

基于改进 VIKOR 法的云计算环境下用户行为安全的评估研究

李存斌 蔺帅帅 徐方秋

(华北电力大学经济与管理学院 北京 102206)

摘要 云计算极大地方便了云端用户对资源的使用,降低了用户为使用存储资源耗费的成本,但也使用户的核心和隐私数据极有可能被非法用户利用,因此对用户行为进行分析评估是有效提升云安全的关键。首先,根据云计算环境下用户行为的特点,建立了评价指标体系;然后,提出了一种基于 AHP-熵权法的改进 VIKOR 法的多属性决策方法,克服了主观赋权法的缺点;最后,以 5 个用户为例进行算例分析,并将所提方法与其他综合评价方法进行了对比分析。结果表明,所提出的方法是科学、有效的,具有一定的优越性。

关键词 云计算,行为安全,VIKOR,排序

中图分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.12.021

Safety Assessment of User Behaviors under Environment of Cloud Computing Based on Improved VIKOR Method

LI Cun-bin LIN Shuai-shuai XU Fang-qiu

(Institute of Economics and Management, North China Electric Power University, Beijing 102206, China)

Abstract Cloud computing brings great convenience and reduces the cost to the cloud users for the use of resources. But it also makes it possible for illegal users to get core and privacy data easily. Therefore, the analysis and evaluation of user behavior is the key to effectively improve the security of the cloud. Firstly, according to the characteristics of user behavior under the environment of cloud computing, the evaluation index system was established. Then, an improved VIKOR method based on AHP-entropy weight method was proposed to overcome the shortcomings of subjective and objective weighting method. Finally, five users was selected for case analysis. Comparative analysis with other comprehensive evaluation methods shows that the proposed method is scientific and effective, and has some advantages.

Keywords Cloud computing, Behavior safety, VIKOR, Ranking

1 引言

云计算^[1]技术不仅方便了云端用户对数据的使用^[2],而且也降低了这些用户的使用成本。但也由此导致他们的核心或者隐私数据很容易被其他用户获取,因此对云计算环境下用户行为安全问题的研究不容小视^[3-4]。

针对云计算环境下的用户行为安全问题,国外学者进行了全面研究。Blaze M^[5]于 1996 年提出了“信任管理”的概念,Abdul-Rahman A 等人在此概念的基础上对信任的内容和程度进行了重新界定,并根据信任的主观性建立了信任评估的数学模型;之后, Beth^[6]为阐述自己构建的信任评估模型,发表了一系列的学术论文。随着云计算以及信任关系的进一步发展,动态的信任评估机制成为了研究热门。在 Shameli-Sendi^[7]提出的框架中采用了几乎完全定量、迭代增量的方法,为客户提供了一种评估和管理风险的思路,并提

出了管理机制;George 等人^[8-9]从有向图的角度出发,构建了动态信任评估模型,利用半球理论来获取最可靠的通信路径,准确识别出了恶意实体;Furuncu E^[10]使用博弈论的思想,提出了一个可扩展的安全风险评估模型作为云计算的解决方案。

国内虽然对信任研究的起步较晚,但是也取得了一定的进展。李小勇教授^[11]提出了一种基于多维决策属性(如激励函数、风险函数等)的信任关系量化模型,该模型利用熵权法计算各属性的权重,因此具有更稳健的动态适应性;Chen H^[12]建议企业合理评估云计算环境下企业的安全风险,确定标准的信息安全风险评估方法和流程,并提出了一个云计算环境下的信息安全风险评估框架;除此之外,吕艳霞^[13]和郭树凯^[14]分别采用三角模糊网络分析法和三角模糊层次分析法对云端用户行为进行了信任评估。

综上所述可知,对用户行为的研究大多都是基于主观分析的,

到稿日期:2016-10-21 返修日期:2017-03-05 本文受国家自然科学基金(71671065, 71271084),国家电网公司总部科技项目:含大规模新能源和高压直流输电的电力系统风险评估研究(5204BB1600CN),中央高校基本科研业务费专项资助资金(2017XS101)资助。

李存斌(1959-),男,教授,博士生导师,主要研究方向为信息管理、风险管理或项目管理;蔺帅帅(1992-),男,博士生,主要研究方向为风险管理、信息管理, E-mail: 18811306733@163.com(通信作者);徐方秋(1992-),女,博士生,主要研究方向为信息管理、能源管理。

还没有专家从主、客观两个方面对用户的行为安全进行评估研究。鉴于此,以上述文献为基础,针对云环境下的用户行为安全问题,提出一种通过 AHP-熵权法计算权重并使用 VIKOR 法^[15]进行评估的数学模型。为了验证该模型的有效性,在算例分析中选取 5 个用户作为研究对象,对其行为进行评估,确定安全大小的排列顺序,并把本文所建立的方法与其他 4 种多属性决策方法进行适用性和性能的比较分析。

2 云计算环境下用户行为安全评估指标体系的建立

云计算环境下用户行为的定义为:在网络环境下,用户为了达到某种特定的目标,与服务商或其他用户进行有意识的活动。对用户行为的研究,最早出现在心理学、社会行为学等学科中,与以上学科中的用户行为相比,云计算环境下的用户行为同样具有规律性和可研究性。研究云计算环境下的用户行为对于云安全具有重要的意义,通过对云计算环境下的用户行为产生的证据进行分析,确定用户行为的信任值,并通过一定的数学方法对用户行为进行信任评估,就可以确定用户行为的安全程度。

根据云计算环境下用户行为的特点,建立评价指标体系,如表 1 所列。

表 1 用户行为安全评价指标体系

一级指标	二级指标	
云计算环境下 用户行为安全 评价指标体系	可靠性	用户平均运行威胁程序次数 C_1 用户 IP 平均异常率 C_2 用户平均携带病毒数 C_3 用户平均登陆服务器异常率 C_4
	安全性	用户非法连接次数 C_5 用户平均扫描重要端口次数 C_6 用户平均尝试非法越权次数 C_7 用户攻击其他用户次数 C_8

3 基于改进 VIKOR 法的云计算环境下用户行为安全评估模型的构建

问题描述:对于某多属性决策问题 $Q = \{M, C, W, D\}$, 其中 $M = \{M_i\} (i = 1, 2, \dots, m)$ 为方案集, $C = \{C_j\} (j = 1, 2, \dots, n)$ 为指标集, $W = (\omega_1, \omega_2, \dots, \omega_n)$ 为指标权重集, $D = \{d_{ij}\}$ 为指标属性值矩阵, d_{ij} 表示第 i 个方案下第 j 个指标的指标值。现拟通过本文建立的算法选出最优的方案,算法的具体步骤如下。

3.1 建立评价指标体系

指标体系的建立在第 2 节已经做了说明,如表 1 所列。

3.2 确定指标权重

AHP 法^[16]是根据决策者的主观思想来确定权重的一种方法。该方法并不能完全反映实际数据中的信息,而熵权法^[17]则正好相反。因此本文将这两种方法进行结合,以弥补它们各自的不足,具体方法如图 1 所示。



图 1 主观与客观综合赋权方法的原理

(1) AHP 法确定指标权重的步骤

根据 AHP 经典模型,云计算环境下用户行为安全评价指标权重的计算步骤如下:

1) 构建指标重要度对比矩阵,并计算出最大特征值和特征向量,然后经过一致性检验来确定各个评价指标的权重向量 X 。

2) 由权重向量 X 得到指标权重矩阵 C :

$$C = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{bmatrix}$$

3) 根据式(1)获得各专家针对云计算环境下用户安全行为评价指标权重向量的相关系数矩阵 D :

$$d_{ij} = 1 - \sqrt{\frac{1}{n} \sum_{k=1}^n (c_{ik} - c_{jk})^2}, i, j = 1, 2, \dots, m \quad (1)$$

$$D = \begin{bmatrix} 1 & d_{12} & \dots & d_{1m} \\ d_{21} & 1 & \dots & d_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ d_{m1} & d_{m2} & \dots & 1 \end{bmatrix}$$

其中, $d_{ii} = 1, d_{ij} = d_{ji}$ 。

4) 根据式(2)淘汰偏离程度大的专家,淘汰比例如表 2 所列。

$$d_i = \sum_{j=1}^m d_{ij} \quad (2)$$

其中, d_i 表示专家权重的偏离程度, d_i 越大,该专家与其他专家的偏离程度越小。

表 2 专家人数及对应淘汰比例

聘请专家人数	5	6	7	8	9
聚类分析淘汰人数	1	1~2	1~2	2	2~3
意见被采用的专家人数	4	4~5	5~6	6	6~7

5) 求取筛选后的权重矩阵列向量的平均值 $\omega_j^a (j = 1, 2, \dots, n)$, 即为每个评价指标的权重值。

(2) 熵权法确定评价指标权重的步骤

1) 设初始评价矩阵为 $X = [x_{ij}]_{y \times n}$, 将矩阵 X 进行标准化处理,得到 $B = [b_{ij}]_{y \times n}$, 标准化公式如下:

$$b_{ij} = \frac{x_{ij} - x_{\min}}{x_{\max} - x_{\min}}$$

其中, x_{\max}, x_{\min} 分别为同一指标下的最大值和最小值。

2) 对于 y 个评价数列和 n 个评价指标的评价问题,根据熵的定义,可得评价指标的熵 H_j :

$$H_j = -\frac{1}{\ln y} \left(\sum_{i=1}^y f_{ij} \ln f_{ij} \right) \quad (3)$$

其中, $f_{ij} = \frac{b_{ij} + 1}{\sum_{i=1}^y (b_{ij} + 1)}$

3) 评价指标的权重值为:

$$\omega_j^b = \frac{1 - H_j}{n - \sum_{j=1}^n H_j}, j = 1, 2, \dots, n \quad (4)$$

(3) 熵权法对 AHP 法的修正

为了将 AHP 法和熵权法进行结合,引入熵值变量,确定出最终的权重值为:

$$w_j = w_j^a H_j + w_j^b (1 - H_j), j = 1, 2, \dots, n \quad (5)$$

经推理可知: $\sum_{j=1}^n w_j = 1$ 。式(5)中, w_j^a 为 AHP 法所确定的权重值, w_j^b 为熵权法确定的权重值。

最终得出的权重值应符合如下两个性质:

性质 1 最终所确定的权重应在两种方法确定的权重之间。

性质 2 熵值 H_j 偏大($H_j > 0.5$)时, w_j 离 w_j^a 较近;熵值 H_j 值偏小($H_j < 0.5$)时, w_j 离 w_j^b 较近。

通过以上方法,得到各指标的最终权重 w_j 。

3.3 求解正理想解和负理想解

这里的评价矩阵选取规范化之后的数据,使得各个评价值之间的联系程度更加凸显,评价结果更加准确。正、负理想解的计算公式如式(6)和式(7)所示。

$$f^+ = \{ \max_i d_{i1}^+, \max_i d_{i2}^+, \dots, \max_i d_{in}^+ \} \quad (6)$$

$$f^- = \{ \min_i d_{i1}^-, \min_i d_{i2}^-, \dots, \min_i d_{in}^- \} \quad (7)$$

其中, f^+ 和 f^- 分别是正、负理想解。

3.4 计算 S_i 的值和 R_i 的值

S_i 和 R_i 分别为有限决策方案的群体效益和最大个别遗憾。

$$S_i = \sum_{j=1}^m w_j \frac{f_i^+ - f_{ij}}{f_i^+ - f_j^-} \quad (8)$$

$$R_i = \max_j \{ w_j \frac{f_i^+ - f_{ij}}{f_i^+ - f_j^-} \} \quad (9)$$

其中, w_j 是各个指标的最终权重,这里采用 AHP 和熵权法相结合的方法确定出的综合权重表示。

3.5 计算 Q_i 的值

$$Q_i = v \frac{S_i - S^*}{S^- - S^*} + (1 - v) \frac{R_i - R^*}{R^- - R^*} \quad (10)$$

其中, $S^* = \min_i \{ S_i \}$, $S^- = \max_i \{ S_i \}$, $R^* = \min_i \{ R_i \}$, $R^- = \max_i \{ R_i \}$ 。 v 为最大化群体效益的决策机制系数, $1 - v$ 为最小化个体损失的决策机制系数。 $v > 0.5$ 表示决策结果是由大多数人的意见制定; $v = 0.5$ 表示决策结果是由大多数比较好的评价和少数较差的评价制定; $v < 0.5$ 表示决策结果是根据少数较差的评价得出的,本文取 $v = 0.5$ 。

3.6 对决策方案进行排序并选出理想方案

依据 Q_i 值从小到大对方案进行排序,假设得到的排序第 1 的方案和第 2 的方案分别为 M_1 和 M_2 。

条件 1(可接受度优势) 排在第 1 位的方案和排在第 2 位的方案之间的差异能被决策者充分接受,可表示为 $Q_1 - Q_2 \geq 1/(m-1)$,其中 m 为方案数目。

条件 2(决策过程中可接受的稳定性) 方案 M_1 的 S_i 或

$$C = \begin{matrix} \begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{matrix} \\ \end{matrix} = \begin{bmatrix} 0.3377 & 0.0283 & 0.1170 & 0.0494 & 0.1152 & 0.0431 & 0.0757 & 0.2336 \\ 0.3223 & 0.0272 & 0.1210 & 0.0591 & 0.1058 & 0.0411 & 0.0756 & 0.2479 \\ 0.3495 & 0.0271 & 0.1339 & 0.0638 & 0.1019 & 0.0409 & 0.0753 & 0.2076 \\ 0.3494 & 0.0277 & 0.1397 & 0.0558 & 0.1084 & 0.0367 & 0.0793 & 0.2029 \\ 0.3650 & 0.0281 & 0.1350 & 0.0699 & 0.1174 & 0.0386 & 0.0798 & 0.1662 \\ 0.3585 & 0.0277 & 0.1241 & 0.0739 & 0.1079 & 0.0378 & 0.0804 & 0.1896 \end{bmatrix}$$

根据式(1)可计算得出云计算环境下用户行为安全评价

R_i 同样排在第 1 位。

判断准则有如下两点。

判断准则 1 若同时满足条件 1 与条件 2,则方案 M_1 为排序第 1 的方案。

判断准则 2 如果上述条件其中一个不满足,则:若不满足条件 1,则一直到找到排序第 i 的方案值满足 $Q_i - Q_{i-1} \geq 1/(m-1)$ 为止,其中 $i \in \{3, 4, \dots, m\}$,此时排序第 1 到第 i 的方案均为理想方案;若不满足条件 2,则 M_1 和 M_2 均为理想方案。

4 算例分析

本文采取文献[18]中列举的方法作为用户行为证据的获取方式,即利用已有的入侵检测软件——萨客嘶入侵检测系统与专家意见及推理等方法相结合,获取用户行为证据的子证据基础数据。因为本文研究的重点是云计算环境下用户行为安全的评估,所以没有对如何获取用户行为做具体的研究。

仍然采用文献[18]中获取到的 5 个用户的数据对本文提出的方法进行验证。具体的数据如表 3 所列。

表 3 规范化数据表

	用户 1	用户 2	用户 3	用户 4	用户 5
C_1	0.4286	0.2858	1.0000	0.0000	0.7143
C_2	0.6667	0.3333	1.0000	0.0000	0.6667
C_3	0.7692	0.0000	0.8462	0.2308	1.0000
C_4	0.3333	0.6667	1.0000	0.3333	0.0000
C_5	0.6667	0.5556	1.0000	0.0000	0.7778
C_6	0.4286	0.4286	1.0000	0.0000	0.7146
C_7	0.4286	0.0000	0.4286	0.1429	1.0000
C_8	0.6667	0.3333	1.0000	0.0000	0.8333

(1)首先采用 AHP-熵权法确定指标权重

为使评价结果科学、客观,邀请 6 位专家进行打分。由于篇幅限制,下面仅给出专家 1 打分的相对重要性矩阵。

$$\begin{bmatrix} 1 & 8 & 4 & 6 & 3 & 7 & 5 & 2 \\ 1/8 & 1 & 1/4 & 1/3 & 1/4 & 1/2 & 1/3 & 1/6 \\ 1/4 & 4 & 1 & 3 & 1 & 3 & 2 & 1/2 \\ 1/6 & 3 & 1/3 & 1 & 1/2 & 1 & 1/3 & 1/6 \\ 1/3 & 4 & 1 & 2 & 1 & 3 & 2 & 1/2 \\ 1/7 & 2 & 1/3 & 1 & 1/3 & 1 & 1/2 & 1/6 \\ 1/5 & 3 & 1/2 & 3 & 1/2 & 2 & 1 & 1/2 \\ 1/2 & 6 & 2 & 6 & 2 & 6 & 5 & 1 \end{bmatrix}$$

获得重要度对比矩阵后,可获得各矩阵的最大特征值与特征向量,并进行一致性检验。6 个矩阵的 CR 依次为 (0.0283, 0.0885, 0.0945, 0.0960, 0.0955, 0.0901),均小于 0.1,满足一致性检验。

各专家的权重向量为 x_i ,向量 x_i 组成权重矩阵 C :

指标权重向量的相关系数矩阵 D :

$$D = \begin{bmatrix} 1.0000 & 0.9910 & 0.9268 & 0.9852 & 0.9725 & 0.9802 \\ 0.9910 & 1.0000 & 0.9821 & 0.9801 & 0.9665 & 0.9751 \\ 0.9268 & 0.9821 & 1.0000 & 0.9951 & 0.9832 & 0.9908 \\ 0.9852 & 0.9801 & 0.9951 & 1.0000 & 0.9846 & 0.9898 \\ 0.9725 & 0.9665 & 0.9832 & 0.9846 & 1.0000 & 0.9899 \\ 0.9802 & 0.9751 & 0.9908 & 0.9898 & 0.9899 & 1.0000 \end{bmatrix}$$

$$C' = \begin{cases} x_1 \\ x_2 \\ x_4 \\ x_5 \\ x_6 \end{cases} = \begin{bmatrix} 0.3223 & 0.0272 & 0.1210 & 0.0591 & 0.1058 & 0.0411 & 0.0756 & 0.2479 \\ 0.3495 & 0.0271 & 0.1339 & 0.0638 & 0.1019 & 0.0409 & 0.0753 & 0.2076 \\ 0.3494 & 0.0277 & 0.1397 & 0.0558 & 0.1084 & 0.0367 & 0.0793 & 0.2029 \\ 0.3650 & 0.0281 & 0.1350 & 0.0699 & 0.1174 & 0.0386 & 0.0798 & 0.1662 \\ 0.3585 & 0.0277 & 0.1241 & 0.0739 & 0.1079 & 0.0378 & 0.0804 & 0.1896 \end{bmatrix}$$

根据式(3)和式(4),利用表3的数据可以确定出熵权法的指标权重。然后利用式(5)对两种方法确定的权重进行修正,从而得出最终的评价指标权重值,如表4所列。指标权重值的折线图如图2所示。

表4 3种方法确定的权重值

	AHP法	熵权法	修正法
C_1	0.3489	0.1173	0.2245
C_2	0.0276	0.123	0.0814
C_3	0.1307	0.1467	0.1415
C_4	0.0645	0.113	0.0897
C_5	0.1083	0.135	0.1249
C_6	0.039	0.1168	0.0807
C_7	0.0781	0.1128	0.0961
C_8	0.2029	0.1354	0.1611

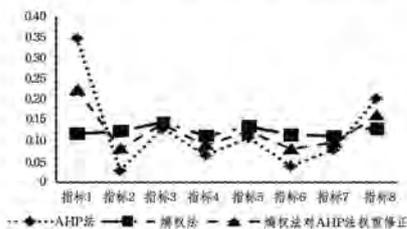


图2 3种方法确定的权重值

分析表4和图2可得,熵权法对AHP法修正得出的权重值介于AHP法和熵权法确定的权重之间,满足性质1;由表3计算可得熵值 $H_j > 0.5$, w_j 离 w_j^0 较近,满足性质2。

(2) 选取正、负理想解

因为所有的指标均为成本型指标,所以根据表3可以得出正理想解为 $\{0, 0, \dots, 0\}$, 负理想解为 $\{1, 1, \dots, 1\}$ 。

(3) 求解 S_i, R_i 和 Q_i 的值

由式(8)一式(10)得出 S_i, R_i 和 Q_i 的值,如表5所列。

表5 S_i, R_i 和 Q_i 的值

方案	S_i	R_i	Q_i
M_1	0.99	0.17	0.61
M_2	0.58	0.15	0.39
M_3	1.63	0.22	1
M_4	0.16	0.07	0
M_5	1.28	0.22	0.88

(4) 对方案进行排序

根据VIKOR方法的排序规则,可以得出用户4的安全风险最小,即 M_1 为理想方案。同理可得 $M_2 > M_1 > M_3 > M_5$ 。因此,最终方案的排列顺序为 $M_1 > M_2 > M_1 > M_5 > M_3$ 。

由相关系数矩阵 D ,并根据式(2)计算出权重意见相似程度之和 $d_i: d_1=5.8557, d_2=5.8948, d_3=5.8779, d_4=5.9349, d_5=5.8967, d_6=5.9258$ 。

根据专家人数及对应淘汰比例表,最终淘汰专家3的权重值。

新的权重矩阵为 C' ,权重向量的平均值即为AHP法确定的各指标的权重值,如下所示。

5 方案结果的对比分析

为了验证该方法的有效性,本文考虑将其与其他决策方法进行对比,如TOPSIS(Technique for Order Preference by Similarity to an Ideal Solution)法^[19]、灰色关联分析法、灰色前景理论^[20]和模糊综合评价法^[21]。TOPSIS法是一种应用最为广泛的多属性决策方法,它通过检测评价对象与最优解、最劣解的距离,用贴近度来对所有的方案进行排序;灰色关联分析法通过灰色关联度对指标的贡献测度大小进行描述;而灰色前景理论将灰关联分析法融入到前景理论中以构建正、负前景价值矩阵,进而根据各方案综合前景值的大小确定方案的排序;模糊综合评价法根据模糊数学的隶属度理论把定性评价转化为定量评价,即用模糊数学对受到多种因素制约的事物或对象做出一个总体的评价。5种方法得出的方案值大小和排序结果如表6所列。

表6 各方案的对比分析结果

方法	M_1	M_2	M_3	M_4	M_5	排序
本文方法	0.61	0.39	1	0	0.88	$M_1 > M_2 > M_1 > M_5 > M_3$
TOPSIS法	0.54	0.36	0.82	0.14	0.65	$M_1 > M_2 > M_1 > M_5 > M_3$
模糊综合评价	0.23	0.32	0.15	0.77	0	$M_4 > M_2 > M_1 > M_3 > M_5$
灰色关联分析	0.48	0.57	0.39	0.82	0.4	$M_4 > M_2 > M_1 > M_5 > M_3$
灰色前景理论	-1.1	-0.29	-2.15	0.68	-1.5	$M_1 > M_2 > M_1 > M_5 > M_3$

其中,TOPSIS法用与正理想方案的贴近度表示,指标值越小方案越优;灰色关联分析法用灰色关联度表示,指标值越大方案越优;模糊综合评价法采用综合评价值表示,评价值越大方案越优;灰色前景理论用综合前景值表示,前景值越大方案越优。

由表6可知,方案4始终是最优方案,并且除了模糊综合评价法在方案3和方案5的排序上出现偏差之外,所有方案的排序均相同,这证明了所提方案的有效性与合理性。

与其他4种方案相比,本文所建立的决策方法的优势如下。

(1)与TOPSIS法对比。以具有两个属性的多准则决策问题为例来进行说明,用TOPSIS法进行求解时,只要当各方案均落在以两准则为横纵坐标的对角线上各方案就具有相同的贴近度。但实际上,TOPSIS法并不能实际反映出各方案与理想方案的贴近度,即无法分出何者较佳。相反,VIKOR法通过最佳化妥协提出了一个新的准则加总的方法,该方法同时考虑了各方案与理想方案和负理想方案的贴近,因此,VIKOR法所得的妥协解即为最佳方案。

如表 6 所列,一般意义上来说,用 TOPSIS 方法得出的方案评价价值之间的相对差异较小,即方案的评价分布比较密集,而过度精确的排序会导致排序结果出现逆序,所以其得到的最终结果并不一定是最优解。因此,当决策方案的数量比较大时,VIKOR 方法会表现出更大的优势。

(2)与模糊综合评价法对比。使用模糊综合评价法进行评价时,指标的权重通常是人为确定的,这就使得评价结果具有很强的主观随意色彩,并且该方法不能解决因素间相关性所造成的评价信息重复问题。而本文所提方法从主客观两个方面对指标的权重进行了分析,使得评价结果更加准确。除此之外,模糊综合评价法也没能解决各个方案值的得分差距较小的问题,因此会使得排序出现偏差,如方案 3 与方案 5 出现的顺序相反的情况。

(3)与灰色关联分析法对比。与本文所提出的方法相比,灰色关联分析法的主观性过强,且各方案的决策值差距较小。如表 6 所列,最大值与最小值的差距为 0.43,且方案 3 和方案 5 之间仅相差 0.01,当决策方案的数量增加时,不利于决策者做出更加合理的判断。

(4)与灰色前景理论对比。虽然前景理论得出的方案值之间的差距大于本文所建立的方法,但是,前景理论是从心理学的角度对问题进行分析,与 VIKOR 法相比,缺乏一个明确的理想方案参考点,具有一定的空洞性;并且作为一个描述性模型,它缺乏严格的理论基础和数学推导。因而,它得出的评价结果在某种程度上也不如 VIKOR 法得出的评价结果客观。

结束语 文章首先介绍了云计算和用户行为的一些相关概念。在此基础上,从可靠性和安全性两个方面构建了云计算环境下用户行为安全评价的指标体系。为了弥补主客观赋权法各自存在的缺点,采用 AHP-熵权法的组合赋权法对用户行为的权重进行了计算。然后利用 VIKOR 法对 5 个用户的安全行为进行了评估排序。算例以及各个决策方法之间的对比分析也证明了本方法的可行性和有效性,因此本方法为决策者提供了一种新思路。

同时,为了维护云计算环境下的网络安全,根据评价的结果,可以适当地对各个用户制定相应的奖惩机制。例如,用户 2 的网络行为较安全,可以对其进行宽带提速或是增加流量,从一定意义上鼓励这样的用户行为;反之,用户 3 的网络行为的侵害性较大,因此可以考虑采取对其进行限速或者禁止其对一些域名的访问等措施来提高其网络行为的安全。本文只是对用户的安全行为进行了评估排序并提出了一些简单的奖惩机制,具体可行的相关机制还需有关部门进行制定,这也是下一阶段要研究的内容。

参 考 文 献

[1] CHANG V, WALTERS R J, WILLS G B. Organisational sustainability modelling An emerging service and analytics model for evaluating Cloud Computing adoption with two case studies [J]. International Journal of Information Management, 2016, 36(1):167-179.

[2] JERMAIN C L, ROWLANDS G E, BUHRMAN R A. GPU-ac-

celerated micromagnetic simulations using cloud computing [J]. Journal of Magnetism and Magnetic Materials, 2016, 401(1): 320-322.

[3] WANG D W. Basic Framework and Key Technology for a New Generation of Data Center in Electric Power Corporation Based on Cloud Computation [J]. Automation of Electric Power System, 2012, 36(11):15-19. (in Chinese)
王德文. 基于云计算的电力数据中心基础架构及其关键技术 [J]. 电力系统自动化, 2012, 36(11):15-19.

[4] YANG S L, LUO H, DING S. Survey on multi-sources information service system based on cloud computing [J]. Journal of Management Science in China, 2012, 15(5):83-96. (in Chinese)
杨善林, 罗贺, 丁帅. 基于云计算的多源信息服务系统研究综述 [J]. 管理科学学报, 2012, 15(5):83-96.

[5] BETH T, BORCHERDING M, KLEINlein B. Valuation of trust in open networks [M]// Computer Security-ESORICS' 94. Springer Berlin Heidelberg, 1994:3-18.

[6] JOSANG A. The right type of trust for distributed systems [C]// Proceedings of the Workshop on New Security Paradigms, Lake Arrowhead, Ca, United States, 1996:119-131.

[7] SHAMELI-SENDI A, CHERIET M. Cloud Computing: A Risk Assessment Model [C]// 2014 IEEE International Conference on Cloud Engineering. 2014:147-152.

[8] THEODORAKOPOULOS G. Distributed trust evaluation in ad-hoc networks [D]. Maryland: University of Maryland, 2004.

[9] THEODORAKOPOULOS G, BARAS J S. On trust models and trust evaluation metrics for adhoc networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):318-328.

[10] FURUNCU E, SOGUKPINAR I. Scalable risk assessment method for cloud computing using game theory (CCRAM) [J]. Computer Standards & Interfaces, 2015, 38(2):44-50.

[11] LI X Y, GUI X L. Trust Quantitative Model with Multiple Decision Factors in Trusted Network [J]. Chinese Journal of Computers, 2009, 32(3):405-416. (in Chinese)
李小勇, 桂小林. 可信网络中基于多维决策属性的信任量化模型 [J]. 计算机学报, 2009, 32(3):405-416.

[12] CHEN H. An Information Security Risk Assessment Framework For Cloud Computing [J]. Advanced Materials Research, 2013, 756-759:1469-1473.

[13] LV Y X, TIAN L Q, SUN S S. Trust Evaluation and Control Analysis of FANP-based User Behavior in Cloud Computing Environment [J]. Computer Science, 2013, 40(1):132-135. (in Chinese)
吕艳霞, 田立勤, 孙珊珊. 云计算环境下基于 FANP 的用户行为的可信评估与控制分析 [J]. 计算机科学, 2013, 40(1):132-135.

[14] GUO S K, TIAN L Q, SHEN X L. Research on FAHP method in user behaviour trust computation [J]. Computer Engineering and Applications, 2011, 47(12):59-61. (in Chinese)
郭树凯, 田立勤, 沈学利. FAHP 在用户行为信任评价中的研究 [J]. 计算机工程与应用, 2011, 47(12):59-61.

[15] SUO W L. Method for uncertain linguistic multiple attribute group decision making based on extended VIKOR [J]. Control and Decision, 2013, 28(9):1431-1440. (in Chinese)

种混沌不透明表达式的构造方法,并通过统计与分析验证了该构造方法具有较高的构造效率。随后基于混沌不透明表达式提出了一种新的不透明谓词构造方法和不透明谓词插入方法,增强了不透明谓词的安全性,并通过实验验证了该技术在各项软件复杂度指标中都有明显的提升,同时给程序增加的代价开销较小。未来将继续研究混沌不透明表达式中关于混沌映射以及二次映射的最优构造方案。

参 考 文 献

- [1] PREDA M D, GIACOBACCI R. Control Code Obfuscation by Abstract Interpretation[C]//IEEE International Conference on Software Engineering and Formal Methods. IEEE Xplore, 2005: 301-310.
- [2] ZHAO Y J, TANG Z Y, WANG I. Evaluation of code obfuscating Transformation[J]. Journal of Software, 2012, 23(3): 700-711.
- [3] COLLBERG C, THOMBORSON C D. Low manufacturing cheap, resilient, and stealthy opaque constructs[C]//Proceeding of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. California: ACM, 1998: 184-196.
- [4] ARBOIT G. A method for watermarking java programs via opaque predicates[C]//The Fifth International Conference on Electronic Commerce Research (ICECR-5). 2002: 102-110.
- [5] MYLES G, COLLBERG C. Software watermarking via opaque predicates: implementation, analysis, and attacks[J]. Electron Commerce Research, 2006, 4(6): 155-171.
- [6] YUAN Z, WEN Q, MAO M. Constructing Opaque Predicates for Java Programs[C]//2006 International Conference on Computational Intelligence and Security. 2006: 895-898.
- [7] SU Q, WU W M, LI Z L, et al. Research and Application of Chaos Opaque Predicate in Code Obfuscation[J]. Computer Science, 2013, 40(6): 155-160.
- [8] XIE X, LIU F, LU B, et al. Mixed Obfuscation of Overlapping Instruction and Self-Modify Code Based on Hyper-Chaotic Opaque Predicates[C]//Tenth International Conference on Computational Intelligence and Security. IEEE Computer Society, 2014: 524-528.
- [9] WANG C X. A security architecture for survivability mechanisms[D]. Charlottesville: University of Virginia, 2001.
- [10] COLLBERG C, NAGRA J. Surreptitious Software Obfuscation, Watermarking, and Tamperproofing for Software Protection[M]. Beijing: Post & Telecom Press, 2012: 204-205.
- [11] MOSER A, KRUEGEL C, KIRDA E. Limits of Static Analysis for Malware Detection[C]//Computer Security Applications Conference, 2007. IEEE, 2007: 421-430.
- [12] WU W M, LIN S M, LIN Z Y. chaotic-based opaque predicate control flow flatten algorithm[J]. Computer Science, 2015, 42(5): 178-182.
- [13] GONZALOALVAREZ, SHUJUNLI. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems[J]. International Journal of Bifurcation & Chaos, 2006, 16(8): 2129-2151.
- [14] YUAN G N, QIN H L, LAI D S. Construct of Tent Map Stream Cipher on Square[J]. Computer Engineering and Applications, 2002, 38(13): 124-126.
- [15] SCHUMACKER R, TOMER S. Understanding Statistics Using R[M]. Springer Publishing Company, Incorporated, 2013.
- [16] COLLBERG C. A Tool for the Study of Software Protection Algorithms[EB/OL]. <http://sandmark.cs.arizona.edu>.
- (上接第 109 页)
- 索玮岚. 基于扩展 VIKOR 的不确定语言多属性群决策方法[J]. 控制与决策, 2013, 28(9): 1431-1440.
- [16] ZHANG S, WANG T, GU X P. Synthetic Evaluation of Power Grid Operating States Based on Intuitionistic Fuzzy Analytic Hierarchy Process[J]. Automation of Electric Power System, 2016(4): 41-49. (in Chinese)
- 张尚, 王涛, 顾雪平. 基于直觉模糊层次分析法的电网运行状态综合评估[J]. 电力系统自动化, 2016(4): 41-49.
- [17] XIE M, DENG J L, LIU M B, et al. Temperature-lowering Load Estimation Method Based on Meteorological Data and Entropy Weight Theory[J]. Automation of Electric Power System, 2016(3): 135-139. (in Chinese)
- 谢敏, 邓佳梁, 刘明波, 等. 基于气象信息和熵权理论的降温负荷估算方法[J]. 电力系统自动化, 2016(3): 135-139.
- [18] WANG C. Trust Evaluation Based on User's Behavior in Cloud Computing[D]. Baotou: Inner Mongolia University of Science & Technology, 2015. (in Chinese)
- 王超. 云计算环境下基于用户行为的信任评估研究[D]. 包头: 内蒙古科技大学, 2015.
- [19] LOURENZUTTI R, KROHLING R A. A generalized TOPSIS method for group decision making with heterogeneous information in a dynamic environment[J]. Information Sciences, 2016, 330: 1-18.
- [20] LI C B, YUAN J H, QI Z Q. Investment Risk-Based Decision of Distributed Generation Based on Grey Cumulative Prospect Theory[J]. East China Electric Power, 2014, 42(5): 993-998. (in Chinese)
- 李存斌, 苑嘉航, 祁之强. 基于灰色累积前景理论分布式电源投资风险型决策[J]. 华东电力, 2014, 42(5): 993-998.
- [21] XU W H, CHEN H Y, ZHANG Y P, et al. Fuzzy Comprehensive Evaluation Method Based on Measure of Medium Truth Degree[J]. Computer Science, 2016, 43(2): 204-209. (in Chinese)
- 徐文华, 陈海燕, 张育平, 等. 一种基于中介真值程度度量的模糊综合评价方法[J]. 计算机科学, 2016, 43(2): 204-209.