EFFICIENT DISTRIBUTED ACCOUNTABILITY AND DATA SHARING IN THE CLOUD

[1]C.VENKATA RAVITEJA, [2]C.V.LAKSHMINARAYANA

Annamacharya institute of technology and sciences, Rajampet-India
Email: cvrteja525@gmail.com, cvlakshminarayana@gmail.com

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. And IT infrastructure proceeds as the amount increases to grow, cloud computing is a new way of virtualization technologies that enable management of virtual machines over a plethora of physically connected systems. Cloud computing provides on demand services. Multiple users need to try and do business of their information exploitation cloud however they get worry to losing their information. Whereas data owner can store his/her information on cloud, he should get confirmation that his/her information is safe on cloud. To unravel higher than downside during this paper this offers effective mechanism to trace usage of information exploitation accountability. Accountability is verification of security policies and it's necessary for clear information access. This implementation shows automatic work mechanisms exploitation JAR programming that improves security and privacy of information in cloud. We provide an effective mechanism known as fog computing to protect user's data from theft by confusing attacker with un useful information. Exploitation this mechanism data owner might apprehend his/her information is handled as per his demand or service level agreement.

Keywords—Cloud Computing, Accountability, Security, Data sharing, Privacy

I. INTRODUCTION

Cloud computing could be a technology that uses internet and remote servers to store information and application. In cloud there's no have to be compelled to install specific hardware, software package on user machine, therefore user will get the specified infrastructure on his machine in low rates. Cloud computing is an infrastructure that provides helpful, on demand network services to use numerous resources with less effort. options of Cloud computing are, immense access of information, application, resources and hardware while not installation of any software package, user will access the information from any machine or any wherever within the world, business will get resource in one place, that's means that cloud computing provides quantifiability in on demand services to the business users. Everybody unbroken their information in cloud, therefore it becomes public therefore security issue will increase towards non-public information. Information usage in cloud is incredibly massive by users and businesses; therefore information security in cloud is incredibly vital issue to unravel. Several users need to try and do business of his information through cloud, however users might not recognize the machines that truly method and host their information. Whereas enjoying the convenience brought by this new technology, users additionally begin worrying concerning losing management of their own information. Cloud provides 3 service models that are; platform as a service, infrastructure as a service and computer code as a service. Underneath the info as a service, this is often having four components as per mentioned below, Encryption and Decryption - For security purpose of data kept in cloud; encryption appears to be accurate security solution. Key Management - If encryption is necessary to store data in the cloud, then encryption keys are not saved, but the user needs key management.

Authentication - For accessing stored data in cloud by authorized users.

Authorization – Rights given to user as well as cloud provider.

To solve the protection issues in cloud; various users can't browse the individual user's data whereas not having access. Data owner mustn't trouble relating to his data, and will not get concern relating to harm of his data by hacker; there is would like of security mechanism that is ready to trace usage of information among the cloud. Accountability is very important for observation data usage, throughout this all actions of users like inflicting of file are cryptographically joined to the server, which executes them as well as it manages protected record of all the actions of past and server can use the past records to grasp the correctness of action. It together provides reliable data relating to usage of data and it observes all the records, therefore it helps in build trust, relationship and name. Therefore accountability is for verification of authentication and authorization. It's powerful tool to ascertain the authorization policies. Accountability describes authorization demand for data usage policies. Accountability mechanisms, that suppose once the actual fact verification are attractive implies that to enforce authorization policies. There are 7 phases of accountability

1. Policy setting with data
2. Use of data by users
3. Logging
4. Merge logs

5. Error correctness in log
6. Auditing
7. Rectify and improvement.

These phases will be modifies as per structure. First information owner can set the policies with data and send it to cloud service supplier (CSP), information are use by users and logs of every record are created, then log are incorporate and error correction in log has been done and in auditing logs are checked and in last section improvement has been done .

II. PRESENT SCENARIO

Cloud computing has raised a range of privacy and security issues. 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 and then develop a privacy manager. Their basic idea is that the user's private data are sent to the Cloud 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) .In addition our work may be similar to logging mechanism but it's different in terms of mechanism, architecture and goal.

2.1Disadvantages

1. Although the Cloud computing is vast developing technology, the database Management system does not have a trustworthiness.
2. Compute power is elastic, but only if workload is parallelizable.
3. Data is stored at an untrusted host.
4. Data is replicated, often across large geographic distances.

III. 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 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).

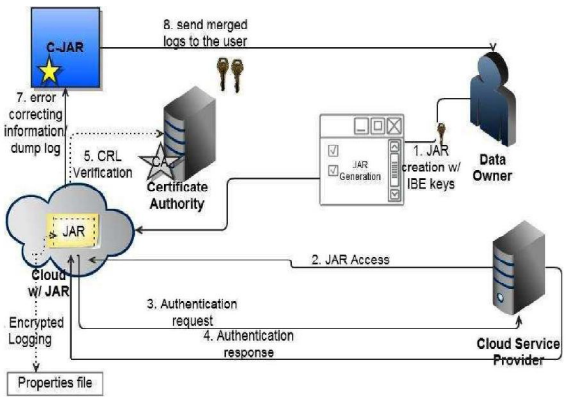

Fig1: Overall Architecture

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.

3.1 Advantages

1. The data is shared in a secured manner.
2. It is a Decentralized
3. Dynamic hierarchy
4. Increasing service level
5. To meet the on demand of the client by improving quality
6. Improving the Quality of service

IV. 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

V. PERFORMANCE EVALUATION

The proposed multi-layered architecture is evaluated by setting up a private cloud infrastructure. The evaluation exhibits that the owners' data remains more safe than the conventional cloud security where sensitive data remains secure from external intrusion behind the enterprise firewall. 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). 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.

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. 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.

FUTURE SCOPE

In future I 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] 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] [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

★★★