Cloud Security Risk Analysis Method based on Fuzzy Logic

L. Sharmila, U. Sakthi

Abstract: This paper proposes a cloud security risk assessment index system through the study of cloud computing structure and services and quantifies the risk through entropy weight and fuzzy theory. This method can determine the value of risk from the three essential attributes of assets, threats, and vulnerability, and it can be applied to the risk assessment of various types of cloud services.

Key words: Cloud Security, Risk Assessment, Fuzzy Theory.

I. INTRODUCTION

With the rapid development and widespread use of cloud computing, the security has become the key restriction element of cloud computing developing. Google's cloud computing services and domestic Ali cloud have all had security issues. The occurrence of cloud security accidents shows that while enjoying cloud computing brings high-performance computing resources, it must also carefully analyse its security issues. In the existing research, many of them only qualitatively evaluate from the risk attributes, or continuously improve an algorithm, and rarely perform a comprehensive analysis and assessment of cloud security from the perspective of attributes and the structure of cloud computing. This paper proposes a cloud security risk assessment index system through the study of cloud computing structure and services and uses entropy weight and fuzzy theory to quantify the risk. Through examples, it is shown that the method can accurately determine the value of risk from the three essential attributes of assets, threats, and vulnerabilities, and is suitable for risk assessment of various types of cloud services.

II. CLOUD SERVICE SECURITY RISK ASSESSMENT INDEX SYSTEM

Focusing on the related issues in cloud service security risk, combined with the operation flow of cloud computing service providers, this paper summarizes the risks that users may encounter during the use of cloud computing services into seven categories: virtualization, data security, infrastructure, applications, soft environments, cloud services, security management. Based on these seven types of risks, we identify measurable risk factors.

Starting from the main links, the key factors were identified and the comprehensive construction of the evaluation index system was initially completed. Then according to the meaning and characteristics of cloud service risk assessment, the established index system is analysed in depth, and the consolidation and elimination of similar indicators, repeated and unimportant indicators in the index system are completed. Finally, through consultation with relevant experts, according to their feedback opinions on the indicator system, scientific and rational improvement of the indicator system [1], the risk assessment indicator system finally established is shown in Table 1.

Table 1. Cloud Security Risk Assessment Index System

Guidelines	Influencing factors
Physical security	Unreliable physical equipment
	Dangerous configuration
	Destruction of facilities
	Inappropriate physical access control measures
	Physical location and environment are not up to standard
data security	Loss or damage of data
	Traditional cyber attacks
	Slow processing
	Privacy leaked
Application security	Versions and Patches
	Upgrade risks
	Wrong operation
	Insecure interfaces and APIs
Network Security	Spam and dissemination of illegal content
	Dangerous configuration
	Abnormal network environment development
Host security	Access control
	Malware protection
	Resource control
	Wrong operation
Management security	Regulatory mechanisms are not sound
	The standard is not uniform
	Internal threat

Manuscript published on 30 September 2019
* Correspondence Author

L. Sharmila, Research Scholar, Faculty of CSE, Department of CSE, Sathyabama Institute of Science and Technology. Email: shar.hariharan@gmail.com

U. Sakthi, Associate Professor, Department of CSE, St.Joseph's Institute of Technology, Chennai. Email: sakthi.ulaganathan@gmail.com

	Inappropriate protective measures
	Wrong operation
	Inappropriate staff and organization configuration
	System construction is not standardized

III. CLOUD SECURITY RISK ASSESSMENT METHOD BASED ON FUZZY LOGIC

In the process of using cloud services, users have a lot of risks due to uncertainty and ambiguity. In the evaluation process, fuzzy theory can effectively reduce the subjective factors of expert evaluation[2]. Therefore, the fuzzy theory is introduced into the risk assessment process of cloud security to analyse the risk factors, and combined with the theory of rampant rights, the risk value of the evaluation object is finally obtained.

A. Membership degree matrix

Focusing on the ambiguity of risk factors to assets, threats and vulnerabilities, this paper uses fuzzy theory to analyse and deal with the various factors involved in cloud service security risk assessment[3].

First, establish a set of security risk factors. Let A = $\{a_1, a_2, \dots, a_n\}$, n is the number of factors; According to the classification of assets, threats, and vulnerabilities, construct their corresponding judgement sets B = $\{b_1, b_2, \dots, b_m\}$, m is the number of elements in its corresponding evaluation set B. Finally, subjective evaluation of each risk influencing factor is made according to the evaluation set $a_i \longrightarrow f(a_i) = \{p_{i1}, p_{i2}, \dots, p_{im}\} \in F(B)$. f(B) is the total fuzzy set on B, and the function f indicates the degree of support of the factors ai for each evaluation result in each evaluation set. For evaluation set B, the membership vector of factor ai is $P_i = (p_{i1}, p_{i2}, \dots, p_{im})$, $i = 1,2, \dots, n$,

According to the influence of assets, the frequency of threats, and the severity of vulnerability[4], various factors in the risk assessment index system are divided into different degrees of membership matrix, pc, pt, and pf , Assume that the corresponding weight vector for each factor is $\theta = \{8_1, 8_2, \dots, 8_n\}$. When calculating the impact of assets, the frequency of threats, and the severity of vulnerability, each indicator in its different judging sets is weighted using the expert evaluation method, and the weight vector of the index in the asset impact evaluation set is integrated, $U = (u_1, u_2, \dots, u_{n1})$. Threat frequency vector $V = (v_1, v_2, \dots, v_{n2})$, weight vector $W = (w_1, w_2, \dots, w_{n3})$, n1 is the number of elements in the assessment of the impact of the asset, n2 is the number of elements in the assessment set of threat frequency, and n3 is the number of elements in the evaluation set of vulnerability severity. The final asset impact is: $R_c = 8 \times P_c \times U^T$, The frequency of threats is: $R_t = 8 \times P_t \times V^T$, The severity of vulnerability is: $R_f = 8 \times P_f \times W^T$.

The three risk attributes of the impact of assets, the frequency of threats, and the severity of vulnerability, this article uses a qualitative approach to its level assignment[5]. According to the degree of importance of the assets, the severity of cloud services affected by the destruction of their security attributes is divided into five levels: high(bc1), relatively high(bc2), medium(bc3), relatively low(bc4), and low(bc5). Threat frequencies are divided into five levels according to the frequency of threats: high(bt1), relatively high(bt2), medium(bt3), relatively low(bt4), and low(bt5). The severity of vulnerability is divided into five levels according to the degree of vulnerability of the vulnerability and the probability of being exploited by the threat: high(bf1), relatively high(bf2), medium(bf3), relatively low(bf4), and low(bf5)[4,5].

B. Entropy weight coefficient

The weight is also called the weight coefficient, which reflects the relative importance of each index. In the evaluation process of multiple indicators, a reasonable allocation of weight for each indicator is a key step in the evaluation [6]. The main methods of index empowerment can be divided into two major categories, namely subjective empowerment and objective weighting. Expert valuation method and AHP method are subjective weighting methods[7]. Subjective weighting method is based on expert judgment and then uses different methods to weight the indicators. Although subjective empowerment law has certain flexibility and convenience, it is difficult to weaken the influence of subjective factors and ambiguity [8].

As a complex and open system, the cloud platform has many kinds of risk factors that affect its security. Many factors are difficult to be measured and assigned directly, and most often rely on expert experience to judge[8]. However, for the assessment of the system's security risk level, even experienced experts are difficult to directly subjectively judge, and they must be analyzed, divided, and classified. The entropy value can be used to measure the size of information, and it can also determine the useful information in the obtained data. Therefore, this paper uses entropy weight theory to determine the weight.

$$H(p_1, p_2, \dots, p_n) = -k\Sigma_{i=1}\, p_i \ln p_i$$
$$H(p_1, p_2, \dots, p_n) = H(p_1, p_2, \dots, p_n, 0)$$
$$H(AB) = H(A) + H(B/A)$$

The factor A_i support factor P_i determines its role in risk assessment. The closer the P_i is to equality, proves that the data obtained by this factor is not comprehensive enough or has poor cohesiveness, and it hardly plays a role in the entire evaluation system. At this time, the entropy value also increases. Based on the actual meaning of information entropy, it can combine support P_i and information entropy to calculate the weight of each index. The closer the equality of P_{ij} in the formula is, the greater the entropy value is, and the greater the degree of uncertainty of the risk factor A_i on the entire security risk assessment, When completely equal, the entropy value reaches its maximum, $H_{max}=\ln m$.

The coefficients k_1, k_2, k_3 indicate the relative importance of the variables R_c, R_t, and R_f, and their values must satisfy the relationship of $k_1+k_2+k_3=1$. The final result obtained and can be determined by referring to the contents in Table 2 and the risk level of each influencing factor can be determined. The user makes a decision on the cloud service according to the determination result.

Table 2. Cloud Security Risk Hierarchy

R	Risk Hierarchy
0-0.2	low
0.2-0.4	relatively low
0.4-0.6	medium
0.6-0.8	relatively high
0.8-1	high

Table 3. The assignment of membership degree matrixes Pc, Pt, and Pf

	bc1	bc2	bc3	bc4	bt1	bt2	bt3	bt4	bf1	bf2	bf3	bf4
a_1	0.15	0.45	0.3	0.1	0.25	0.3	0.3	0.15	0.2	0.25	0.35	0.2
a_2	0.1	0.35	0.4	0.15	0.2	0.35	0.35	0.1	0.25	0.35	0.2	0.2
a_3	0.2	0.35	0.35	0.1	0.25	0.4	0.3	0.05	0.3	0.2	0.4	0.1
a_4	0.15	0.3	0.35	0.2	0.25	0.35	0.4	0	0.2	0.35	0.35	0.1

Calculate the entropy weight coefficient of each factor

The corresponding weight vector of each factor can be obtained from equations 3 and 4:

$$\theta_c=(0.243,0.294,0.322,0.141)$$

$$\theta_t=(0.216,0.273,0.279,0.232)$$

$$\theta_f=(0.198,0.263,0.383,0.152)$$

According to the data in Table 2, we can conclude that the risk of data security is relatively small, and the data on this cloud platform is relatively safe.

Using the same method, we can find other risk values in turn. According to the industry nature of the enterprise and the requirements for security, it is defined that if the risk value is higher than a certain value, it is necessary to consider adopting certain security measures to reduce the risk, so as to obtain the overall cloud platform security.

IV. CONCLUSIONS AND FUTURE WORK

In this paper, cloud security risk assessment index system is built. Based on this, a method of cloud security risk assessment was established by integrating entropy weight and fuzzy theory, and the risk was evaluated quantitatively. Finally, an example analysis of the cloud security risk assessment method was conducted to verify its practicality.

With the development of technology, cloud computing systems are constantly upgraded and changed. In the process, different influencing factors will emerge, and the risk assessment index system will also need to be updated and improved. In the future work, dynamically sense changes in the cloud environment for evaluation can be considered.

REFERENCES

1. Jame McCloskey, Maggie Hao. Saas Security Governance Program. Info-Tech Research Group Publication, October 2, 2015:11-12.
2. Latif R, Abbas H, Assar S, et al. Cloud Computing Risk Assessment: A Systematic Literature Review. Lecture Notes in Electrical Engineering, 2014, 276:285-295.
3. Saad Ullah Khan, Aerospace Avionics. Exploring the Effect of Poletical Risks in Large Infrastructure. Construction and Project Management Faculty of Science and Engineering. 2014, 2 (25): 1-14.
4. Cioffi D F, Khamooshi H A. Practical method of determining project risk contingency budgets. The Journal of the Operational Research Society, 2009, 60(4): 565-571.
5. Sharmila, L. & Sakthi, U. J Supercomput (2018).https://doi.org/10.1007/s11227-018-2340-7.
6. L.Sharmila, U.Sakthi, “Chronological Pattern Exploration Algorithm for Gene Expression Data Clustering and Classification”, Wireless Personal Communications, ISSN 0929-6212 Vol 98, Number 1, January(1) 2018.
7. L.Sharmila, U.Sakthi, “Analysis on Various Search Algorithms”, Global Journal of Pure and Applied Mathematics, ISSN 0973-1768 Volume 12, Number 2 (2016), pp. 1397-1402.
8. L.Sharmila, U.Sakthi, “Search Algorithm for Multiple Histories Using Time-Sorted Array”, Journal of Computational and Theoretical Nanoscience, ISSN 1546-1963Vol. 15 No 9/10, pp .2917–2919, 2018.

AUTHORS PROFILE

L.Sharmila received her B.E., and M.E., Computer Science & Engineering in Anna University, Chennai, India. She is pursuing Ph.D. in the Department of Computer Science & Engineering, Sathyabama University, India. Currently, she is working as a Senior Assistant Professor in the Department of Computer Science & Engineering at Alpha College of Engineering, Chennai, India. Her area of research interest includes the grid computing, data mining and data analytics.

U.Sakthi received her M.E., and Ph.D., in the Department of Computer Science & Engineering from Anna University, Chennai, India. She is currently working as Associate Professor in the Department of Computer Science & Engineering at St.Joseph’s Institute of Technology, Chennai, India. Her research interests include grid computing and mobile computing. She has published many scientific papers in refereed journals and conference proceedings.