Security evaluation model for the enterprise cloud services based on grey fuzzy AHP

Yu Bengong[1, 2], Wang Liu[1*], Guo Fengyi[1]

[1]*School of Management, Hefei University of Technology, Hefei 230009*

[2]*Key Laboratory of Process Optimization and Intelligent Decision-making, Ministry of Education, Hefei 230009*

Received 2 July 2014, www.cmnt.lv

Abstract

This paper analyses the application status of cloud services to identify four factors that affect the security of enterprise cloud services (ECSs), including platform facilities, operational safety, operations management, and legal factors. Based on the four factors, the grey fuzzy analytic hierarchy process (GFAHP) is used to construct an evaluation model for the security of ECSs. An example is investigated to demonstrate the proposed model.

Keywords: enterprise cloud services, cloud safety, grey fuzzy AHP, evaluation model

1 Introduction

Inspired by the commercial operations of international network companies, the cloud service, as a new business model has been continuously refining and developing. Resources can be accessed anywhere on any device via the Internet. With more and more cloud platforms being applied, the security issues of the ECSs have arisen.

Recently many famous companies, such as Amazon [1], Google [2], and Sony, have paid much attention to the security of ECSs because of a large number of repeated security incidents. Specific security issues for the ECSs mainly include the technology and management in virtualized environment, the security issues of cloud service platforms, and etc. Those issues not only challenge the security technology and collaboration between the companies and service providers, but also pose threat to judicial supervision and privacy protection. Therefore, it is practically important to construct the security evaluation system of the ECSs.

The international research firm Gartner [4] enumerated seven major risks in the cloud computing which include the data access of the privileged users, auditability, data location, data isolation, data recovery, investigation support, long-term survival. FENG Deng-guo et al. [5] analysed the information security challenges of technologies, standards, regulatory and other aspects in the cloud computing. They also proposed the reference framework and investigated the key technology for cloud security.

FU Sha et al. [6] studied the information security risk assessment and presented a fuzzy analytic hierarchy process (AHP) methodology whose feasibility and effectiveness were demonstrated by an example. On the same issue, HUANG Jianxiong et al. [7] proposed a different evaluation index system and used a new model, which combined fuzzy AHP with grey evaluation method to evaluate the risk of information systems.

Cloud service has played a strategic role in the technical innovation of companies. A lot of research has been conducted, but there is little research about the security evaluation of the ECSs. This paper studies the security evaluation of the ECSs by which the security levels of the cloud service providers are evaluated. To avoid the subjectivity of experts, the grey theory and fuzzy AHP are combined to build the security evaluation model of the ECSs, which improve the accuracy of security evaluation.

2 Security evaluation model of the ECSs construction

There are many factors in cloud security. Huang Ying et al. [8] carried out research on security of cloud infrastructure. It observed the state-of-the-art of cloud infrastructure security, analysed security problems existing in cloud infrastructure from a wide perspective. In combination with a technical framework of cloud infrastructure security, it discussed principle key techniques of cloud infrastructure security. Liu Xiehua et al. [9] introduced the basic concept, and analyse the challenges of security model and policy in cloud computing. Ma Xiaoting et al. [10] described the characteristics and principles for the digital library based on cloud computing, discussed the factors affecting digital libraries securities, studied the threats and countermeasures of data security, application and

* ***Corresponding author*** e-mail wangliuatu@gmail.com

virtualization security for the digital library under cloud computing.

With a view to solving the practical problems in the application of cloud services, this paper construct an evaluation index model for the ECSs based on analysing and summarizing the affective factors.

2.1 AFFECTIVE FACTORS FOR THE SECURITY OF THE ECSS

The awareness and acceptance of users about the cloud service need to be improved because the applied models are diverse. The enterprises should reasonably analyse, actively participate even for the security risk, if they want to make full use of the cloud services to enhance their competitiveness. The affective factors for the security of the ECSs are presented as follows:

2.1.1 Platform facilities

When enterprises use the cloud platform, the security of facilities provides the basic guarantees, including the security of the server, network and user identity management. Server security mainly refers to the security of the infrastructure, such as the keys being lost, the port listening to hijack accounts, and etc. Network security refers to the existing Internet DOS attack, hacker malicious behaviours such as network intrusions. And security of the user identity management includes the authenticity and reliability of user identity. It is possible that the users' information was stolen or false users can freely access the cloud.

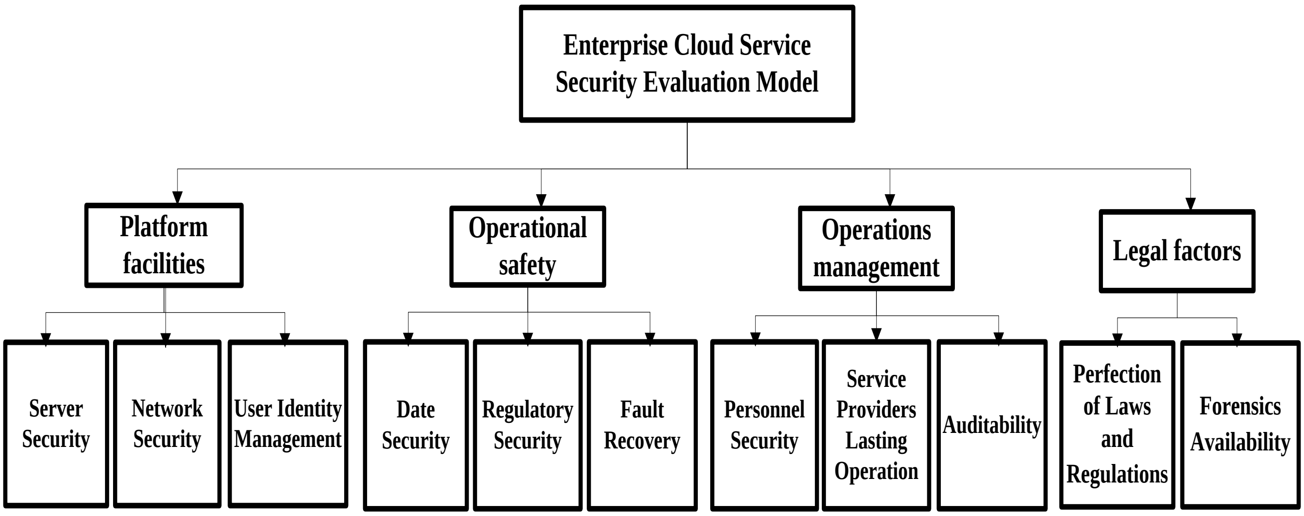


FIGURE 1 Security evaluation model of the ECSs

2.1.2 Operational safety

The security of the data resources is the most important in the cloud security. The regulation and recovery also need to be considered during the operation of services. The data security includes the security of the storage, migration, integrity, and etc. But there are still some security threats that the data isn't transferred completely or left history list. The security threats of regulatory mainly reflect that whether the security reports and the early warning system are submitted regularly. And the security threats of fault repair refer to the difficulty of restoring, retrieving or locating effectively when unknown security threats occurred.

2.1.3 Operations management

The specific model of cloud service strengthens the collaboration between users and providers. Nevertheless, the uncertainty of human resource and management increases the risk. In the operating process, the durable operation and auditability also need to be considered.

2.1.4 Legal factors

Cloud services make it complex to abide the laws and regulations. Different places have different rules. For example, some regulations require that certain data cannot be mixed with other data in a shared server or database; in some countries and regions, the citizens' data must be retained locally. As a large-scale resource centre, the cloud makes the data closer and breaks the geographical restrictions, but it brings the legal problems about data isolation and privacy protection at the same time. Besides, there are more security threats such as incomplete laws and regulations as well as the more difficultly forensic processes.

2.2 BUILDING SECURITY EVALUATION MODEL OF THE ECSS

Base on the mentioned factors and the principle of AHP [11], the model is established as shown in figure 1.

3 Security evaluation of the ECSs base on GFAHP

In order to reduce the large subjective errors in the evaluation and decision, this paper uses a new algorithm to comprehensively evaluate the security of the ECSs which combines grey theory with fuzzy AHP to form an integrated algorithm called the grey fuzzy AHP (GFAHP).

3.1 DETERMINE THE FUZZY CONSISTENT MATRIX AND THE WEIGHT SET

3.1.1 Determine the assembly of evaluation factors

The model is divided into 4 first-level indexes and 11 second-level indexes, respectively recorded as B_i, C_{ij}, index set $B=(B_1,B_2,\ldots,B_m)$, which, m is the total number of categories for the indicator, $B_i=(C_{i1},C_{i2},\ldots C_{in})$, $(i=1,2,\ldots n)$, where n is the sub-index number of categories of the category i.

$B=(B_1,\ B_2,\ B_3,\ B_4)$,

$B_1=(C_{11},\ C_{12},\ C_{13})$,

$B_2=(C_{21},\ C_{22},\ C_{23})$,

$B_3=(C_{31},\ C_{32},\ C_{33})$,

$B_4=(C_{41},\ C_{42})$.

3.1.2 Determine the weight set

First, we establish the fuzzy consistent matrix. Let the experts to adopt 0.1-0.9 scale method [12] on the various indicators to judge by the statistics and analysis, then we establish the fuzzy judgment matrix. Respectively obtain the upper layers of fuzzy consistent matrixes R, R_1, R_2, R_3, R_4 by the consistency of conversion.

Second, we do the consistency check by using fuzzy consistent judgment matrix properties on the judgment matrix.

Finally, we calculate the weight of each factor in fuzzy consistent matrix set. Known for each element of the fuzzy consistent judgment matrix $R=(a_1,\ a_2,\ldots,\ a_n)$, the weights were set as $w_1,w_2,\ldots w_n$, the weight calculation formula [13] is:

$$W_i=\frac{1}{n}-\frac{1}{2a}+\frac{1}{na}\sum_{k=1}^{n}r_{ik},(i=1,2,\ldots,n)$$

And a is the parameter, here we take $a=\frac{n-1}{2}$. It can significantly reflect the difference and identification among the indicator elements.

After expert scoring and the calculation of the above steps, get the index system of weights set are shown in table 1 as follows:

TABLE 1 Index system of the total weight value

A	First level index	First level index weight	Second level index	Second level index weight	
				Single weight	Total weight
Security evaluation of the ECSs	B_1	0.2850	C_{11}	0.3134	0.0893
			C_{12}	0.3633	0.1035
			C_{13}	0.3233	0.0921
	B_2	0.3050	C_{21}	0.4334	0.1322
			C_{22}	0.3133	0.0956
			C_{23}	0.2533	0.0773
	B_3	0.2183	C_{31}	0.3233	0.0706
			C_{32}	0.3867	0.0844
			C_{33}	0.2900	0.0633
	B_4	0.1917	C_{41}	0.5300	0.1016
			C_{42}	0.4700	0.0901

3.2 GREY FUZZY COMPREHENSIVE EVALUATION

3.2.1 Determine the evaluation grade and sample evaluation matrix

According to evaluation requirements, the review set is divided into five grades. $V=(V1,V2,V3,V4,V5)$ = (Very safe, relatively safe, generally safe, not safe, unsafe). Suppose there are p evaluators, according to the range 0 to 10 score, get the evaluation sample matrix X:

$$X=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & \cdots & x_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{np} \end{pmatrix},$$

x_{ij} - the j evaluator to C_i index of evaluation results.

3.2.2 Determine the evaluation of grey type

Determine the evaluation of grey type is to determine the rating number of the grey type evaluation, a grey degree and whitening weight function of grey number. Grey type must be defined by evaluation grade and qualitative analysis. Divide evaluation of grey type into five categories and serial set of grey type evaluation is $k = \{1,2,3,4,5\}$. Then, make the whitening weight function $f_k(k \in \{1,2,3,4,5\})$ as follows [14]:

$$f_1(x) = \begin{cases} 0; x_{ij} < 0 \\ \frac{1}{9}x_{ij}; x_{ij} \in [0,9] \\ 1; x_{ij} \in [9,+\infty] \end{cases}, \quad f_2(x) = \begin{cases} 0; x_{ij} \notin [0,14] \\ \frac{1}{7}x_{ij}; x_{ij} \in [0,7] \\ -\frac{1}{7}x_{ij}+2; x_{ij} \in [7,14] \end{cases},$$

$$f_3(x) = \begin{cases} 0; x_{ij} \notin [0,10] \\ \frac{1}{5}x_{ij}; x_{ij} \in [0,5] \\ -\frac{1}{5}x_{ij}+2; x_{ij} \in [5,10] \end{cases}, \quad f_4(x) = \begin{cases} 0; x_{ij} \notin [0,6] \\ \frac{1}{3}x_{ij}; x_{ij} \in [0,3] \\ -\frac{1}{3}x_{ij}+2; x_{ij} \in [3,6] \end{cases},$$

$$f_5(x) = \begin{cases} 0; x_{ij} \notin [0,5] \\ 1; x_{ij} \in [0,1] \\ -\frac{1}{4}x_{ij}+\frac{5}{4}; x_{ij} \in [1,5] \end{cases}.$$

3.2.3 Determine the grey number

The evaluation grey number of the index C_{ij} that belongs to the k th evaluation grey type is $n_{ijk} = \sum_{n=1}^{m} f_k(x_n)$

The overall evaluation grey number of C_{ij} that belongs to the all grey type is $n_{ij} = \sum_{k=1}^{5} n_{ijk}$.

3.2.4 Determine the grey evaluation weight

The k th grey evaluation weight of the j th evaluation index in the i th project is $y_{ijk} = n_{ijk} / n_{ij}$.

So we can structure the grey fuzzy weight matrix Y_i.

3.2.5 Calculate the grey fuzzy comprehensive evaluation matrix

Calculate the grey fuzzy comprehensive evaluation matrix of the i th project according to weight set and grey and fuzzy weight matrix. $Z_i = W_i \cdot Y_i;\ i\{1,2,3,4\}$.

3.2.6 Calculate the evaluation result

$Z = W * (Z_1, Z_2, Z_3, Z_4)^T$, Z is the result of the grey fuzzy comprehensive evaluation, according to the maximum membership degree principle to evaluate enterprise cloud service security.

4 Data and computation

This paper investigates the evaluation of application project of cloud email in a large manufacturing enterprise. It aims to comprehensively evaluate the security level of enterprise cloud mailbox project.

For various factors of security, the evaluation team adopts the form of scoring table. The five team members

Include the senior leadership of the manufacturing companies, IT department members, cloud computing experts. Scores as shown in Table 2.

TABLE 2 Enterprise cloud services security index mark sheet

	C_{11}	C_{12}	C_{13}	C_{21}	C_{22}	C_{23}	C_{31}	C_{32}	C_{33}	C_{41}	C_{42}
1	8	8	7	7	6	7	6	8	5	5	4
2	7	6	4	7	7	6	9	9	8	7	2
3	8	7	7	8	10	7	5	6	7	5	5
4	8	6	8	7	6	8	6	9	4	6	6
5	6	8	7	7	9	3	5	5	6	7	3

4.1 CALCULATE THE GREY NUMBER

The sample matrix is calculated to get the grey numbers of C_{11} index according to the formula $n_{111} = \sum_{n=1}^{5} f_1(x_{n1})$.

$= f_1(8) + f_1(7) + f_1(8) + f_1(8) + f_1(6) = 4.111$

Similarly $n_{112} = 4.429, n_{113} = 2.600, n_{114} = 0, n_{115} = 0$.

Finally $n_{11} == \sum_{j=1}^{5} n_{11j} = 11.14$.

4.2 CALCULATE THE GREY FUZZY WEIGHT MATRIX

To C11 index, the grey evaluation weights are: $y_{111} = n_{111} / n_{11} = 4.111/11.14 = 0.369$, $y_{112} = 0.398, y_{113} = 0.233, y_{114} = 0, y_{115} = 0$.

The grey evaluation weight vector is: $y_{11} = (y_{111}, y_{112}, y_{113}, y_{114}, y_{115})$ $= (0.369, 0.398, 0.233, 0, 0)$

Similarly $y_{12} = (0.344, 0.391, 0.265, 0, 0)$, $y_{13} = (0.305, 0.369, 0.250, 0.056, 0.021)$

Finally

$$Y_1=\begin{bmatrix}y_{11}\\y_{12}\\y_{13}\end{bmatrix}=\begin{bmatrix}0.369&0.398&0.233&0&0\\0.344&0.391&0.265&0&0\\0.305&0.369&0.250&0.056&0.021\end{bmatrix},$$

$$Y_2=\begin{bmatrix}0.343&0.417&0.240&0&0\\0.391&0.381&0.228&0&0\\0.339&0.317&0.229&0.076&0.038\end{bmatrix},$$

$$Y_3=\begin{bmatrix}0.293&0.328&0.323&0.057&0\\0.351&0.330&0.291&0.028&0\\0.274&0.328&0.295&0.082&0.021\end{bmatrix},$$

$$Y_4=\begin{bmatrix}0.271&0.349&0.326&0.054&0\\0.173&0.222&0.280&0.208&0.117\end{bmatrix}.$$

4.3 CALCULATE THE SECOND LAYER OF GREY FUZZY

The comprehensive evaluation vectors can be calculated by the formula: $Z_i = W_i \cdot Y_i$.

The results are:

$Z_1 = (0.3292\ 0.3861\ 0.2501\ 0.0181\ 0.0068)$

$Z_2 = (0.3570\ 0.3804\ 0.2335\ 0.0193\ 0.0096)$

$Z_3 = (0.3099\ 0.3288\ 0.3025\ 0.0530\ 0.0061)$

$Z_4 = (0.2249\ 0.2893\ 0.3044\ 0.1264\ 0.0550)$

4.4 CALCULATE THE FIRST LAYER OF GREY FUZZY COMPREHENSIVE EVALUATION VECTOR

$$Z = W\cdot\begin{bmatrix}Z_1\\Z_2\\Z_3\\Z_4\end{bmatrix}.$$

$=(0.3135\ 0.3533\ 0.2669\ 0.0502\ 0.0167)$

The results show that the maximum of Z is 0.3533, according to the maximum membership degree principle, the cloud email security level is identified as "relatively safe".

5 Conclusion

This paper investigates the assessment of the security of ECSs.

First, the influence factors of ECSs are analysed to construct an evaluation index system.

Second, based on the index system, the paper give the specific modelling steps:

(1) Establish a fuzzy consistent matrix and the value of the index weighting factor Wi;

(2) Create a score sample matrix and make it be whitened;

(3) Use the grey fuzzy comprehensive evaluation.

Finally, the security evaluation of cloud services in a large manufacturing enterprise is investigated to demonstrate the validity and effectiveness of the proposed model.

With the development of ECSs, their security evaluation index system will be correspondingly developed to stimulate new security evaluation models. Therefore, further researches will be devoted to a further and deeper understanding of the index system to construct the more comprehensive models.

Acknowledgments

1. The MOE Layout Foundation of Humanities and Social Sciences (12YJA630176); 2. Fundamental Research Funds for the Central Universities (2011HGBZ1324).

References

[1] Amazon Security Bulletins [EB/OL] http://aws.amazon.com/security/security-bulletins/2009

[2] Google [EB/OL] http://googledocs.Blogspot.Com/2009/03/just-to-clarify.html 2009

[3] Microsoft. [EB/OL] http://www.Microsoft.Com/technet/security/2010

[4] Gartner, Teleworking in the cloud: Security risks and remedies 2010 [2010-11-11] http://www.gartner.com/resources/167600/137661/teleworking_in_the_cloud_sec_167661.pdf

[5] Feng D G, Zhang M, etc. 2011 Study on Cloud Computing Security *Journal of Software* **22** 71-83 2011

[6] Fu S, Liao M H, etc. 2012 Research and Exploration on Fuzzy AHP in the Field of Information Security *Journal of The China Society For Scientific and Technical Information* **31**(10) 1105-9

[7] Huang J X, Ding J L 201 Evaluation model for information system risk based on fuzzy analysis *Computer engineering and design* **33**(4) 1285-9

[8] Huang Ying, Shi Wenchang 2011 Survey of Research on Cloud Infrastructure Security *Computer Science* **38**(7) 24-9

[9] Liu Kaihua, Li Xiong 2011 Analyse the Security Model and Policy of Cloud Computing *Computer Knowledge and Technology* **7**(8) 1150-1

[10] Ma X T, Chen C 2011 On the Threat to the Security of Digital Library Information Resource and Its Tactics: Under the Environment of Cloud Computing *Information and Documentation Services* **2** 55-9

[11] Xu S B 1988 *The principle of analytic hierarchy process* Tianjin: Tianjin University Publisher

[12] Zhang J J 2000 Fuzzy analytic hierarchy process *Fuzzy Systems and Mathematics* **6** 80-8

[13] Lv Y J 2002 Fuzzy AHP Sort based on Fuzzy Consistent Matrix *Fuzzy Systems and Mathematics* **2** 81-2

[14] Liu S F, Xie N M 2011 New grey evaluation method based on reformative triangular whitenization weight function *Journal of Systems engineering* **26**(2) 244-50

[15] Yang X K, Wang Y Z 2012 Government Information Sharing Capability Evaluation based on Grey Fuzzy Theory *Journal of Dalian University of Technology* **52**(2) 297-303

[16] Wang J S, Fu Y, etc. 2011 Information System Security Risk Assessment based on Fuzzy Neural Network *Wuhan University of Technology (Transportation Science & Engineering Edition)* **35**(1) 51-4, 58

[17] Chen Y, Katz VPARH 2010 What's New About Cloud Computing Security? *Electrical Engineering and Computer Sciences*

[18] Carlin S, Curran K 2011 Cloud computing Security *International Journal of Ambient Computing and Intelligence (IJACI)* **3**(1) 14-9

[19] Jamil D, Zaki H 2001 Cloud computing security *International Journal of Engineering Science and Technology* **3**(4) 3478-83

[20] Sriram I, KhajehHosseini A 2010 Research Agenda in Cloud Technologies *Technical Report*

[21] Armbrust M, Fox A, Griffith R, et.al. 2009 Above the clouds: A Berkeley view of cloud computing *Communication Magazine*

[22] Chang D Y 1996 Applications of the extent analysis method on fuzzy AHP *European journal of operational research* **95**(3) 649-55

[23] Gumus A T 2009 Evaluation of hazardous waste transportation firms by using a two step fuzzy- AHP and TOPSIS methodology *Expert Systems with Applications* **36**(2) 4067-74

[24] Chiou H K, Tzeng G H 2001 Fuzzy hierarchical evaluation with grey relation model of green engineering for industry *International Journal of Fuzzy Systems* **3**(3) 466-75

[25] Ho W, Xu X, Dey P K 2010 Multi-criteria decision making approaches for supplier evaluation and selection: A literature review *European Journal of Operational Research* **202**(1) 16-24

[26] Marciano F A, Vitetta A 2011 Risk analysis in road safety: An individual risk model for drivers and pedestrians to support decision planning processes *International Journal of Safety and Security Engineering* **1**(3) 265-82

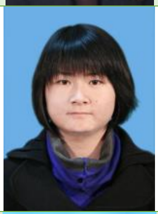
[27] De Wrachien D, Mambretti S 2011 Mathematical models for flood hazard assessment *International Journal of Safety and Security Engineering* **1**(4) 353-62

[28] Bertino E, Paci F, Ferrini R 2009 Privacy - preserving digital identity management for cloud computing *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering* **32**(1) 21-7

Authors

Yu Bengong, born on December 29, 1971, Hefei, Anhui, China

Current position, grades: Director of the Department of information management.
University studies: Hefei University of Technology
Scientific interest: decision-making science and technology, information system.
Experience: Yu Bengong received the B.Sc. degree (1994) in Computer Science, the M.Sc. degree (2005) and Ph.D. degree (2011) in Management Science and Engineering from Hefei University of Technology, Hefei, China. He is currently working as an professor for School of Management at Hefei University of Technology, Hefei, Anhui, China.



Wang Liu, born on December 14, 1989, Huanggang, Hubei, China

Current position, grades: Master of Hefei University of Technology, grade two
University studies: Hefei University of Technology
Scientific interest: information management, information system
Experience: Wang Liu is currently studying for the master degree, and received the B.Sc degree (2012) in Information Management and Information System from Hefei University of Technology.

Fengyi Guo, born on December 23, 1987, Luoyang, Henan, China

Current position, grades: Master of Hefei University of Technology, graduate
University studies: Hefei University of Technology
Scientific interest: information management, information system
Experience: Guo Fengyi received the master degree (2013) in Information Management and Information System from Hefei University of Technology, Hefei, Anhui, China.