BENTHAM OPEN

CrossMark

The Open Cybernetics & Systemics Journal

Content list available at: www.benthamopen.com/TOCSJ/

DOI: 10.2174/1874110X01610010210

RESEARCH ARTICLE

A Research for Cloud Computing Security Risk Assessment

Hua Tang[*, 1,2], Jiejun Yang[1,3], Xiaofang Wang[1] and Qi Zhou[4]

[1]*College of Safety Science and Engineering, Nanjing Tech University, Nanjing, Jiangsu, 211800, China*
[2]*Information Technology Center, Hubei University of Technology, Wuhan, Hubei, 430068, China*
[3]*School of Legal Studies, Guangdong University of Foreign Studies, Guangzhou, Guangdong, 510420, China*
[4]*School of Industrial Design, Hubei University of Technology, Wuhan, Hubei, 430068, China*

Received: May 19, 2016 Revised: September 08, 2016 Accepted: September 09, 2016

Abstract: In order to solve the problem of the complexity of the process and the accuracy of evaluation results in cloud computing security risk assessment, the hierarchical holographic modeling method is applied to cloud computing risk identification phase, so as to clearly capture the cloud computing risk factors through a comprehensive analysis of cloud computing security domains. Moreover, with cloud computing security factors as the basic unit, fuzzy set theory and entropy weight method are used to accurately quantify the probability of cloud computing security risks and the resulting losses for a comprehensive assessment of cloud computing security risks. Finally, an example is given for calculation and verification, and the deficiencies of cloud computing security risk assessment are analyzed.

Keywords: Cloud computing security, Entropy weight method, Fuzzy set theory, Hierarchical holographic modeling, Risk assessment.

1. INTRODUCTION

In June 2008, the world-famous research firm Gartner issued a report "Assessing the Security Risks of Cloud Computing" in which cloud computing security risks have been studied for the first time from the perspective of risk management with specific elaboration on seven risks such as user access, regulatory compliance, and so on. In April 2009, the nonprofit organization Cloud Security Alliance (CSA) released "Security Guidance for Critical Areas of Focus in Cloud Computing" which promotes the best practice of cloud computing security in a standardized form. As cloud computing security issues become increasingly prominent, research on cloud computing security risk theories has received increasing concern in the industry and academics. Neela, K. L. *et al*. analyzed the security risks, threats, and the impact on different users of cloud computing [1]. Latif R. *et al*. elaborated the risk factors of cloud users/business organization cloud environment and mapped them as the actual needs of cloud users / business organization [2]. Considering all kinds of security risk factors provided by cloud computing risk management decision support system, Fan C.K. *et al*. adopted a model algorithm to complete the identification and analysis of the losses resulting from cloud computing risks, and maintained social engineering, cross-cloud compatibility, and mistakes made by employees as high risk factors in a variety of cloud applications [3]. By exploring a variety of risks in cloud computing, Schllings C. and Simon S. used risk breakdown structure (RBS) from the perspective of cloud users and proposed specific measures and recommendations based on the analysis and evaluation of the extracted risk factors [4]. Through designing a cloud computing security risk assessment model, Wang H.B. *et al*. put forward a specific risk assessment method, with which the vulnerability of security management in cloud computing environment was revealed effectively in the experimental environment [5]. Using standards such as ISO 27005, NIST SP800-30 and AS/NZS 4360, Albakri S. H. *et al*. presented a security risk assessment framework which allows not only cloud service providers' assessment on security risks in

* Address correspondence to this author at the Information Technology Center, Hubei University of Technology, Wuhan, Hubei, 430068, China; Tel: +86 27 59750810; Fax: +86 27 59750815; E-mails: th@mail.hbut.edu.cn, tanghua_2008@163.com

cloud computing environment but also cloud customers' contribution to risk assessment. Through cloud clients' evaluation on the security risk factors, the framework can provide a more realistic and accurate risk assessment, and thereby reduce the complexity of customer participation in the process of risk assessment [6].

2. THE CONNOTATION OF CLOUD COMPUTING SECURITY RISK ASSESSMENT

According to the theory of risk management, cloud computing security risk assessment involves cloud computing security risk identification, risk calculation and other processes so as to effectively meet the requirements of cloud computing in the SLA commitment and QoS constraint service selection. Firstly, cloud computing related assets, such as cloud infrastructure, computing resources, application software, and cloud users, and threats to these assets are listed and organized into risk source table to identify the main risk factors through the corresponding risk identification model. Secondly, the probability of risk occurrence resulting from cloud computing threats and vulnerabilities is calculated according to related theories and methods and the "high probability" of cloud computing security risk consequences is inferred. Meanwhile, under certain conditions, the extent of potential losses is relatively accurately calculated and cloud computing security risk level is determined so as to provide support for cloud computing service providers, cloud users and regulators in risk decision-making and implementation.

Concerning domestic and international academic and industrial world, the theory and practice of cloud computing security started late, research on cloud computing security risk assessment is even scarcer. There are two major problems: one is the lack of systematic research on the whole process of cloud computing security risk assessment with either focus on cloud computing security risk analysis or risk calculation; the other is the tendency of qualitative research rather than quantitative research which, if any, is only applied to some specific areas (such as storage resources).

3. CLOUD COMPUTING SECURITY RISK ASSESSMENT

3.1. Identification of Cloud Computing Security Risks

The components of cloud computing (as a pay-per-use model) can not only be allocated, deployed and recovered quickly, but also reduced or expanded swiftly. This high scalability and flexibility has brought considerable convenience and benefits for users, but also many difficulties in cloud computing security risk management, especially in risk identification. In Hierarchical Holographic Modeling (HHM), with the system as the research object, the inherent nature is displayed through a multi-angle and multi-dimensional analysis in the form of a chart framework. In order to obtain a full understanding of large-scale systems and reveal the essential characteristics of the system, HHM divides the large and complex system into different classifications from different angles and aspects. Each classification can only describe the relevant content and attributes of a certain aspect of the hierarchical system which break down in a stepwise manner until the last breakdown.

HHM method is suitable for solving large-scale complex problems. Considering the complexity, randomness and uncertainty of security risk identification of cloud computing, with the application of HHM, the definition and identification according to the background reasons, characteristics and expected consequences of cloud computing security risks, and the hierarchical classification of all risk factors, cloud computing system can be described hierarchically from different perspectives and comprehensive security risk identification and inherent relationship between different risk factors can be organized effectively [7]. The major steps are as follows:

I. Compilation and analysis of historical data. Before cloud computing security risk identification, the existing theoretical research and related materials on cloud computing security risk factors and security applications are collected, collated and analyzed.

II. Establishment of HHM framework of cloud computing security risk. A full understanding of cloud computing risks is acquired by means of expert research and academic seminars, and a preliminary HHM framework of cloud computing security risks is established. In this paper, according to the security architecture of cloud computing, cloud computing security risk factors are analyzed from three domains (1^{st} hierarchy), which are cloud computing security operation management, cloud computing security technology implementation and cloud computing security support platform [8] to establish the preliminary HHM framework.

III. Identification of cloud computing security risks. Based on the HHM framework, the three domains of cloud computing security risks are broken down again. The domain of cloud computing security operation management, for

example, can be broken down into security operations, business continuity and backup and security operation organization process (2nd hierarchy). Security operations can be classified into four factors – monitoring and warning, security scan and penetration test, security audit and privacy protection (3rd hierarchy). At this point, these four specific factors cannot be broken down again, and therefore they are the atomic objects in the final analysis of cloud computing security system.

IV. Analysis of cloud computing security risks. Cloud computing security risk factors are analyzed based on HHM to identify potential security risks and risk factors and establish a formal cloud computing security risk factors HHM framework (Fig. **1**), which lays the foundation for cloud computing security assessment.

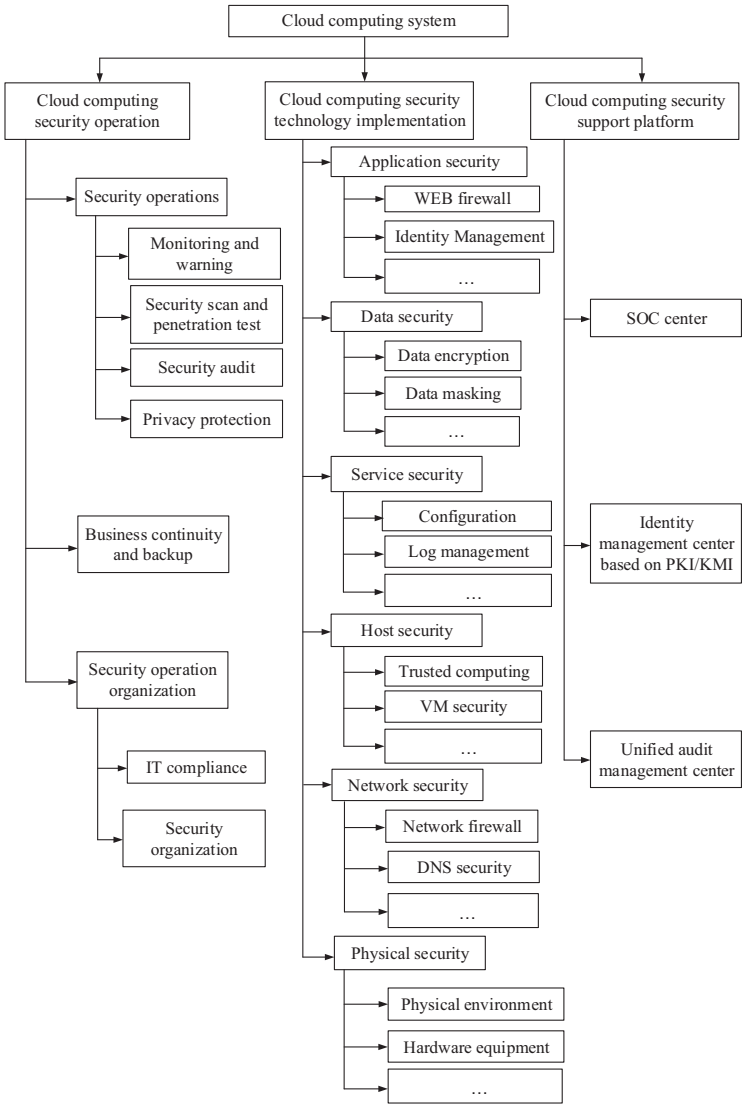

Fig. (1). Cloud computing security risk factors HHM framework.

It should be noted that cloud computing security risk identification requires a cyclic iterative process (factor acquisition → cloud computing security HHM diagram → factor acquisition → …) to ultimately determine cloud computing security risk factors. If a certain cloud computing security risk source cannot be determined by using the current HHM framework, then the framework should be constantly improved and extended in new dimensions for the identification of all cloud computing security risk factors through the continuous cycle. According to "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0" released by Cloud Security Alliance (CSA), cloud computing security operation management involves cloud computing architectural framework, governance and enterprise risk management, legal issues and electronic discovery, compliance and audit, information management and

data security and other key domains; cloud computing security technology implementation includes traditional security, business continuity and disaster recovery, data center operations, incident response, application security, encryption and key management, identity, entitlement and access management, virtualization, *etc*.; cloud computing security operation management, technology implementation and support platform all demonstrate the critical domain of security as a service. As interoperability and portability (Domain 6) involves business compatibility and portability among multiple operators, it is not unique to cloud computing risk factors. Therefore by applying HHM to cloud computing security risk identification phase, risk factors can be fully captured and identified.

3.2. Cloud Computing Security Risk Calculation

Cloud computing security risks and the probability of potential security incidents along with the resulting losses are closely related. Therefore, the probability and losses must be quantified for relatively accurate measurement of cloud computing security risks. According to GB/T 20984-2007 (Risk Assessment Specification for Information Security), risk calculation of information systems follows the paradigm: risk value = $R(A, T, V)$ (R represents a security risk calculation function; A stands for assets; T represents threats, V indicates vulnerability). The degree of the impact of risk on assets, threat frequency and vulnerability severity is defined as levels 1-5. Cloud computing is a "special" information system, and its security risk value R can be regarded as function of assets, threats and vulnerability. Namely, cloud computing security risk $R = G(c, t, f)$, where c is impact on assets, t is threat frequency, f is vulnerability severity.

As shown in HHM framework, risk factors resulting in cloud computing security incidents have the characteristics of complexity, ambiguity and uncertainty. Therefore, fuzzy comprehensive evaluation method is chosen for the calculation of cloud computing security risks [9, 10]. The evaluation of security risk factors and the construction of membership matrix of the corresponding evaluation set are completed with the use of fuzzy set theory from dimensions of impact on assets, threat frequency and vulnerability severity, and the entropy weight method is used to determine the weight of risk factors to the security risks of cloud computing. Ultimately the security risk values of the three dimensions are determined and quantified into cloud computing security risk values and their corresponding levels.

3.2.1. Fuzzy Sets and Membership Matrices

Firstly, a set of risk factors for cloud computing security is established. Let $A=\{a_1, a_2,\ldots, a_n\}$, where n is the number of risk factors.

Secondly, evaluation sets are constructed. Different evaluation sets B_c, B_t, B_f are set up for assets, threats and vulnerability respectively: $B_c = \{b_{c1}, b_{c2}, \ldots, b_{ci}\}$, $B_t = \{b_{t1}, b_{t2}, \ldots, b_{tj}\}$, $B_f = \{b_{f1}, b_{f2}, \ldots, b_{fk}\}$, where i, j and k represent the number of factors in corresponding evaluation sets.

Thirdly, fuzzy mapping is conducted. Different factors in risk factor set A are evaluated with the use of evaluation set B, and fuzzy mapping is $f{:}A\rightarrow F(B)$. $F(B)$ is the fuzzy set of B, $a_i \rightarrow f(a_i) = \{p_{i1}, p_{i2},\ldots,p_{im}\} \in F(B)$, where f represents the degree of support of risk factor a_i for each index in evaluation sets.

Fourthly, membership matrices are constructed. The membership vector of risk factor a_i for evaluation set B is $p_i = \{p_{i1}, p_{i2},\ldots,p_{im}\}$ (i=1,2,…,n), where n is the number of risk factors and m is the number of indexes in corresponding evaluation sets. Cloud computing security risk membership matrix is:

$$\boldsymbol{P} = \begin{bmatrix} p_{11} & p_{12} & \ldots & p_{1m} \\ p_{21} & p_{22} & \ldots & p_{2m} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \ldots & p_{nm} \end{bmatrix}$$

Similarly, membership matrices of impact on assets, threat frequency and vulnerability severity are P_c, P_t and P_f respectively.

3.2.2. Entropy Weight of Risk Factors

Firstly, assuming that the system may be in different states n: $S_1, S_2,\ldots,S_n$, P_i represents the probability that the

system is in state S_i, where i=1,2,…,n, $0 \le P_i \le 1$, $\sum_{i=1}^{n} P_i \ln P_i = 1$. Then the entropy can be expressed as:

$$H\left(p_1, p_1, \cdots, p_n\right) = \sum_{i=1}^{n} P_i \ln P_i \tag{1}$$

The information entropy H indicates the orderly degree of the system.

Secondly, the relative importance of risk factor a_i can be measured by entropy:

$$H_i = \sum_{j=1}^{m} P_{ij} \ln P_{ij} \tag{2}$$

Here p_{ij} (i=1,2,…,n;j=1,2,…,m) represents the degree of support of risk factors for each index in evaluation sets. The closer they are equal to each other, the greater the entropy value and uncertainty of risk factor a_i to cloud computing security assessment is.

Thirdly, formula (2) is normalized by using $H_{\max}$ ($H_{\max}$=ln$m$) for the entropy of relative importance which measures cloud computing security risk factor a_i:

$$e_i = \frac{1}{\ln m} \sum_{j=1}^{m} P_{ij} \ln P_{ij} \tag{3}$$

According to the formula (2), when the values of p_{ij} are equal, e_i is the maximum value 1, that is $0 \le e_i \le 1$. When the entropy of relative importance of risk factor a_i is the maximum value, this risk factor's contribution to cloud computing security risk assessment is the smallest.

Fourthly, normalization is conducted again by using 1-e_i to represent the weight of cloud computing security risk factor a_i, and the weight value is:

$$\varphi_i = \frac{1 - e_i}{n - \sum_{i=1}^{n} e_i} \tag{4}$$

3.2.3. Index Weight Vector of Each Evaluation Set

When calculating the impact on assets, the corresponding weight is given to each index in evaluation sets, and the index weight vector $U_i = (u_1, u_2, \ldots, u_i)$. Similarly, the index weight vector of threat frequency evaluation set is $V_j = (v_1, v_2, \ldots, v_j)$, and the index weight vector of vulnerability severity evaluation set is $W_k = (w_1, w_2, \ldots, w_k)$.

3.2.4. Cloud Computing Security Risk Values

According to the formula (4), the corresponding weight vector of cloud computing security risk factors is $\varphi_i = (\varphi_1, \varphi_2, \ldots, \varphi_n)$, where i=1,2,…,n. The security risk value of impact on assets is:

$$R_{\mathrm{c}} = \boldsymbol{\varphi}_i \boldsymbol{P}_{\mathrm{c}} \boldsymbol{U}_{\mathrm{t}}$$

$$= (\varphi_1, \varphi_2, \ldots, \varphi_n) \begin{bmatrix} p_{11} & p_{12} & \ldots & p_{1m} \\ p_{21} & p_{22} & \ldots & p_{2m} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \ldots & p_{nm} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_i \end{bmatrix} \tag{5}$$

Similarly, the security risk values of threat frequency and vulnerability severity are R_{t} and R_{f}. Cloud computing security risk value is:

$$\begin{aligned} R &= G\left(c,\ t,\ f\right) = R_{\mathrm{c}} \oplus R_{\mathrm{t}} \oplus R_{\mathrm{f}} \\ &= k_1 R_{\mathrm{c}} + k_2 R_{\mathrm{t}} + k_3 R_{\mathrm{f}} \end{aligned} \tag{6}$$

Here k_1, k_2 and k_3 represent the relative importance of the three aspects, and satisfy $k_1 + k_2 + k_3 = 1$.

As shown in cloud computing security risk factors HHM framework, cloud computing system is composed of multiple security domains; a cloud security domain is composed of multiple security classes and a certain security class is composed of multiple risk factors. The overall risk level value of cloud computing is:

$$R = \sum_{j=1}^{m} w_{ij} R_{ij} \sum_{i=1}^{n} w_i R_i \tag{7}$$

Here w_i stands for the weight of the i-th security class in a specific domain (i=1,2,…,n), and satisfies $w_1 + w_2 + \ldots + w_n = 1$; R_i stands for the risk value of the n-th security class. w_{ij} represents the weight of the j-th security domain (j=1,2,…,m), and satisfies $w_{i1}+w_{i2}+\ldots+w_{in}=1$; R_{ij} represents the risk value of the j-th security domain.

3.2.5. Cloud Computing Security Risk Levels

When the security risk value of cloud computing system is determined, security risk level can be decided according to security risk membership levels (Table **1**).

Table 1. Security risk membership levels.

R	0-0.2	0.2-0.4	0.4-0.6	0.6-0.8	0.8-1.0
Levels	Low	Relatively low	Medium	Relatively high	High

4. APPLICATION CASE

To verify the validity and correctness of the construction system and assessment method in this paper, a cloud computing platform of a school is used as an example for analysis. Security assessment is conducted in security domains of cloud computing security operation management, technology implementation and support platform.

4.1. Construction of Cloud Computing Risk Factors and Evaluation Sets

For simplicity, only the domain of "cloud computing security technology implementation" is used for analysis in this article. According to cloud computing security risk factors HHM framework (Fig. **1**), security risk in this domain is subdivided and the risk factor set is as follows:

Given the parallel linear property of the secondary classification A_1, A_2,…, A_6, here only application security (A_1) is discussed, and the method can be applied to other classes. The security class A_1 consists of six risk factors (Table **2**), and its factor set is $\{a_1, a_2, a_3, a_4, a_5, a_6\}$. The assessment on impact on assets, threat frequency and vulnerability severity is categorized into five levels: high, relatively high, medium, relatively low, and low. Hence the evaluation set of A_1 is $B_c = \{b_{c1}, b_{c2},\ldots,b_{c5}\}$, $B_t = \{b_{t1}, b_{t2},\ldots,b_{t5}\}$, $B_f = \{b_{f1}, b_{f2},\ldots,b_{f5}\}$.

Table 2. Risk factor set in cloud computing security technology implementation domain.

Security domain	Security classes	Risk factors
Cloud computing security technology implementation	Application security (A_1)	WEB firewall, identity management, binary analysis, terminal access security, application security, application scanner
	Data security (A_2)	Data encryption, data masking, data residual erasure, access control, backup and recovery, data lineage
	Services security (A_3)	Configuration management, log management, identity management, vulnerability management
	Host security (A_4)	Trusted Computing, VM security, host firewall, intrusion prevention
	Network security (A_5)	Network firewall, DNS security, intrusion detection, anti-DDOS, QoS / DNS Security
	Physical security (A_6)	Physical environment, hardware equipment, personnel security

4.2. Membership Matrix

According to expert scoring method (15 experts), the degree of influence of risk factors on assets, threats and vulnerability are rated and the probability of each risk factor belonging to each evaluation index is calculated. The corresponding membership matrices P_c, P_t, and P_f are shown in Table **3**.

Table 3. Membership matrix.

	b_{c1}	b_{c2}	b_{c3}	b_{c4}	b_{c5}	b_{t1}	b_{t2}	b_{t3}	b_{t4}	b_{t5}	b_{f1}	b_{f2}	b_{f3}	b_{f4}	b_{f5}
a_1	0.27	0.13	0.33	0.07	0.20	0.33	0.33	0.07	0.13	0.13	0.27	0.13	0.40	0.07	0.13
a_2	0.00	0.07	0.27	0.33	0.33	0.40	0.27	0.20	0.00	0.13	0.20	0.13	0.07	0.40	0.20
a_3	0.40	0.07	0.13	0.13	0.27	0.13	0.20	0.20	0.27	0.20	0.13	0.27	0.00	0.20	0.40
a_4	0.07	0.27	0.20	0.33	0.13	0.47	0.20	0.33	0.00	0.00	0.47	0.00	0.13	0.13	0.27
a_5	0.47	0.13	0.07	0.13	0.20	0.40	0.13	0.27	0.07	0.13	0.40	0.13	0.07	0.27	0.13
a_6	0.33	0.20	0.13	0.27	0.07	0.13	0.27	0.40	0.20	0.00	0.20	0.13	0.00	0.27	0.40

4.3. The Weight Vector of Each Evaluation Index

$\theta_c = (\theta_{c1}, \theta_{c2}, \theta_{c3}, \theta_{c4}, \theta_{c5}, \theta_{c6}) = (0.109, 0.313, 0.160, 0.109, 0.200, 0.109)$

$\theta_t = (\theta_{t1}, \theta_{t2}, \theta_{t3}, \theta_{t4}, \theta_{t5}, \theta_{t6}) = (0.105, 0.197, 0.017, 0.372, 0.112, 0.197)$

$\theta_f = (\theta_{f1}, \theta_{f2}, \theta_{f3}, \theta_{f4}, \theta_{f5}, \theta_{f6}) = (0.117, 0.101, 0.206, 0.252, 0.117, 0.206)$

The corresponding weights of evaluation sets of assets, threats and vulnerability are:

$U = (1/15, 5/15, 3/15, 2/15, 4/15)$

$V = (3/15, 2/15, 4/15, 1/15, 5/15)$

$W = (2/15, 3/15, 5/15, 1/15, 4/15)$

4.4. Identification of Cloud Computing Security Risk Value and Risk Level

According to formulas (5) and (6), the risk values of cloud computing application security in three dimensions (A_1) are:

$R_c = \theta_c P_c U_T = 0.186$

$R_t = \theta_t P_t V_T = 0.202$

$R_f = \theta_f P_f W_T = 0.184.$

For cloud computing application security class (A_1), assets, threats and vulnerability are of equal importance, therefore $k_1=k_2=k_3=1/3$, and the risk value of this class (A_1) is $R_1 = k_1R_c + k_2R_t + k_3R_f = 0.191$.

According to formula (7), the computing security risk value is: $R = \sum_{j=1}^{3} w_{ij}R_{ij} \sum_{i=1}^{6} w_iR_i$ =0.173, where i=6, j=3.

According to Table **1**, the cloud computing platform security risk level of this school is low.

CONCLUSION

Cloud computing security risk assessment is a complex process. In this paper, hierarchical holographic modeling method is applied in cloud computing risk identification phase, which ensures a comprehensive, effective and clear capture of risk factors. Additionally, with the application of fuzzy set theory and entropy weight method, the interrelations among various risk factors are identified and the result of risk assessment is quantified for a comprehensive evaluation. The analysis of the example demonstrates that this method is simple and feasible and it provides an effective way for the study of cloud computing security risk assessment. However, the accuracy of input data acquired by expert scoring method and whether security domains, classes and their interrelations is a simple linear relationship require further exploration and research.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

The authors would like to appreciate the support from Humanities and social science project of Hubei Provincial Department of Education (No. 15Q065).

REFERENCES

[1] K.L. Neela, V. Kavitha, and R.K. Ramesh, "Cloud computing: Threats and security issues", *Int. J. Engi. Sci. Res. Tech.,* vol. 2, no. 8, pp. 2070-2072, 2013.

[2] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud Computing Risk Assessment: A Systematic Literature Review", In: J.J. Park, I. Stojmenovic, M. Choi, and F. Xhafa, Eds., *Future Information Technology,* vol. 276. Germany Springer Publishers, Verlag: Berlin, 2014, pp. 285-295.

[3] C.K. Fan, and T.C. Chen, "The risk management strategy of applying cloud computing", *Int. J. Adv. Comp. Sci. App.,* vol. 3, no. 9, pp. 18-27, 2012.

[4] C. Schllings, and S. Simom, "Risk Management on the Security Problem in Cloud Computing", In: *First ACIS/JNU International Conference on Computer, Networks, System and Industrial Engineering,* 2011, pp. 147-152.

[5] H.B. Wang, F. Liu, and H. Liu, "A Method of the Cloud Computing Security Management Risk Assessment", In: D.H. Zeng, Ed., *Advances in Intelligent and Soft Computing,* vol. 141. Germany Springer Publishers, Verlag: Berlin, 2012, pp. 609-618.

[6] S.H. Albakri, B. Shanmugam, G.N. Samy, N.B. Ldris, and A. Ahmed, "Security risk assessment framework for cloud computing environments", *Security Com. Netw.,* vol. 7, no. 11, pp. 2114-2124, 2014. [http://dx.doi.org/10.1002/sec.923]

[7] T.P. Chen, L.J. Zheng, and X.Y. Zhang, "Application of HHM in risk identification of information system", *J. Safety Sci. Tech.,* vol. 4, no. 6, pp. 98-100, 2008.

[8] C.R. Chen, Y.T. Li, G.P. Liu, and L.W. Yang, *Cloud Computing Services - Operations, Management, and Technical Architecture.,* China Tsinghua University Publishers: Beijing, 2014.

[9] Y. Fu, X.P. Wu, Q. Ye, and X. Peng, "An approach for information systems security risk assessment on fuzzy set and entropy-weight", *Tien Tzu Hsueh Pao,* vol. 38, no. 7, pp. 1489-1494, 2010.

[10] R. Jiang, Z.F. Ma, T. Li, and Q.J. Zhang, "Study on security risk assessment for technology of cloud computing", *App. Elec. Tech.,* vol. 41, no. 3, pp. 111-115, 2015.