2011 International Conference on Computational and Information Sciences

Security and privacy issues within the Cloud Computing

Ziyuan Wang
International School
Beijing University of Posts and Telecommunications
Beijing, China
wangziyuan89@hotmail.com

Abstract— **Cloud Computing has been regarded as evolutionary paradigm recently. It has much strength, such as large storage, ubiquitous network access, cost effective and so on. However it also faces security and privacy concerns. In this paper, we discussed several major security and privacy issues. And we also proposed four effective methods to handle such issues. According to the features of issues, we investigated the feasible solutions and finally found four methods. Such methods can be applied to the generalized Cloud Computing. This paper is original that we consider the characteristics of Cloud Computing adequately, so the methods are well functioned and can be developed further to solve other problems.**

Keywords—Cloud Computing; Security issues; Privacy issues; Security solutions; Privacy solutions

I. Introduction

Cloud Computing is an evolving paradigm with lots of benefits. It can be seen as an integration of traditional computing technologies and network technologies, such as grid computing, distributed computing, parallel computing, network storage technology, virtualization and load balancing. Cloud is regarded as the visual computer resources, which is usually large scale group of servers, including computing server and storage server. Clouds have the computing capability which is equivalent to hundreds of thousands of computers. The main concept of Cloud Computing is to improve the capability of Cloud in order to reduce the computing load of client side. The ultimate goal is to simplify the client side to become the input device, which can take advantage of the powerful computing capability of Cloud.

Cloud Computing have five key characteristics [1], which is shown in the following:

- On-demand self-service: Cloud is a large scale pool of resources. Users need to buy as they demand.
- Ubiquitous network access: Cloud is virtualized devices. As a result, users can acquire the application service at any location with any API. The demanded resources are from Cloud, which is virtualized.
- Cost effective: Cloud realizes the centralized management of resources, which reduce the necessity of the clients to operate the processing.
- Rapid elasticity: The scale of Cloud is dynamic, which is in accordance with the demand of the users.
- High commonality: Cloud Computing is not aimed at specific application. Different applications can utilize the same Cloud resources.

In order to realize the Cloud Computing, three major models have evolved [2]: Software-as-a-service (SaaS), which can reduce the total cost of hardware and software operations; Platform-as-a-service (PaaS), which reduce the cost of managing platform; Infrastructure-as-a-service (IaaS), which reduce the cost of managing the hardware and software infrastructure components.

Although there are many benefits mentioned above, the Cloud Computing unique architecture features raise several concerns about security and privacy issues. The data is outsourced to the Cloud, which minimize the clients' control over their data. Moreover, as users no longer possess the physical data, the primitive protection of data is not feasible any more. So security and privacy issues need to address. Our paper takes discussions about this key issue and brings up some solutions.

The remainder of the paper is structured as follows: Section Ⅱ introduces the primary concerns about the security and privacy issues. Section Ⅲ introduces and discuss the solution of these concerns. Section Ⅳ make the conclusion and point out future works.

II. Key Security And Privacy Issues

A. Security issues

Security issues are treated as the most concerned challenges of Cloud Computing in the latest survey [3]. Cloud is expected to offer the capabilities including: trusted encryption scheme to ensure safe data-storage environment; stringent access control; safe and stable backup of user data. However, cloud allows users to obtain the computing power which exceeds their own physical domain. This leads to several security problems. We will discuss the major security concerns in the following:

- Access control: It is probable for the confidential data to be illegally accessed due to the astringent access control. Unauthorized access may exist if security mechanism is not adequate. Entities in the service chain can easily utilize the vulnerability to access users' data. As data usually exists in the

978-0-7695-4501-1/11 $26.00 © 2011 IEEE
DOI 10.1109/ICCIS.2011.247

Cloud for a long time, the risk of illegal access is higher.

- Authentication and Identification: Multi-tenancy is one of the major features of the Cloud Computing. It allows one single instance of software to serve various clients. However, this will cause authentication and identification problems as well. Due to multi-tenancy, different users may use different identity tokens and negotiation protocols, which will cause the interoperability defects. The data security protection mechanism will become complicated, which is likely to provide chances for malicious utilization.

- Availability: As the client data is virtualized, clients no long possess the physical data. If service or data on the Cloud in not available, it is hard to retrieve the data. So availability is a major concern about the Cloud Computing.

- Policy integration: The Cloud is heterogeneous, which means that different Cloud servers may have different mechanisms to ensure the clients' data security, thus policy integration is one of the concerns. If not addressed properly, security breaches may exist. Problem between Google, Amazon and LoadStorm is one example.

- Audit: As the Cloud Service Provider (CSP) has the powerful control of the data, so it is probable for CSP to copy, move and edit the data in the procession. So there is a need to have a mechanism to audit the process. Users need to make sure that all the activities are traceable so that they can trust the environment. However, there are several aspects unsolved, for example, as data in the Cloud is in huge amount, it is not possible to audit all the data procession. And it is usually hard to determine which data need to audit.[4]

B. *Privacy issues*

Privacy issues are also major challenges in the Cloud Computing, which includes protection of identity information, transaction histories and sensitive data. The idea of Cloud Computing is to transfer the computing load to the shared infrastructure. Such idea will cause the problem that customers' private information faces the risk of unauthorized access and retrieval [5]. We will discuss the major privacy concerns in the following:

- Unauthorized secondary usage: Users' data can be utilized by the Cloud Service Provider in some cases, most commonly form is advertisement. However, there are several usage of data is against users' will, such as junk advertisement. Moreover, such unauthorized usage of data may cause serious security problems, which becomes one significant concern.

- Lack of user control: In the Cloud Computing, Cloud Service Provider is in charge of the data procession. So there is a case that the data procession is not transparent to the users, which means that users have lost the control of the data. Such case raises the concern about the theft and misuse of users' data. Moreover, users' privacy can be easily uncovered. So there is need to establish the privacy protection mechanism to deal with this.

- Unclear responsibility: There is one problem related to the privacy that it is sometimes unclear about which CSP is responsible for privacy protection, detecting who use and modify the user data or ensuring user data privacy requirements [6]. Users are also concerned about whether the rights of data procession of one single third party can be transferred to another third party if bankruptcy is emerged.

III. MOTHODS USED FOR CLOUD COMPUTING

A. *Methods dealing with security issues*

In Section Ⅱ, we discussed the major security issues in the Cloud Computing. There have been several researches and works focusing on dealing with the security issues. Based on the already existed works, we will propose two methods handling the access control aspect and policy integration aspect of the Cloud Computing security issues:

- Access control method: There is one powerful and generalized approach to security management, which is role-based access control (RBAC). We apply the idea of RBAC to the Cloud Computing to work out one algorithm, which is called Cloud-based RBAC. The basic components in the Cloud-based RBAC are: Cloud User, Access Permission, Role and Session. The Cloud User is the client side of the Cloud. Access Permission is an access mode which grants the right to manipulate certain data in the cloud. Role is a collection of permissions needed to operate certain functions in the cloud. Session is a kind of relationship which relates one Cloud User to several Roles [7]. At the beginning of each Session, Cloud Users can request to acquire some of the Roles. Some sensitive request can only be granted if the Role is enabled and Cloud Users acquire the rights to operate the Role. In this way, the malicious attack to the user data can be prevented as such activity user cannot acquire the Access Permission. In order to support the basic components, Cloud-based RBAC defines two assignment algorithms to correlate each other. One is Cloud User Role Assignment (CURA), which is responsible for mapping the sessions to the Cloud Users. The other is Role Permission Assignment (RPA), which is responsible for mapping between one session and several related roles. These two algorithms make the components of Cloud-based RBAC connected together to provide the secure access control. Moreover, to better protect some most important data and data procession, such algorithm defines the disable state for each role. If Cloud User chooses the disable state, then none of the sessions can use this role. In this way, such data is locked until Cloud User wish to make use of.

- Policy integration method: In order to handle the multi-policy problems, we propose the dynamic policy control mechanism, which can dynamically determine the dominant policy during certain data procession. In this data procession, different CSPs have to conform to such policy. The mechanism architecture is shown in Figure 1.

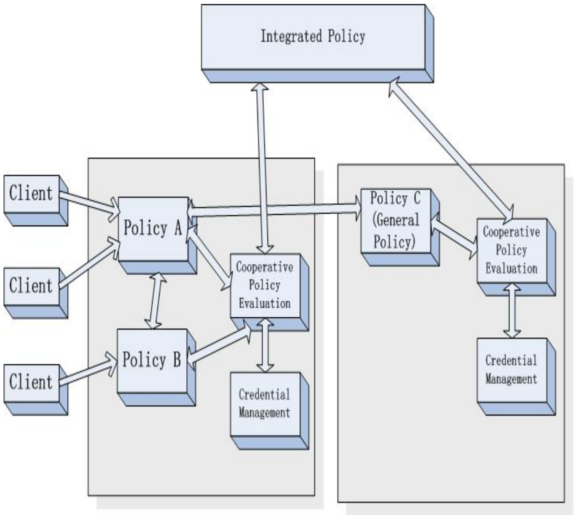

Figure 1 Policy integration mechanism architecture

Policy integration mechanism eliminates the rigid boundaries between different policies. In this architecture, clients will be provided with two secure policies, Policy A and Policy B. In order to achieve the integrated secure policy, such two policies will go through Cooperative Policy Evaluation (CPE) [8], which will evaluate and balance two policies. After CPE procession, an integrated policy is reached. If there is no optimal integrated policy, the Generalized Backup Policy C will be evaluated and treated as the temporal policy for the data procession. Also, in order to improve the trusty of CPE, we can allow the feedback to the CPE. In such means, CPE can dynamically adjust the criteria of judgment to optimize the evaluation.

B. Methods dealing with privacy issues

Apart from security issues are discussed in Section Ⅱ, privacy issues need to call equal attention. There are several works and researches which are focusing on finding solution to the privacy issues. Based on these works, we will propose two methods handling the unauthorized secondary usage and lack of user control aspect of Cloud privacy issues.

- Identity management method: In order to prevent the unauthorized secondary usage of the data, we propose one identification management method. User-centric identity management is proved to be one significant approach to the identity control [9].

We add the Cloud Privacy Label (CPL) to the user-centric identity management to get a mechanism to protect the Cloud users' privacy. In the User-centric identity management, each user is assigned several attributes of the identity. Such attributes are responsible to identify the user and lock out the unauthorized access. Users can manage their own attributes freely according to their will. In this way, other users will have much less opportunity to obtain the identity to access and use the user data, also CSP can release many burden to focus on providing better functions. Moreover, in order to get optimized privacy protection, users can also mange other aspects of the identity attributes, such as semantic. In many researches, privacy protocols are addressed to verify the identity attributes. In this method, we utilize the Cloud Privacy Label to address the privacy issues. CPL is used to represent the privacy sensitivity in the Cloud Computing. During Cloud Computing, CSP and users both set certain CPL before accessing the Cloud data. Then after the comparison between these two CPLs, the CSP can decide whether such user is authorized or not. One CPL comparison rule is presented in [9]:

If $L(r) \geqslant L(u)$, $P(r)$ is satisfied with $P(u)$

If $L(r) < L(u)$, $P(r)$ is not satisfied with $P(u)$

Where $P(r)$, $L(r)$ and $P(u)$, $L(u)$ are referred to CSP privacy label, policy and Cloud user privacy label and policy.

- User control methods:

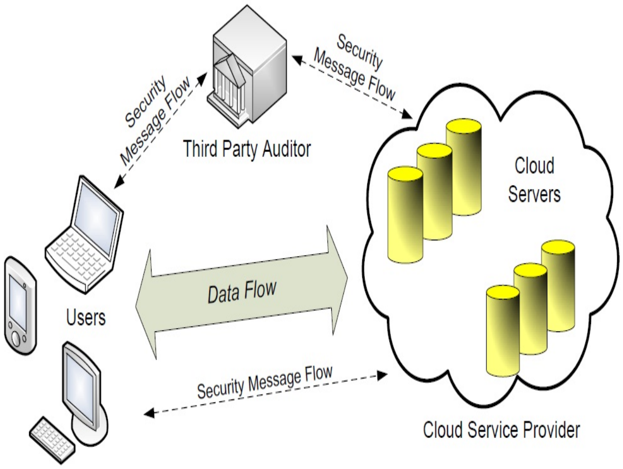

Figure 2 Third Party Auditor architecture [10]

As mentioned before, as the Cloud data is virtualized, Cloud users face the problem that they will lose control of their data. Some CSP chooses private cloud to solve the problem. However, private cloud can only support small scale of users. To address the problem in public cloud or hybrid cloud, we introduce the Third Party Auditor (TPA)

[10] to balance the power between CSP and Cloud users. TPA is on behalf of the Cloud users and obtains the capability which is not available to such users. The responsibility of TPA is to monitor and audit the CSP for data storage and data utilization. In this way, users can have more control of their data, especially sensitive data. There are two phases in this method, Startup and Audit. During Startup phase, users will generate one verification data to the TPA for later auditing use. Then TPA will poll the state of the data and analyze the response data. In such means, users can gain more control on the data and establish more trust with CSPs.

IV. Conclusion

In this paper, we analyze the major security concerns and privacy concerns in the Cloud Computing. In order to handle such concerns, we introduce and propose four effective methods dealing with key security and privacy concerns. These methods can only deal with one or two aspects of Cloud Computing problems, so in order to provide a more secure, privacy-preserving and effective Cloud, some more efficient methods and mechanism have to be proposed.

References

[1] Hassan Takabi, James B.D. Joshi, Gail-Joon Ahn, “Secutity and Privacy Challenges in Cloud Computing Environments” IEEE Computer and Reliability Society, November 2010.

[2] N. Leavitt, “Is Cloud Computing Really Ready for PrimeTime”, IEEE Computer, January 2009

[3] IDC, Enterprise Panel, September 2009, http://www.slideshare.net/HorFigOr/cloud-conputing-2010-an-idcupdate

[4] Hall, J.A.& Liedtka, L.L. “The Sarbanes-Oxley Act: implictions for Large-scale IT outsourcing”, Communications of the ACM, 2007, pp. 95-100

[5] Y.Chen, V.Paxson, R.H.Katz, “What’s new about Cloud Computing security”, tech. report UCB/EECS-2010-5, EECS Dept. Univ of Califonia, Berkeley, 2010

[6] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing”. IEEE, 2009

[7] James B.D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, “A Generalized Temporal Role-Based Access Control Model”, IEEE Computer Society, 2005

[8] S.Ioannidis, “Security Policy Consistency and Distributed Evaluation in Heterogeneous Environment”, doctoral dissertation, University of Pennsylvania, 2005.

[9] Moonam Ko, Gail-joon Ahn, Mohamed Shehab, “Privacy enhanced User-Centric Identity Management”, IEEE International Conference on Communications, 2009

[10] Cong Wang, Qian Wang, Kui Ren, Wenjing Luo, “Privacy-preserving public audting for data storage security in Cloud Computing”, IEEE Communication Society, 2010