we can achieve accountability in cloud and describes how accountability strengthen the trust among cloud service provider and customers [4]. They proposed three layer model for cloud accountability which are system layer, data layer and workflow layer. System layer contains logging of actions and events within some components such as operating system, file systems and network. Data layer contains logging of actions performed on data and entire life cycle of data. Workflow layer relates with auditing of organizational transaction flow in business process. In [5], Siani Pearson also describes how to provide accountability in cloud.

Marianthi Theoharidou et al describe privacy risks in cloud when services, applications and data are transferred from one virtual machine to another or from one physical machine to another [6]. They explained the methodologies, to select which cloud deployment model, which cloud type to use and which cloud service provider is more secure to subscribe. Based on these questions, they performed risk assessment for accountability in cloud. In paper [7], Marco Casassa Mont, et al proposed a privacy model which provides more control to the customer's personal data and manages the accountability information.

Smitha Sundareswaran et al presented a new object oriented approach for accountability of data sharing in cloud [8], in which they are performing the logging of each and every actions performed on the user's data. These generated logs can assure data owner that his data is not accessed by any unauthorized users and the data is handled according to the service level agreement. This scenario supports decentralized accountability framework and contains two major components such as logger and log harmonizer which performs logging and error correction respectively [10].

Cong Wang et al proposed an idea for auditing of cloud storage, in which they have introduced one third party auditor (TPA) to check integrity of outsourced data in cloud [9]. Advantage of this scenario is that, TPA concurrently handles multiple auditing upon different users delegation for better efficiency. But the limitation is that, TPA could learn the outsourced data after the audit, so it may not be trustworthy. In [11], Ming Li et al presented a framework for sharing of patient health records which is patient centric approach and it uses attribute-based encryption (ABE) technique to encrypt each patient's health record files.

S. Pearson et al discussed some privacy issues in [12], and defined accountability as privacy protection in cloud computing. In [13], S. Pearson described a privacy manager to reduce the privacy risk in cloud computing. In [14] and

[15], accountability is presented as a framework and explained logic behind the accountability. In [16], Boyang Wang et al proposed privacy preserving auditing mechanism to audit the shared data storage on cloud. Yan Zhu also proposed an audit service to verify the integrity of outsourced data in cloud [17]. Kan Yang proposed an auditing protocol for cloud data storage [18].

V. Conclusion

In this paper, we have explained how accountability is important for trust establishment between cloud consumers and cloud service providers. Accountability framework can help to monitor the data on cloud storage and whether this data is handled as per the service level agreement. Accountability can ensure the privacy of services, applications and data in cloud. Also we have discussed, some issues and problems in cloud computing related to security and privacy. We referred number research paper and discussed necessity of accountability in cloud computing.

REFERENCES

[1] Zhifeng Xiao and Yang Xiao, “Security and Privacy in Cloud Computing,” *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 2, 2013.

[2] Ramgovind S, Eloff MM and Smith E, “The Management of Security in Cloud Computing,” *IEEE Information Security for South Africa (ISSA)*, 2010.

[3] Daniele Catteddu et al. "Towards a model of accountability for cloud computing services," *Proceedings of the DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC)*, 2013.

[4] Ryan K. L. Ko, Bu Sung Lee, Siani Pearson, “Towards Achieving Accountability, Auditability and Trust in Cloud Computing,” *Springer Advances in Computing and Communications Communications in Computer and Information Science*, Volume 193, pp 432-444, 2011.

[5] Siani Pearson, “Toward Accountability in the Cloud,” *View from the Cloud, IEEE Internet Computing, IEEE Computer Society*, July/August issue, vol. 15, no. 4, pp. 64-69, 2011.

[6] Marianthi Theoharidou, Nick Papanikolaou, Siani Pearson and DimitrisGritzalis, “Privacy Risk, Security, Accountability in Cloud Platforms,” *IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 177 – 184, 2013.

[7] Marco Casassa Mont, Siani Pearson and Pete Bramhall, “Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services,” *Proc. Int’l Workshop Database and ExpertSystems Applications (DEXA)*, pp. 377-382, 2013.

[8] 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.

[9] Cong Wang, S. M. Chow, Qian Wang, KuiRen, Wenjing Lou, “Privacy-preserving public auditing for secure cloud storage,” *IEEE Transaction on Coputers*, 2013.

[10] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, “Promoting Distributed Accountability in the Cloud,” *Proc. IEEE Int’l Conf. Cloud Computing*, 2011.

[11] Ming Li, Shucheng Yu, Yao Zheng, KuiRen, Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,” *IEEE Transactions on Parallel And Distributed Systems*, 2013.

[12] S. Pearson and A. Charlesworth, “Accountability as a Way Forward for Privacy Protection in the Cloud,” *Proc. First Int’l Conf. Cloud Computing*, 2009.

[13] S. Pearson, Y. Shen, and M. Mowbray, “A Privacy Manager for Cloud Computing,” *Proc. Int’l Conf. Cloud Computing (CloudCom)*, pp. 90-106, 2009.

[14] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, “TrustCloud: A Framework for Accountability and Trust in Cloud Computing,” *2nd IEEE Cloud Forum for Practitioners*, 2011.

[15] 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.

[16] Boyang Wang, Baochun Li, Hui Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” *IEEE 5th International Conference on Cloud Computing*, 2014.

[17] Yan Zhu, Gail-Joon Ahn, Hongxin Hu and Yau, S.S., “Dynamic Audit Services for Outsourced Storages in Clouds,” *Services Computing, IEEE Transactions on* Volume 6 , Issue 2, 2013.

[18] Yang, Kan, and Xiaohua Jia. “An efficient and secure dynamic auditing protocol for data storage in cloud computing,” *Parallel and Distributed Systems, IEEE Transactions on* Volume 24, Issue 9, 2013.

Nitin P. Doiphode received B.E. degree in Computer Science Engineering from K.I.T.’s College of Engineering, Kolhapur and currently persuing his M.E. degree in Computer Engineering from Pune Institute of Computer Technology, Pune. His research interest includes in cloud computing and distributed systems.

Prof. H. P. Channe is an Assistant Professor in Computer Engineering department at Pune Institute of Computer Technology, Pune. Her interest includes many areas in networks and security.