TELKOMNIKA, Vol. 11, No. 12, December 2013, pp. 7351~7357
e-ISSN: 2087-278X

A Service Management Mode Dealing with Information Leakage Risk in the Online Payment

Wu Xiaogang*[1], Zhou Weifeng[1], and Du Rongwei[2]
[1]Zhejiang Gongshang University, No.18, Xuezheng Str., Hangzhou, Zhejiang, China, 310018, +86-571-28811455
[2]Chizhou Branch of Agricultural Bank of China, Chizhou, China
*Corresponding author, e-mail: edujob.org@163.com

Abstract

In view of personal information leakage risk in the process of online payment, this study puts forward a cloud protection system which can improve personal information security. The system includes two modules: personal information security model and cloud service providers trust evaluation system. Among them, the personal information security model includes four layers design: the user, interface, platform and management layers. User layer is used to complete the user authentication and login, interface layer is used for the classification and encryption of complex personal information, platform layer is used to complete the data storage, and the management layer is used to guarantee the overall effectiveness of the system work. The cloud service providers trust evaluation system based on the Theory of Membership Degree, can improve the trust assessment level to cloud service providers. This study can ensure the personal information security in the online sales, and be beneficial to the healthy development of e-commerce.

Keywords*: cloud services, online payment, information security*

1. Introduction

With the popularity of Internet, more and more people are accepting this marketing mode of online sales, and the number of people shopping online increases year by year. It also brings up some personal information security problems: some illegal businesses or individuals are logging in the users' computers using the tracking software Cookie or a hacker without the consent of them, and collecting the personal information of users shopping online through methods such as spam mail for illegal profit, with damage to the seller's reputation and buyer's privacy. Network security is, therefore, dual protection for the interests of the online sellers' trust and netizens. The measures for personal information security management in the existing sales network are mainly bank account security, firewall protection and "phishing" prevention, etc. With the expansion of the online business and the upgrading of network security management model, the network must have the ability to solve the burstiness and concurrency of visits and the data security, which requires a strong data service center for the storage of massive data.

In recent years, cloud computing have been applied across all areas. Originated in grid computing, cloud computing belongs to a distributed computing model [1]. To judge by technical means, cloud computing is not an emerging technology, but it belongs to the emerging service mode [2-4]. The computing tasks in cloud computing service mode are not accomplished on the local computer or remote server, but rather on a large number of distributed computers [5-7]. This makes a lot of storage devices connected to form a large-scale resource sharing pool, thus becoming a data service center which has the ability to store huge amounts of data [8].

The introduction of this cloud data service center which is able to handle big data will generate a certain amount of hidden danger to personal information security: users can't control the storage location of personal information in the public clouds. To solve this problem, this study puts forward a cloud service management model with reasonable structure design which can deal with the personal information leakage risk in the online payment.

Received June 27, 2013; Revised August 2, 2013; Accepted August 20, 2013

2. Technical Solution

The technical solution adopted by this study to solve the above problems is: building a personal information security model and cloud service providers trust evaluation system. Among them, the personal information security model includes four layers design: the user, interface, platform and management layers; Based on the Theory of Membership Degree, the cloud service providers trust evaluation system establishes the cloud service providers' behavior trust evaluation algorithm [10]. The specific content is as follows.

2.1. Personal Information Security Model

The personal information security model consists of user layer, interface layer, platform layer and management layer.

(1) The user layer uses both ways including identity authentication mechanism and access control mechanism to complete the user authentication and login. It ensures the security of access permissions and cloud computing platform. The control mode therein is divided into three steps: (a) the user sends request to the cloud, i.e. the description of the resource to access, (b) the cloud parses the information the user requested, and matches with the personal information stored in private clouds, (c) the user layer responses to the result of the second step, and sent the response results to the user.

(2) The interface layer is used to achieve the classification of the users' personal information, gateway filtering and cryptographic operations. Based on the classification of the users' personal information, it achieves the classification storage of the users' key information and general information. Data evaluation and classification are based on: 1) the rating of hazard to the user caused by the leakage of personal information; 2) the degree of secrecy for the data information insisted by businesses. Data encryption is still the best choice for sensitive information. Data encryption storage can ensure the confidentiality of key information on the shared storage platform, by which the security problem of data storage is solved.

(3) The devices of interface layer are set at the site where the private cloud entry and exit is located. The key information after processing through the classification of interface layer, can only flow to the private cloud. If the interface layer encrypts the key information, the encrypted data can also be stored in a public cloud.

(4) The platform layer is used to complete the data storage. It involves two parts-public cloud and private cloud. Strictly speaking, the key information must be stored in a private cloud. But if the key information has been encrypted strictly, such key information can be also stored in a public cloud. General information is also required to pass through cloud computing filtering gateway. The intercepted sensitive information must be stored in a private cloud, and the rest of the filtered information can be stored in a public cloud.

(5) The management layer ensures the whole system can work effectively. It includes risk assessment, strategy formulation, audit and other ways, which is the guarantee and support of the entire model to implement its operation

Color figures will be appearing only in online publication. All figures will be black and white graphs in print publication.

2.2. Cloud Service Providers Trust Evaluation System

The cloud service providers trust evaluation system is based on the theory of membership degree. The system flow includes:

(1) Publishing services, namely, the provider completes its registration from the service registry, and the service registry returns the registered results to the service provider.
(2) The user sends a query request to the registry and the service registry returns the results to the user.
(3) The system queries the trustfrom the trust evaluation center according to the request result, and the system returns the trustresult.
(4) The user chooses the best cloud service provider according to the result.
(5) The service provider returns the chosen provider to the user and the service monitoring center calculates the attribute value.
(6) The service monitoring center sends the assessment to the user.
(7) The user returns the results of assessment.
(8) The monitoring center updates the truststore.

The cloud service provider's performance indicators are monitored by the monitoring center. The service evaluation information obtained by users will be stored in the truststore, which will be stored according to the quintuple of Equation (1):

$$\{S_i, U_i, t, w_n, V_n\}, n = 1, 2, 3, \ldots, N \quad (1)$$

S_i — service providers,

U_i — users,

t — the time provided by Services,

w_n — the attribute,

V_n — the attribute value.

Definition 1: if **a** represents the entity attribute, **X** represents the value for trust level language, and the domain of discourse.

$$\Pi = \{a\} \quad (2)$$

And,

$$\lambda X(a) \in [0,1] \quad (3)$$

Is tenable with regard to:

$$\forall a \in \Pi \quad (4)$$

Then λ will be called the membership function of **X**, and the distribution of the function will be also known as the trusted cloud of **a.**

Definition 2: the trusted cloud is represented by **P**, and

$$P = P(EX, EN, HE) \quad (5)$$

EX — the expectation,

EN — the entropy,

HE — the super entropy.

Further more, the steps computing the attributes of a trusted cloud are shown as follows:

Input: $(a_{1i}, a_{2i}, \ldots a_{ni})$, the **i** attribute evaluation value of **n** entities for the entity X ;

Output: P, the trusted cloud of the attribute **i**.

First, the sample mean will be obtained by:

$$\overline{a_i} = \frac{1}{n}\sum_{j=1}^{n} a_{ji} \quad (6)$$

Then, the sample center distance shall be solved according to Equation (7):

$$d_i = \frac{1}{n}\sum_{i=1}^{n} \left| a_{ji} - \overline{a_i} \right| \quad (7)$$

Next is the sample variance:

$$s_i^2 = \frac{1}{n}\sum_{j=1}^{n}(a_{ji} - \overline{a}_j)^2 \quad (8)$$

So that:

$$\left.\begin{aligned} Ea_i &= \overline{a_i} \\ En_i &= \sqrt{\frac{\Pi}{2} * d_i} \\ He_i &= \sqrt{s_i^2 - En_i^2} \end{aligned}\right\} \quad (9)$$

The trusted cloud will be obtained by Definition 2, and the cloud center of gravity will be obtained according to Equation (9).

$$G = (G_1, G_2, ...G_n) = h \times l \quad (10)$$

$$G_i = h_i \times l_i, i = 1,2,..., n \quad (11)$$

Compute the weighted deviation, according to Equation (12):

$$\phi = \sum_{i=1}^{n}(\chi_i G_i) \quad (12)$$

Compute the trusts, according to Equation (13):

$$P_{ij} = x * DP_{ij} + y * RP_{ij} \quad (13)$$

In Equation (12), the **i** value in the subscript of P_{ij} represents users, **j** represents services; both **x** and **y** are the scale parameters. In this paper, the trust is divided into direct trust and recommendation trust, respectively expressed in DP and RP. DP is obtained by the historical transaction records of users and service providers, for the computing of direct trust needs to use a quintuple trust table:

$$\{S_k, U_i, t_j, w_n, V_n\},\ j = 1, 2, 3, \ldots, N \quad (14)$$

You can determine the interval of trusted cloud distribution according to the deviation of trusted cloud center of gravity obtained finally, so as to choose a suitable cloud service provider.

3. Specific Implementation Solution

In order to further describe the application of cloud service management mode, we will further elaborate the specific implementation solution combining with the graphic below.

3.1. Personal Information Security Framework based on Cloud Computing

As shown in Figure 1, a cloud service management mode dealing with information leakage risk in the online payment consists of a personal information security model and cloud service providers trust evaluation system. The personal information security model consists of user layer, interface layer, platform layer and management layer. The user layer uses both ways including identity authentication mechanism and access control mechanism to complete the user authentication and login. The interface layer is used to achieve the classification of the

users' personal information, gateway filtering and cryptographic operations. The platform layer is used to complete the data storage. The management layer ensures the whole system can work effectively.

3.2. Cloud Service Trust Evaluation System

As shown in Figure 2, the cloud service providers trust evaluation system is based on the theory of membership degree. The system flow includes: the provider completes its registration from the service registry, the service registry returns the registered results to the service provider, the user sends a query request to the registry, the service registry returns the results to the user, the system queries the trust from the trust evaluation center according to the request result, the system returns the trustresult, the user chooses the best cloud service provider according to the result, the service provider returns the chosen provider to the user, the service monitoring center calculates the attribute value, the service monitoring center sends the assessment to the user, the user returns the results of assessment, and the monitoring center updates the truststore.

3.3. Cloud Service Attribute Settings

In the concrete implementation of this system, you need to build cloud platform first, and apply the model framework presented in Figure 1 and 2 to a cloud environment. You can use an open source Eucalypts platform, for example, with a single cluster installation. A computer is used to install the cloud controller (CLC), the cluster controller (CC) and the storage controller (SC), while another computer is used to install the virtual machine. Among them, the cloud controller is the entry of the administrator and end users to enter the cloud platform, responsible for display and management of virtual resources. The cluster controller is the front-end computer running in the cluster server, which is used for the collection of virtual information. The node controller (NC) can control the running of the virtual machine on it, which is used for the extraction and clearance of a mirrored local copy. After completing the platform building, you can simulate its running.

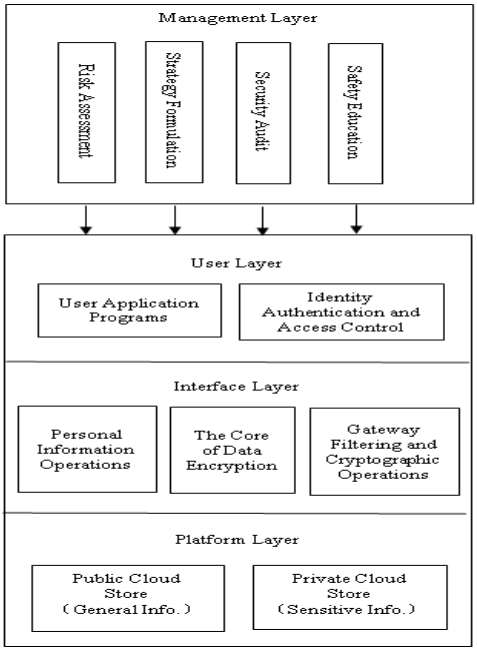

Figure 1. Personal Information Security Frame Diagram based on Cloud Computing

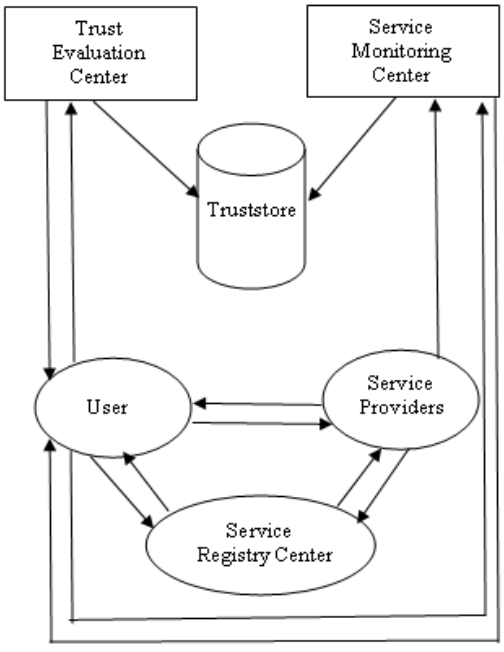

Figure 2. Cloud Service Trust Evaluation System Diagram

The table shows the performance attributes of cloud service providers in the conditions of 2 cloud service providers and 200 users (see Table 1).

The trusts will be compared with the calculation way in this paper and the method after the Qos (Quality of Services) evaluation is passed. When a user requires a higher cloud service response speed, the trust level comparison results are as shown in Figure 3.

Table 1. Cloud Service Attribute Table

Attributes	Cloud Service Provider 1	Cloud Service Provider 2
Trust Level	0.4	0.8
Storage Capacity	0.9	0.9
Transmission Rate	0.9	0.5
Success Rate	0.8	0.8

It can be found from Figure 3 that the theory of membership degree in this study can definitely differentiate the trust of cloud service. Cloud Service Provider 1 has higher trust than Cloud Service Provider 2; If a user requires a higher transmission rate, the testing results will be as shown in Figure 4.

Figure 3. Trust Level Comparison Diagram when a High Response Speed is Required

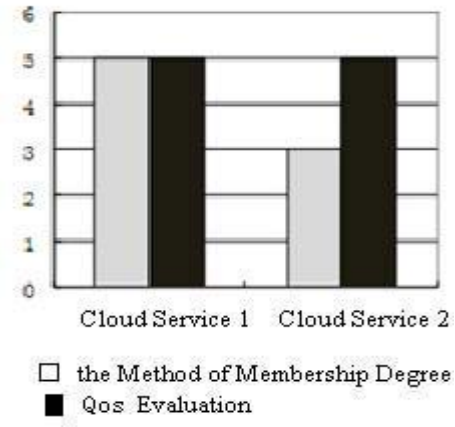

Figure 4. Trust Level Comparison Diagram when a Higher Transmission Rate is Required

It can be found from Figure 4 that Cloud Service Provider 1 has a higher trust. The results don't conflict with those in Figure 4, because the different user has different cloud service attributes. When a user requires a higher transmission rate, Cloud Service Provider 1 will have better trust. According to the Qos evaluation, however, it is unable to distinguish the trust of each cloud service provider.

4. Conclusion

The significant effect of this study is: putting forward the corresponding cloud service management model with regard to the personal information security problems in the online payment. This model can present the trust evaluation on the cloud service providers, and effectively protect the personal information security. The results have great theoretical significance and practical value for the healthy development of e-commerce.

Acknowledgements

This work was supported by the Ministry of Education's Humanities and Social Sciences Project "Study for knowledge matching service of Agile Supply chain—based on

context-aware (12YJA630160)" and Zhejiang Provincial Natural Science Foundation (Y13G030053).

References

[1] Alabbadi MM. *Cloud Computing for Education and Learning: Education and Learning as a service. 14th* International Conference Proceedings Interactive Collabrative Learning. Slovakia. 2011: 589-594.
[2] Banerjee, Srikanth, Cukic. *Log-Based Reliability Analysis of Software as a service*. IEEE 21st International Symposium on Software Reliability Engineering (ISSRE). San Jose. 2010: 239-248.
[3] Bernstein, Vidovic, Modi. *A Cloud PAAS for High Scale, Function, and Velocity Mobile Applications with Reference Application as the Fully Connected Car.* The Fifth International Conference on Systems and Networks Communications. Nice. 2010: 117-123.
[4] Hall. *Evolution of Telcoservices Utilising Infrastructure as a Service.* 15th International Conference on Intelligence in Next Generation Networks. Berlin. 2011: 247-252.
[5] Zhonghua Deng, Yongbo Liu, Youlin Zhao. *Analysis on Integration Technology for Information Resources Cloud.* 2011 International Conference on Fuzzy Systems and Neural Computing (FSNC). Berlin. 2011: 309-317.
[6] Rings T, Grabowski J, Schulz S. Grid and Cloud Computing: Opportunities for Integration with the Next Generation with the Next Generation Network. *Grid Computing*. 2009; 7: 375-393.
[7] Hofer CN, Karagiannis G. Cloud Computing Services: Taxonomy and Comparison. *Journal of Internet Services and Applications.* 2011; 2 (6): 81-94.
[8] Mishra AK, Hellerstein JL, Cirne W, et al. Towards Characterizing Cloud Backend Workloads: Insights from Google Compute Clusters. *Sigmetrics Perform Eval Rev*. 2010; 3 (37): 34-41.