Analysis of Information Security Risk and Application Security of Cloud Computing from the Aspect of Hierarchical Protection

ZhaoLi[1, a]

[1]School of computer science, Wuhan Donghu University, Wuhan,HuBei,430212 China

[a]6115480@qq.com

Keywords: hierarchical protection; cloud computing; information security risk; security

Abstract

Cloud computing has many advantages such as on-demand service, high extendibility, universality, low cost and virtualization, and so on, which is widely promoted and applied in each industry of the society. However, the development of cloud computing is also faced with many risks and challenges, among which information security risk has become on the main factors of restricting the development of cloud computing. Cloud computing application security protection system can be created with cloud computing hierarchical protection technology system, which can effectively solve various information security risks in cloud computing; it is very important to ensure the information security of cloud computing and to accelerate the continuous development of cloud computing technology. Therefore, the paper briefly introduces cloud computing and cloud computing security, analyzing cloud computing hierarchical protection system, exploring the information security risks in cloud computing and putting forward the application security protection system in cloud computing.

Introduction

At the present stage, with the accelerating global networking and gradually increasing categories of network application, the complexity of network improves unceasingly, and network and information security have become the focus of all sectors of society. The cloud computing techniques developing based on network techniques are widely promoted and applied in every industry with its unique advantages (such as on-demand service, high extendibility, universality, and low cost). In the environment of cloud computing, information security has become an inevitable issue and how to solve the information security risk in the environment of cloud computing has become a challenge perplexing many technicists. The nature of cloud computing hierarchical protection is to conduct cascade protection on the security of cloud computing information system, so as to continuously elevate the level of cloud computing information security protection. Therefore, the study on the information security and application security of cloud computing from the aspect of hierarchical protection has very important practical significance.

Analysis on the information security risks of cloud computing

The security control of cloud computing and the safety control of the traditional IT environment have many things in common; however, as the cloud computing adopts cloud service technology, cloud computing model, and cloud computing operating mode, there are more information security risks in the cloud computing than in the traditional IT environment, which mainly includes following several aspects: the first one is the imperfection of cloud laws. Although cloud computing technology in China is developing very fast, but cloud computing starts relatively late, and there are no improved laws or regulations to control and manage the information security risks in the cloud computing; in the absence of perfect law for security, there are many unsafe factors in cloud computing environment leading to a threat to information security. Secondly, as for the cloud access control security risks, with the promotion and application of cloud computing technology, all kinds of enterprises transfer the data information to the cloud server, and the data information of many competitors may exist in the same physical device or virtual environment; how to control the cloud security risks has become the emphasis that cloud computing information security needs to focus on. The third one is the security risks of cloud log. With the development of cloud computing technology, many systems have migrated to cloud computing systems, and cloud service provider may keep the logs. These logs are internal, which increases the difficulty of cloud log monitoring, leading to certain security risks in cloud logs. The fourth one is cloud key security risks. As data information security is the core of the cloud computing level protection, it is necessary to encrypt the data information from technical angle and management angle and many authentication operations also need to encrypt; the cloud key safety protection has become the key of the cloud computing information security protection. The fifth one is confidentiality and integrity of cloud data. As in cloud computing, users only know that data use a kind of logical storage to store, but do not know which specific physical location that data information is stored in, they do not know the confidentiality and integrity of the cloud data storage, which leads to that the confidentiality and integrity of data information storage become the focus of users.

Application security protection system of cloud computing based on the hierarchical protection

1.Application security threat in cloud computing

The key to solve the application security issue of cloud computing is to create comprehensive computing security protection framework and to reinforce the research on the key technology and management methods of cloud computing security. To ensure the application security of cloud computing users, it is necessary to conduct analysis on the application security threat in cloud computing, which includes following aspects: (1) Security flaws in cloud computing. The reason of security flaws is that the cloud service provider doesn’t develop technical protection and security management, which means that the issue of cloud computing software itself brings security troubles. (2) During the transference of cloud applications among virtual systems, the analysis isn’t conducted towards the performance and stability of application process, which leads to the problem of service interruption during transference and causes damages to users. (3) Leakage of cloud application logs. The shortage of necessary hierarchical management and supervision in the application process of cloud applications leads to abnormal operations or cross-right log access, causing damages to users. (4) Management of key management in cloud application. In the cloud application process, the certificate may lose efficacy or the password custody may ineffective or be falsified, which may lead to the leakage of users’ secret key, causing damages to users. (5) Security flaws in operation data. When users use cloud application to visit data information, the data information needs to pass storage processing and the data information may meet such problems as being stolen or leaked in the process of storage, which will cause loss for users.

2.Requirements on the application security protection of cloud computing

To elevate the application security level of cloud computing, it is necessary to formulate the requirements on the application security protection of cloud computing according to Basic *Requirements on Security Level Protection of Information System,* which includes: (1) Continuous availability. During the transference of cloud computing in virtual environment, it is necessary to examine cloud application to ensure safe and steady operation of cloud application; (2) Access control security. It is necessary to conduct strict audit, supervision and control on application logs, to divide access level of log access, to conduct encryption management on data logs, and to avoid such phenomena as unauthorized access.

3. Build hierarchical structure model of cloud service

Based on information security risk assessment index system of cloud service above, this paper builds hierarchical structure model on first-level indicator “technical risk” and “non-technical risk”. The hierarchical structure model is usually divided into three levels, target level on the top-level, scheme level on the down-level, and criterion level or index level on the middle level. The concrete model of “technical risk”is shown in Table 1:

Table 1: Information security risk assessment index system of cloud service

Risk assessment (A Level)	B1 authorization setting risks	C11 client identity authentication failure C12 abuse of service provider authority C13 access control failure
	B2 data risks	C21 lack of data storage space C22 interception in data transmission C23 data leakage in uploading or downloading C24 non-effective isolation in data C25 stored data is stolen, modified, or deleted C26 data cannot be stored after loss or damage
	B3 network security risks	C31 deficiency in network bandwidth C32 network attack C33 port leakage
	B4 software program risks	C41 disorder in version and patch C42 updating dangers C43 faulty operation C44 system bugs C45 insecure pot and API
	B5 hardware device security risks	C51 harsh room environment C52 no equipment monitoring C53 no alternate device C54 unreliable physical equipment C55 wrong operation C56 dangerous configuration

Figure 1 takes “technical risks” as example and the structural model is as following:

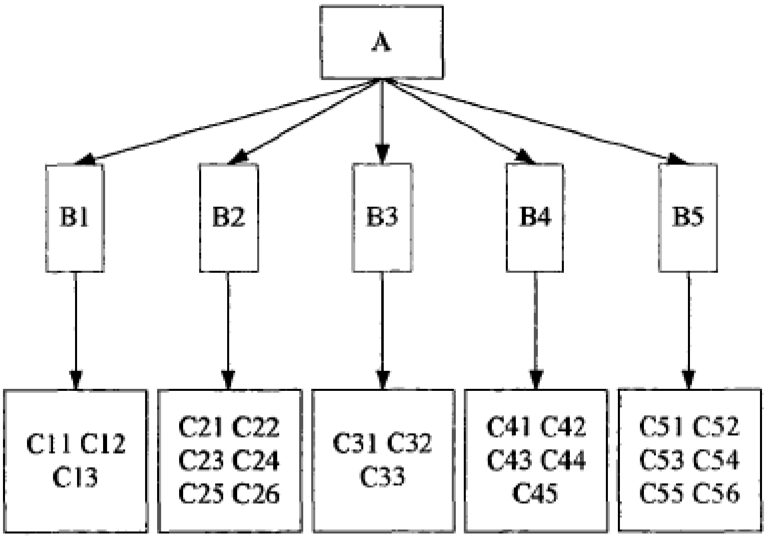

Figure 1 “Technical risks” structural model

As for “technical risks”, there is a factor on criterion level; if $x=\{x_1, x_2, x_3, x_4, x_5\}$, it is necessary to compare their influence degree on the “technical risks” target of the upper level, so as to confirm the proportion of them against the target of “technical risks” (rank the influence degree of this gactor on the “technical risks” target of upper level). The comparison above adopts comparison of wide dimension in pairs and b_{ij} stands for the comparison outcome of i factor against j factor.

$b_{ij}=1/b_{ij}$

$$B=(b_{ij})_{5X5=}\begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} \\ b_{31} & b_{23} & b_{33} & b_{34} & b_{35} \\ b_{41} & b_{42} & b_{43} & b_{44} & b_{45} \\ b_{51} & b_{52} & b_{53} & b_{54} & b_{55} \end{pmatrix}$$

B is pairwise comparison matrix. Single hierarchical arrangement of cloud service is the process to define the influence degree of every factor of the down-level on certain factor of the upper level. The influence degree is expressed with weight. Here, take a simple example to display how to define weight. For example, the weight of a heavy object is marked as , which is divided into small portions, whose weight can be marked as w_1, w_2, w_3, w_4, ... , w_n respectively.

$$B=\begin{pmatrix} 1 & w_{1/}\ w_2 & \ldots\ldots & w_{1/}\ w_n \\ w_{2/}\ w_1 & 1 & \ldots\ldots & w_2\ w_n \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots. \\ W_{n/}\ w_1 & w_{n/}\ w_2 & \ldots\ldots & 1 \end{pmatrix}$$

From the matrix, it can be seen that $W_{i/}\ w_j$ $=W_{i/}\ w_k=W_{k/}\ w_{j,}$ and $b_{ik\ x}\ b_{kj}=b_{ij,}$ It is called as unanimous matrix.

Pairwise comparison of consistent matrix array; take the normalized eigenvector {w_1, w_2, w_3, w_4, ... , w_n} of the maximum characteristic root n; w_i shows the weight value of the influence of i factor to certain factor on the upper level. If the pairwise comparison matrix is not consistent, it is necessary to take the corresponding normalized eigenvector of the largest eigenvalue as weight vector W, and $Bw=\lambda w$, w ={w_1, w_2, w_3, w_4, ... , w_n}; this way to define the weight vector is called as eigenvalue method.

Define random consistency index: construct pairwise comparison matrix in random. We can get w_1, w_2, w_3, w_4, ... , w_{500} and the consistency index is CI_1, CI_2, CI_3, CI_4, ... , CI_{500}

$$RI=\frac{CI_1+CI_2+\cdots CI_{500}}{500}=\frac{\frac{\lambda_1+\lambda_2+\cdots+\lambda_{500}}{500}-n}{n-1}$$

The values of random consistency index can be seen in Table 2.

Table 2: Random consistency index RI

n	1	2	3	4	5	6	7	8	9	10	11
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51

Generally, when the consistency ratio CR=CI/RI<0. 1, it is believed that the inconsistency of A is within the tolerance range and its normalized eigenvector can be taken as the weight vector; otherwise, it is necessary to reconstruct paired comparison matrix and to adjust B. Consistency check summary: using the consistency index and the numerical table where the consistency ratio is less than 0.1 and there is random consistency index; it is the process of testing B.

4. Hierarchical order and consistency check of cloud service

The process to define the order weight of the relative importance of all the factors in certain level of cloud service to the total goal, is hierarchical order. It is from the bottom level upwards, and in “technical risks”:

5 factors in B level are B1，B2，B3，B4，B5, and their order to the total goal A are b1，b2，b3，b4，b5. N factors on C level to the factors on upper level B is BJ; the hierarchical single order is C_{1j}, C_{2j},.....C_{ij}(j=1,2,.....5)

The Hierarchical order of C level is:

$C_1:b_1C_{11}+b_2\ C_{12}+\ldots b_5\ C_{15}$

$C_2:b_1C_{21}+b_2\ C_{22}+\ldots b_5\ C_{25}$

....

$C_n:b_1C_{n1}+b_2\ C_{n2}+\ldots b_5\ C_{n5}$

The weight of i factor on C level to the total goal A is: $\sum_{j=1}^{5} b_j c_{ij}$, which can be seen in the following table.

C	B1，B2，B3，B4，B5 b1，b2，b3，b4，b5	Hierarchical order of C level
C_1	b_{11} b_{12} b_{13} b_{14} b_{15}	$\sum_{j=1}^{5} b_j C_{1j}=C_1$
C_2	b_{21} b_{22} b_{23} b_{24} b_{25}	$\sum_{j=1}^{5} b_j C_{2j}=C_2$
C_3	b_{n1} b_{n2} b_{n3} b_{n4} b_{n5}	$\sum_{j=1}^{5} b_j C_{3j}=C_3$

5. Construct cloud service fuzzy membership degree matrix

Suppose the set of various factors: U={u_1，u_2，u_3，u_4，.... ，u_n}, then the fuzzy set on U is A:

$$A=\frac{A(u_1)}{u_1}+\frac{A(u_2)}{u_2}+\cdots\frac{A(u_n)}{u_n}$$

As for the features of information security risk index system of cloud service, this paper adopts expert adjudicate method to get the membership of different index. Evaluate the three levels (this paper adopts three-level evaluation set: “small”, “middle”, and “large”) of the evaluation set from experts; results are filled in the evaluation sheet and the fuzzy evaluation set of various index are calculated as: R (r1, r2, r3); r1,r2, r3 are the relative frequencies of this index towards the first term to the third term in the evaluation set (which is membership).

6. Risk analysis from the aspect of application security

To solve the application security problem in a better way, it is necessary to adopt corresponding measures to solve possible threats effectively, which needs to know specific security threats so as to put forward relevant handling methods according to the basic requirements of hierarchical protection. Firstly, cloud application itself and its operation data process have security flaws, which mainly because that cloud service provider neither develops effective technical protection and management nor provides effective data storage handling methods; it needs cloud service provider to conduct comprehensive monitoring on the functions of applications in daily life, to provide corresponding performance test report and to conduct encryption transmission management in the process of data transmission, and to take measures to isolate virtual machines completely, so as to ensure the security of applications and data. Secondly, there is no strict distinction between special and non-special cloud applications. During the operation in a virtual machine, if sensitive data and non-sensitive data co-exist in the same virtual without separation, it increases the risk of data leakage to a great degree. Therefore, it is necessary to distinguish servers for data center, sensitive data and non-sensitive data; in data transmission, it is necessary to transmit information through different channels. Thirdly, there are great risks in the secret key and certificate of cloud application and it is probably to create log leakage. It is mainly because that the code may have been let out or tampered, or the management and supervision of logs is not proper. It is necessary to separate virtual machines and cloud applications in the process of management and to conduct effective management on secret keys and certification according to relevant laws. Meanwhile, it is necessary to make analysis and management on logs and to prohibit other users to visit and modify as required; as long as sensitive logs are related, it is necessary to conduct encryption handling. Lastly, in the dynamic migration of cloud application, problems may appear in the performance stability. In the process of opt-out, the data destruction is not complete. The reason for these problems to appear is mainly because that the performance of applications hasn’t reached specified standards and that effective techniques and management are in short; as a result, interruptions take place in the using process and data destruction is not complete. It needs us to conduct tests on the performance of cloud application programs to ensure normal operation; at the same time, we need to examine whether data destruction techniques reach standards and requirements, to solve these problems effectively and let cloud application come into use regularly, so as to ensure the security of data.

Summary

This paper takes cloud service information security as research subject, comprehensively analyzing relevant problems on risk assessment of cloud service information security. This paper elaborates related concepts on the risk assessment of cloud service information security, including basic concepts of cloud computing and cloud service, factors on risk assessment of information security, relation model and evaluation process, and basic methods of risk evaluation. This paper also constructs index system, puts forward a multi-level fuzzy comprehensive evaluation model, and uses this model to conduct multi-level evaluation on the cloud service security risks, providing theoretical references for the risk management of cloud service.

References

[1] Tao Jiayi. Exploration on Security Protection System of Cloud Computing [J]. Guizhou Electric Power Technology, 2015,01:44-46.
[2] Shen Cong. Analysis on Information Security Risks and Application Security of Cloud Computing from Hierarchical Protection [J]. Electronic World, 2016,11:37-38.
[3] Zhang Xiangdong. Exploration and Analysis of Cloud Computing Security Risk Evaluation Based on Hierarchical Protection Strategies [J]. Network Security Technology and Application, 2016,06:65-66.
[4] Zuo Danxia. Detection Analysis on Information System Security Hierarchical Protection Based on Cloud Security Model [J]. Computer Knowledge and Technology, 2016,19:52-53.
[5] Liu Yabo. Analysis on Power Grid Cloud Computing Security Protection Based on Hierarchical Protection [J]. Digital Technology and Application, 2016,09:208.
[6] Zhu Shengcai. Analysis and exploration on Information Security Risks Based on Cloud Computing [J]. Journal of Xi’an University of Posts and Telecommunications,2013,04:89-94.
[7] Li Wenjing. Exploration on Cloud Security Issues Based on Hierarchical Protection [J]. Network Security Technology and Application, 2015,06:25+28.
[8] Wang Xizhong, Wang Jianli, Huang Junqiang. Hierarchical Protection Appraisal in Cloud Computing Environment [J]. Information Technology, 2015,07:184-186.