Enhancing Accountability for Distributed Data Sharing in the Cloud

MdMasoomRabbani
M.Sc(Computer Sc.), Final Year
School of Computing Science & Engineering,
VIT University, Vellore - 632014, Tamil Nadu, India
masoomrabbani112@ymail.com

IlangoParamasivam
Professor
School of Computing Science & Engineering,
VIT University, Vellore - 632014, Tamil Nadu, India
pilango@vit.ac.in

***Abstract*-In cloud computing environment resources are shared among various clients and it's important for system provider to allocate the necessary resources for the clients. As the sizes of IT infrastructure continue to grow, cloud computing is a new way of virtualization technologies that enable management of virtual machines over a plethora of physically connected systems[13].Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis a major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services [1]. In this paper, the multi-layered architecture is proposed to address accountability of the data while sharing in the multi user, heterogeneous and distributed computing environment. The multi-layered architecture is evaluated and shows that the accountability of the data is ensured which increases the trust between the end user and the service provider.**

***Keywords*-Accountability, Cloud computing, Cloud storage, Data sharing, Security**.

1.INTRODUCTION

The main concept behind cloud computing is here computing is done in remote location. Basically it is done in a virtualization environment implemented on large servers [2]. Cloud computing gives new way of hosting andprocessing of data by providing scalable and often virtualised resources. Now a days there are many commercial cloud service providers are offering service including Amazon,Google, Microsoft, Yahoo and Salesforce etc. The main advantage behind the success of this technology is that anyone can use this technology for that user don't need to be expertise of that technology infrastructure. While enjoying the facility brought by this emerging technology user also started worrying about the fate of their data as they don't know in which machine their data is stored and who is processing their data[12],[14]. This worry has raised so many security issues and it is a known fact that only SLA's(service level agreement) can't give desired security to the user's data . Cloud is a layered architecture where user data is processed by so many service providers and it is highly impossible for the user to track their data[3].

2. PRESENT SCENARIO

Cloud computing has raised a range of privacy and security issues [5],[6],[7]. The user data or application resides in cloud at least for a certain time in that time period those users don't know who is actually handling his/her data or to whom it is passing to control.Till date very few works has been done on this particular area. Pearson et al. have proposed accountability mechanisms to address privacy concerns of end users [7] and then develop a privacy manager [8]. Their basic idea is that the user's private data are sent to theCloud storage in an encrypted form, and the processing is done on the encrypted data. The output of the processing is decrypted by the privacy manager to reveal the correct result. The main issue with the privacy manager is it only gives minimum security to the user's data. Once it is decrypted it does not guarantee the safety of the data.

A significant work is done by SmithaSundareswaran et al.have illustrated the method of automatic and enforceable logging mechanism in the cloud. Using object oriented approach (SDO). They also have illustrated the mechanism of pull mode and push mode. In this paper they have used object oriented technology to ensure transparency in

user's data (using JAR).Another work is by Mont et al. who proposed an approach for strongly coupling content with access control, using Identity-Based Encryption (IBE) [9].In addition our work may be similar to logging mechanism [1] but it's different in terms of mechanism, architecture and goal.

3. ENHANCING THE ACCOUNTABILITY

The cloud computing paradigm is the backbone of various Internet services and increasing fraction of time people spend on computers now-a-days. It allows customers to only pay for the computing resources they need, when they need them. The cost effective manner and to lower the barrier to entry for such applications and it is a cloud-based applications to enabled supports [4] but at the same time the security issues has created the barriers to the wide adoption of the cloud services. Here the proposed multi-layered architecture is defined in view of the specific case scenario.

Suppose Alice wants to upload her data to some Xcloud service. User has the following requirements

a) User wants to sign a formal SLA with the Cloud service provider and user wants that her SLA should be followed strictly.
b) The prospective user can see her application demo for a specific timing.
c) If some user wants to download her application then that user has to get permission from CKG (cloud key generator).
d) User wants to ensure that the cloud service providers of "Xcloud Service" do not share her data with other service providers, so that the accountability provided for individual users can also be expected from the cloud service providers.
e) All the user information who has downloaded Alice's application will be sent to her periodically or it will store in a third party place from there Alice can take them.

Keep above scenario in mind, several guidelines have been stated and the common requirements are also identified to achieve accountability in cloud. As user who wants to join the cloud service has to give his/her personal data as well as access control policies (owner of any application, e.g -Alice).Then the Service provider will have granted access right on the data. After uploading the data in cloud ,it will be fully available to the cloud service provider. In order to track the actual usage of owner data the multi-layered architecture is designed.

4. MULTI-LAYERED ARCHITECTURE

Here the proposed design is a three layered architecture that will ensure the accountability and track the usage of owner's data. This architecture is developed to bring trust between end user and the owner regarding the usage of data. This architecture also enforces the proper handling of the owner's data according to the SLA. Another advantage of this architecture is it can track the usage of data ,in future if any conflict arise then it can easily be trace down by the owner as well as the Cloud Service provider.

4.1 Three layered Architecture

The proposed three layered architecture is stated and the functionality of every layer is discussed with the algorithm towards enhancing the accountability of the data sharing in the multiple, heterogeneous and distributed computing environment. Each layer is co-ordinating with other layers while the data is being shared by multiple users while the privacy preservation is also taken care.

4.1.1Fistlayer – Registration

a) The owner of any application or data will choose the Cloud Service Provider (CSP) according to their business need.
b) A formal Service Level Agreement (SLA) will be signed between the CSP and the owner.
c) The owner can attachits service policy with its service.

Any end user who wants to access the application has to follow several steps. That end user has to go through the specific CSP to avail that application. Steps to be followed

a) User has to give all necessary details and has to agree with the terms and condition of the specific application.
b) Through user's mail id a password will be given to the user to login into the cloud as a valid user.
c) According to the service policy the user can avail the service.

Algorithm

```
If (new user)   // Owner
        then register and complete SLA; // SLA should be signed between CSP and service owner
     else
        login and upload service with service policy; // registered user

 if (new user) // end user
   then register with valid details;
   get new password through mail; //sent by the CKG(cloud key generator)
else
   login;    // already registered users
```

4.1.2 Second layer Security Measures

The second layer security is mainly concern with the end user, this layer will make sure that only authorised users should get all the privileges(according to the service policy). The steps involved in this layer

a)End user can check different applications for a specific time stamp thus we can achieve Alice's second requirements.

b) If that end user wants to download or avail any applications he/user has to ask permission from CKG(Cloud key generator,which is a third party),after getting the key only end user can access specific services by paying it to the owner.

c) The new generated key will be send to the owner along with users IP address and another copy will be send to the CSP(storage), this information will be periodically send to the owner or owner can download it from CSP storage.

d) Thus it is possible to maintain transparency on owners' data usage, in future if any dispute come, they can easily be traced from their log.

Algorithm

```
// this layer is dealing with user key generation and maintaining user log
If (user wants to access service)
{
    Apply to the CKG
       {
            If CKG grant user's request
              {
                 A secret key will be send to the user; // that key user will use at the time of accessing
                That key and user's IP will be sending to owner's mail-id;
                 That key and the User's IP will be stored to the log file; // to maintain access history
              }
else
{
    Wait for the CKG response;
}
```

Thus creating this layer can maintain the access history and keep data usage tranceparent.

4.1.3 Third layer- Service Level Agreement

The third is the last layer will work in between owner and the CSP. This layer will make sure that the signed Service Level Agreement (SLA) is followed. The salient features of this layer is

a) SLA will be followed strictly and automatic update regarding owners' data will be sent to them periodically.
b) If the CSP wants any third party to process its service then owners will get updates regarding the usage of their data and that third party will only have read permission.
c) The hired third party also has to get CKG permission before processing user's data

5. PERFORMANCE EVALUATION

The proposed multi-layered architecture is evaluated by setting up a private cloud infrastructure. The evaluation exhibits that the owners' data remainsmore safe than the conventional cloud security where sensitive data remains secure from external intrusion behind the enterprise firewall [10]. The multi-layered architecture will provide an end to end solution for not only proper data usage but also keep track of data by maintaining user log. The highly de-centralized nature of this architecture makes it user friendly and easy to implement over any type of cloud(public, private or hybrid[11],[15]). Irrespective of the size or data usage in a cloud infrastructure this architecture will make sure that the owners' data is safe and also ensure that the Service Level Agreement is maintained. The multi-layered architecture also helps to modify the Service Level Agreement wherever and whenever necessary as the user log is getting updated dynamically in terms of the accountability.

6. CONCLUSION

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. Cloud computing is currently the latest trend when it comes to online computing, it may help the enterprise and the end user by providing their needs, but the provider has to make sure that they are valuable and customer data is safe.[3].The purpose of this work is to provide a simple yet effective architecture that will give end to end solution for cloud security as wells it will maintain transparency among owner,CSP and End user.

REFERENCES

[1] SmithaSundareswaran, Anna C. Squicciarini, and Dan Lin Ensuring Distributed Accountability for Data Sharing in the Cloud , IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 4, July/August 2012
[2] A short introduction to cloud platform by David Chappel [Aug 2008] .
[3] Secure Cloud Computing with a Virtualized Network Infrastructure, Fang Has, T.V. Lakshman, Sarit Mukherjee, Haoyu Song, Bell Labs, Alcatel-Lucent
[4] T.Dillon, C.Wa, and E.Chang, "Cloud Computing" IEEE Int'I.Conf.AdvancedInfo.Networking and Apps. 2010, pp.
[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] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), first ed. O' Reilly, 2009.
[7] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Proc. First Int'l Conf. Cloud Computing, 2009.
[8] S. Pearson, Y. Usern, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.
[9] M.C. Mont, S. Pearson, and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," Proc. Int'l Workshop Database and Expert Systems Applications (DEXA), pp. 377-382, 2003.
[10] Francesco Maria Aymerich, Gianni Fenu, Simon Surcis. An Approach to a cloud Computing Network.Department of Computer Science.
[11] Peter Mell and Tim Grance, The NIST Definition of Cloud computing
[12] Qian Wang et.all"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"
[13] Ramgovind S, Eloff MM, Smith E The Management of Security in Cloud Computing
[14] Balachandra R K, Ramakrishna P V, Dr. Rakshit A, 'Cloud Security Issues', 2009 IEEE International Conference on Services Computing, viewed 26 October 2009, pp 517-520.
[15] Imad M. Abbadi Operational Trust in Clouds' Environment

AUTHORS

Md.MasoomRabbani received the Bachelor's degree(B.Sc(Hons)) in Computer Science from AliahUniversity,Kolkata,India.Currently he is pursuing his masters(M.Sc) in Computer science from VIT University,Vellore,India. His research interest area is Cloud Computing and data Security.

IlangoParamasivam obtained Ph.D in the area of Data Warehousing and Mining from National Institute of Technology, Tiruchirappalli, India. Presently he is a Professor, Intelligent Systems Division, School of Computing Science & Engineering, VIT University, Vellore, India. His specializations include Data Warehousing & Mining, Text Mining, Image Processing and Network Security. He serves as TPC member in various conferences, including the IEEE International Conferences. He is a member of the IEEE, ISTE and CSI.