TELKOMNIKA, Vol. 11, No. 12, December 2013, pp. 7331~7338
e-ISSN: 2087-278X

Cloud Computing Application of Personal Information's Security in Network Sales-channels

Qiong Sun*, Min Liu, Shimming Pang
Tourism Institute of Beijing Union University, No 99,Beisihuan Donglu, Chaoyang District, Beijing China,100101
*Corresponding author, e-mail: sunqiongbhs@163.com

Abstract

With the promotion of internet sales, the security of personal information to network users have become increasingly demanding. The existing network of sales channels has personal information security risks, vulnerable to hacker attacking. In this paper, a cloud computing security management model is proposed to tackle information leakage for the network sale of personal information security applications. It divides the personal information into critical information and general information to ensure that the private data does not leak out and is stored by private cloud. The membership-based cloud service is also introduced. A cloud platform built to test the new framework model is applied and the results show the model is applicable.

Keywords: *internet sales, cloud computing, security management strategy*

1.Introduction

Internet sales are about using the internet to sell products [1]. With the popularity of the internet, people have gradually recognized this marketing approach and the number of netizes has also increased. According to the "market survey report China's online shopping of 2013”, the ratio that prefer alipay reaches 77.4%, the size and permeability investigation of online shopping shows there are totally 2,703 people in 21 cities had bought something online and the total amount used in online shopping reaches 73.4 billion yuan. Basically, internet sales are divided into two ways the direct sales and indirect sales, according to whether it is through dealers. The direct sales companies build websites to promote their products directly to the consumers, and the indirect sales are the channel to sell products through internet dealers. For either sales channel, we need to have good security measures, which not only improve the credibility ofinternet vendors, but also do not damage the interests of netizens. However, according to the 2011 annual security report released by Rising, it shows that the e-commerce has become the main target spied out by hackers. Encroaching on the consumer's personal information includes the illegal collection, disclosure and using of consumer's information, which results in network security issues.

In the existing internet sales, the security management of personal information mainly includes bank account confidentiality, firewall protection, prevent "phishing websites" [2]. These measures aim to do well in safe mode management of data information. In recent years, the cloud computing has been applicated in various fields. After the research on security management mode of cloud computing, it puts forward to apply the cloud computing security measures in personal information protection strategy of internet sales.

2.Security Problems of Personal Information in Internet Sales

The internet vendors If understand the customer's shopping preferences, could very well identify the market needs and increase profits. Therefore, if the user's personal information is open to vendors, there likely exist the security risks [3]. The sales channels must be learned. The user, when carries out online shopping, must register, login, fill out order and make payment, in which there is security problem in every step [4]. The consumers should provide personal information when register and the site may use personal information

Received June 24, 2013; Revised July 27, 2013; Accepted August 15, 2013

submitted by users to do illegal activity, which will hurt consumers. Therefore, the consumers do not want to provide personal information for security and privacy, which also bring trouble to the internet vendors. When the user selects their goods, it will leave log record in the network server. The merchants could analyze the user's expense calendar with the logs.

Presently, the existing security problems mainly include the illegal collection and exploitation and utilization of user's personal information and illegal profit-making from user's personal information [5]. It mainly through the following ways: Using cookie tracking software; hackers to login in computers of others and spam mails. Analyzing the user's personal information is the prerequisite for the merchants to promote. The internet vendors make use of users' personal information collected to make secondary development to seek benefits and send spam mails or messages to conduct malicious promotion. The above is derived from the disclosure of personal information of user, so it must make clear first why the information disclosure issue exists. The internet sales process must require users to fill in personal information, in order to conduct transaction [6]. However, the information when submitted is not encrypted, it is easily stolen. Internet sales makes transactions networked and virtualized, which results in credit risk issues. The cookie technology is widely used in web design. The cookie records the personal information. if criminal intercepts the cookie, it will cause leakage of personal information.

3. Cloud Computing and Cloud Security

Cloud computing is not emerging technology in light of technical means. It belongs to the distributed computing mode and is originated from the grid computing [7]. However, the cloud computing belongs to the emerging service mode, which link lots of storage devices to form large-scale resource shared pool and allow users to enjoy the computing of high storage and high performance, without having to purchase expensive hardware equipments [8]. The computing tasks are not conducted in the local computer or remote server, but in lots of distributed computers, so that the resources can be allocated to the demand. Keep increasing the processing capacity of the cloud and reduce the processing load of the terminal computer. The terminal enjoys powerful computing and storage capabilities provided by the cloud, to be simplified into input and output devices. Cloud computing is divided into three kinds, infrastructure on-demand service (IaaS), platform on-demand service (PaaS) and software on-demand service (SaaS), which not only achieve the sharing of resources and reduce the burden on of user's computer to manage resources. Cloud computing has many technical advantages. It not only has superior processing and storage capacity, but also support virtualization and transparence of the user.

The cloud computing mainly involves three aspects, the security access control, virtualization and security protection [9]. The solutions are mainly data encryption and backup and private cloud. The paper ensures data security with the help of private cloud. Security management ensures data confidentiality, integrity, availability, etc. Confidentiality is that the data is restricted to be used by authorized users only. Integrity is that information in the process when stored or transmitted, is not arbitrarily tampered. Availability refers to that cloud service has the ability to control data.

Under the cloud computing environment, there are plentiful security authentication mechanisms, like identity authentication, intrusion detection, security audit, access control and credibility mechanism of user behavior [10]. Even identity authentication is the most basic security protection, when internet user logs in, the user's identity should be first verified, but it is a challenge to cloud security. The premise of security is that the cloud service provider must be trustworthy. The intrusion detection mechanism is to gather anomaly data packets and analyze whether it is attacked. Security audit mechanism is related to the "black box" work. Access control mechanism is to control the right of the use of resources. User behavior credibility mechanism is the mechanism that verifies whether user behavior is trustworthy.

4. Application and Exploration of Cloud Computing on the Personal Information Security in Internet Sales

With the development of science and technology, new consumption patterns are gradually being recognized by us. Internet sales is an online trading place, establishing a virtual trading platform for merchants and customers [11]. The internet must be able to solve the burstiness and the parallelism of visitor volume and there must be a powerful data center to store massive data and ensure of data security [12]. The advantages of cloud computing, the distributed processing, brings a lot of convenience to internet sales channels. Cloud computing can reduce the hardware consumption costs and improve data transmission efficiency and its security mechanism can better ensure of the security of electronic transactions [13].

4.1. Cloud Security Management Mode in Internet Sales

The popularity of Internet sales should make the server have the basic characteristics, enough storage space and sensitive response. Such large data processing allows us to introduce the idea of cloud computing. The personal information submit by users is sent for cloud storage. If choosing public cloud, the user cannot control data storage location, causing problems to the security of personal information. This paper adopts the hybrid cloud framework to ensure of security of personal information, namely two kinds of cloud storage, public and private clouds to store user data information. The basic idea is to divide user's personal information into two kinds, of which, one is critical information, like phone numbers, home addresses and other private data information, the other is called common information, such as purchase history, preferences, recommendations and other information. It lets the key information be stored by private cloud and common information be stored in the public cloud, which could very well solve the security issues of critical information. The personal information security mode designed is as follows:

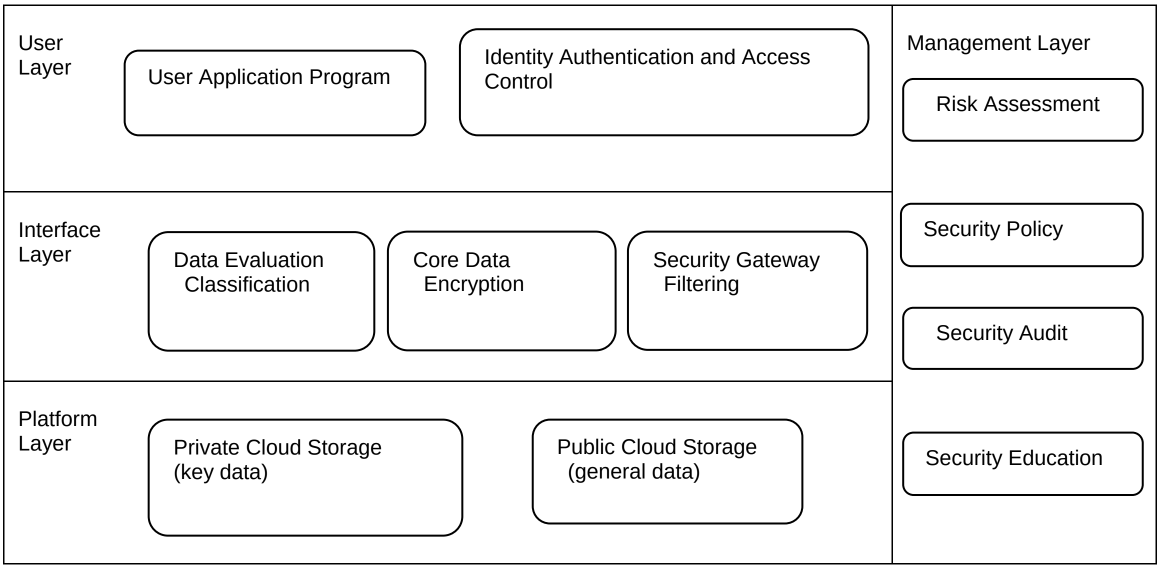
User Layer
User Application Program
Identity Authentication and Access Control
Management Layer
Risk Assessment
Interface Layer
Data Evaluation Classification
Core Data Encryption
Security Gateway Filtering
Security Policy
Security Audit
Platform Layer
Private Cloud Storage (key data)
Public Cloud Storage (general data)
Security Education

Figure 1. Personal Information Security Framework of Basic Cloud Computing

The framework consists of four layers: platform layer completing data storage, interface layer for complex personal information classification and encryption, user layer completing user identity authentication and management layer ensuring of overall effective working.

User layer mainly completes identity authentication and user login authentication, adopts the two methods, authentication mechanisms and access control mechanisms and ensure of access and security of cloud computing platform. The access control is divided into three steps:

- Step one: User send request to the cloud terminal, namely the description of the resources accessed;
- Step two: Cloud terminal analyzes information requested by user and match personal information stored by private cloud.

- Step three: Response to the results of the second step and the send responsed results to the user.

Interface layer is to achieve the classification of users' personal information and operations of gateways and encryption, of which classification of the users' personal information is a newly added algorithm. Data evaluation classification is based on: First, how much harm is caused by disclosure of personal information of user, Second, merchants considering the confidentiality degree of such data. Data encryption is still the best choice for sensitive information. After the sensitive information is encrypted, data security is guaranteed. Encrypted storage can ensure of the confidentiality of critical information in the shared storage platform, solving the data storage security. To apply the cloud computing security gateway technology in the internet sales channels plays the role of secure filtering of personal information data. In addition, the security gateway in the cloud computing technology also plays an important role. We arrange interface layer devices in the inlet and outlet of the private cloud, to conduct classification, filtering and encryption processing of the user's personal information. The classified critical information can only flow to the private cloud. If the critical information is encrypted, the encrypted data can also be stored in public cloud.

Platform layer involves two parts: public and private clouds. Strictly speaking, critical information must be stored in a private cloud. However, if being precisely encrypted, such critical information can be stored by public cloud. General information needs to be filtered through the cloud computing gateway. The intercepted sensitive information must be stored in private cloud and the other information filtered must be stored in the public cloud. Platform layer more obvious explains that the system is based on the hybrid cloud. Netizens generally do not have private cloud and the private cloud can be considered as the user internal network. As long as the user internal network has sufficient security protection, it still meets the overall security protection of the system.

Management layer includes risk assessment, strategy making and auditing, etc. The layer is the guarantee and support for operation of the entire mode. Cloud computing security mechanisms is almost the same with the security mechanism realized by common network, but it is merely extended on the basis of common network, so that the security risks are concentrated in the cloud provider. With the general risk technology, it cannot be very well solved, so we use management tools for help.

4.2. Cloud Service Trust Evaluation System

It has proposed in the above section that personal information security depends largely on the cloud service provider. Before requiring the user to request service, to select appropriate cloud service provider according to the trust level, it needs to conduct assessment on the credibility of the cloud service providers. This paper is based on membership degree theory, and proposes to establish the behavior trust evaluation of the cloud service provider. The system model is as follows:

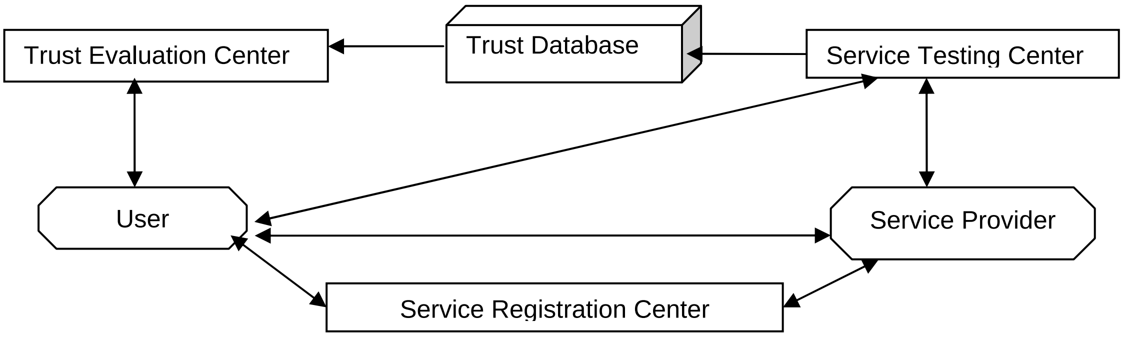

Figure 2. Evaluation System

The system process is: (1) release services, namely provider to complete the registration in the registration center; (2) Service registration centre to return the result to the service provider; (3) User to send query request to the registration center; (4) registration centre returns the results to the user; (5) in accordance with the outcome of the request, inquirie trust degree in the trust assessment center; 6) Returns trust degree results; (7) in accordance with the results, the user chooses the best cloud service provider;(8) the service provider returns the selected enhancer to the user. (9) Service monitoring centre gets property values;10) Service testing center send the evaluation to the user; (11) user returns evaluated results; (12) testing center updates the trust database.

The performance indicators of cloud service provider are monitored by the monitoring center. Store the service evaluation information received from user in the trust database. It is to be stored according to the quintuple in the following formula:

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

S_i in the above formula is service provider U_i means the user t means the time provided for the service w_n means the property V_n means property value.

Definition 1 a is physical attribute X is language value of the trust level let domain $\Pi = \{a\}$ for $\forall a \in \Pi$ there is $\lambda X(a) \in [0,1]$ then call λ the subordinating degree function of X The distribution of function is also called trust cloud.

Definition 2 trust cloud is represented by P P=P(EX,EN,HE) of which, Exis expectation En is entropy He represents extra- entropy.

The property trust cloud computing is as follows:

Input Evaluation value of the i-th attribute of n entities to entity X.

Output Trust cloud P of attribute i.

First, obtain the sample mean:

$$\overline{a}_i = \frac{1}{n}\sum_{j=1}^{n} a_{ji} \tag{2}$$

Then according to the following formula, obtain the sample center distance:

$$d_i = \frac{1}{n}\sum_{i=1}^{n} \left| a_{ji} - \overline{a}_i \right| \tag{3}$$

Followed by the sample variance:

$$s_i^2 = \frac{1}{n}\sum_{j=1}^{n} (a_{ji} - \overline{a}_j)^2 \tag{4}$$

Then

$$Ea_i = \overline{a}_i, En_i = \sqrt{\frac{\Pi}{2} * d_i}, He_i = \sqrt{s_i^2 - En_i^2} \tag{5}$$

For the above formula, according to definition 2, aquire trust cloud, abtain cloud core:

$$\begin{cases} G = (G_1, G_2, \ldots, G_n) = h \times l \\ G_i = h_i \times l_i, i = 1, 2, \ldots, n \end{cases} \tag{6}$$

Obtain weighted deviation degree, according to the formula:

$$\phi = \sum_{i=1}^{n} (\chi_i G_i) \tag{7}$$

To calculate the trust degree, according the following formula:

$$P_{ij} = x * DP_{ij} + y * RP_{ij} \tag{8}$$

Where i marked below the parameter P_{ij} in the above formula represents user， j represents service， x， y are the proportion parameter， The paper divides trust degree into direct trust degree and recommendation trust degree, which are represented by DP and RP respectively. DP is obtained with the historical transaction records of user and the service provider. For the calculation of direct trust degree, it needs the quintuple trust table for help:

$$\left\{S_k, U_i, t_j, w_n, V_n\right\},\ j = 1, 2, 3, \ldots, N \tag{9}$$

According finally obtained degree of deviation of barycenter of trust cloud, determines the distribution interval of the trust cloud, thus choose the appropriate cloud service provider.

4.3. Experimental Conditions and Results Analysis

First build the cloud platform, and apply the framework model proposed in the paper in the cloud environment. This paper adopts the open source Eucalypts platform and single cluster installation. One is installed in cloud controller (CLC), cluster controller (CC) and storage controller (SC), the other one is installed in virtual machine, of which the cloud controller is the entrance for administrator and end-user to access cloud platform, responsible for the presentation and management of virtualized resources. Cluster controller runs on the front-end of the cluster to collect virtual information; NC controls operation of the virtual machine on it, extract a and remove a the mirrored local copy. After the platform is built, this paper provides two cloud service providers and 200 users, the performance attributes table of cloud service provider is as follows:

Table 1. Cloud Service Attribute Setting

Each attribute	Cloud service provider 1	Cloud service provider 2
Response rate	0.4	0.8
Storage capacity	0.9	0.9
transmission rate	0.9	0.5
Success rate	0.8	0.8

The experiment compares trust degree with the methods proposed by Qos evaluation. When user requires higher response speed of cloud services, for the comparison of the trust level results, refer to Figure 3:

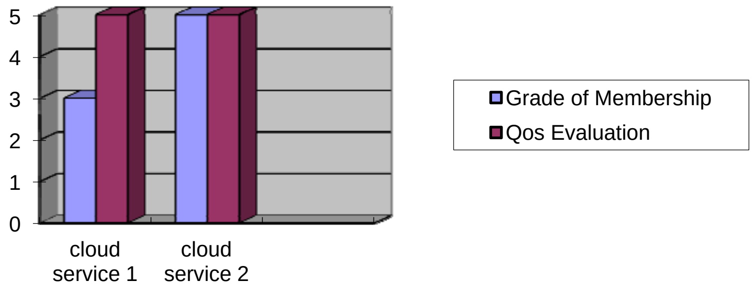

Figure 3. Trust Level when Higher Response Speed is Required

By comparing the above table, the degree of membership theory proposed in the paper clearly distinguishes the trust degree of cloud services. Cloud service providers 1 has higher level of trust than cloud service provider 2; If the user requires higher transmission rate, for the experimental results, refer to Figure 4.

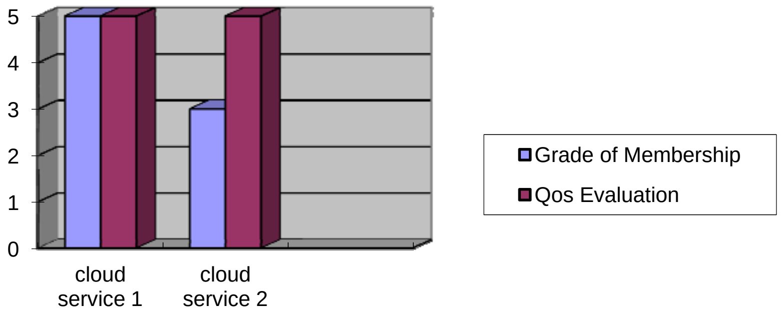

Figure 4. Trust Level when High Transmission Rate is Required

It can be learnt from Figure 4, the cloud service 1 has higher trust level, which does not conflict with the results of Figure 3, because for different user, different attributes provided by cloud services is required. When the user needs higher transmission rate, cloud service providers 1 has higher degree of trust, If according to the Qos evaluation, it cannot distinguish trust degree of various cloud services.

5. Conclusion

The possibility of disclosure of personal information is very serious impact to internet sales. It needs urgently solve the personal information security existing in the internet sales. The internet sales channel have many modes, the merchants must make the right choice based on their actual situation. Currently using the reputable sales platform is the best choice for merchants. Personal information security is the premise for better operation of internet sales. There are many ways to improve information security degree of internet sales. Security is the prerequisite for the user to select cloud computing. The security policy of cloud computing can very well ensure of data security, so the paper introduces security policy of cloud computing into internet sales channels.

The paper is based on personal information security in the internet sales to study confidentiality and security of data privacy. It divides the personal information into critical information and general information to ensure that the private data does not leak out and is stored by private cloud. Personal information is to be stored by cloud, so information security degree depends entirely on the cloud service provider. The paper also adopts the membership degree to determine the selection of trust cloud. And compare experimental result and the trust cloud result selected with Qos evaluation, the paper can achieve better results as expected.

References

[1] Liu Z. Internet sales situation and development strategy of our enterprise. *Beijing Technology and Business University*. 2009; 4(5): 29–34 .
[2] Joshua G. Protection in the cloud: risk management and insurance for cloud computing. *Journal of Internet Law*. 2012; 5(12): 1–28.
[3] Harold L, Johnson D. Are home-based sales representatives aware and proactive regarding security risks in the internet era. *Journal of Internet Commerce*. 2008; 7(3) :40–46.
[4] Wijesekera D, Jajodia S. A propositional policy algebra for access control. *ACM Trans. on Information and System Security*. 2003; 6(2): 286–325.
[5] Naresh K. A cross section of the issues and research activities related to both information security and cloud computing. *IETE technical review*. 2011; 28(4): 80–89.
[6] Shafiq B, Ghafoor A. Secure interoperation in a multi-domain environment employing RBAC policies. *IEEE Trans. on Knowledge and Data Engineering*. 2005; 17(11): 1557–1577.

[7] Zhang J, Gu Z, Zheng C. Cloud computing research overview. *Application Research on Computer*. 2010; 27(2): 429–433.
[8] Qu D. Dynamic trust computing model based on context sensing. *Computer Engineering and Design. 2*009; 30(7) :1647–1649.
[9] Cheng F. Lai W, Creating environment for the prosperity of cloud computing technology. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2012; 1(4):878–886.
[10] Rimal B, Jukan A, Katsaros D. Architectural requirements for cloud computing systems: an enterprise cloud approach. *Journal of grid computing*. 2011; 9(11): 77–89.
[11] Lijuan Z, Hui W, Wang W. Parallel implementation of classification algorithms based on cloud computing environment. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2012; 10(5): 1353–1362.
[12] Yang X, Nasser B, Surridge M, Middleton S. A business-oriented cloud federation model for real-time applications. *Future Generations Computer Systems*. 2012; 28(8): 123–134.
[13] Mercy A. A study on cloud security Issues and challenges. *International Journal of Computer Technology and Applications*. 2012; 3(01):55–70.