

基于 FANP 的云用户行为信任评估优化机制

张艺¹, 田立勤^{1,2}, 毋泽南², 武文星¹

(1. 华北科技学院计算机学院, 北京 101601; 2. 青海师范大学计算机学院, 青海 西宁 810000)

摘 要: 开放的云计算环境面临着安全挑战, 传统的用户行为评估机制已经无法保障云端的安全性。为科学量化评估用户的行为信任, 确保权重赋值科学合理, 提高云平台下用户行为的安全可信度, 设计出一种结合模糊网络分析法的信任评估优化机制。将模型中用户行为信任评估一个控制目标扩展为历史访问行为与当前访问环境两个控制目标模块, 同时将历史访问行为模块划分为常规行为与灰色行为两个方面, 将当前访问环境模块划分为信息完整性与访问安全性两个方面。在不同的控制目标下划分相对应的控制准则, 从而构造不同控制目标下的网络分析模型, 借助网络层次分析法软件计算各个目标模块下的极限超矩阵从而获取各个元素最终的稳定权重。选取开发平台下的真实用户行为数据来综合计算出不同模块下的信任度作为最终的行为评估结果。用户行为评估模块的扩展细化了评估粒度使评估结果的客观性更强, 准确性更高。实验结果表明, 与传统的用户行为信任评估模型相比, 在相同恶意比率的云环境下, 所提优化机制对恶意用户具有更好的识别效果, 能够更早更快地识别出信任度低的云用户, 从而提高了云端的安全性与合法性, 同时为云环境下解决用户的安全可信问题以及进行有效的风险控制方面提供了新的研究思路。

关键词: 云计算; 用户行为; 模糊网络分析法; 信任度

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2021100

Trust evaluation optimization mechanism for cloud user behavior based on FANP

ZHANG Yi¹, TIAN Liqin^{1,2}, WU Zenan², WU Wenxing¹

1. School of Computer, North China Institute of Science and Technology, Beijing 101601, China

2. School of Computer, Qinghai Normal University, Xining 810000, China

Abstract: The open cloud computing environment is facing security challenges and the traditional user behavior

收稿日期: 2021-08-20; 修回日期: 2021-10-13

通信作者: 田立勤, tianliqin@ncist.edu.cn

基金项目: 国家重点研发计划(2018YFC0808306); 河北省重点研发计划(19270318D); 河北省物联网监控工程技术研究中心(3142018055); 青海省物联网重点实验室(2017-ZJ-Y21)

Foundation Items: The National key R&D Program of China (2018YFC0808306), Key Research and Development Projects in Hebei Province(19270318D), Internet of things Monitoring Engineering Technology Research Center of Hebei Province(3142018055), Key Laboratory of Internet of Things of Qinghai Province(2017-ZJ-Y21)

引用格式: 张艺, 田立勤, 毋泽南, 等. 基于 FANP 的云用户行为信任评估优化机制[J]. 网络与信息安全学报, 2022, 8(2): 175-182.

Citation Format: ZHANG Y, TIAN L Q, WU Z N, et al. Trust evaluation optimization mechanism for cloud user behavior based on FANP[J]. Chinese Journal of Network and Information Security, 2022, 8(2): 175-182.

evaluation mechanism cannot guarantee the security of the cloud. In order to scientifically and quantitatively evaluate the user's behavior trust, ensure the scientific and reasonable weight assignment, improve the security and credibility of user behavior under the cloud platform, a trust evaluation optimization mechanism combined with fuzzy analytic network process (FANP) was designed. In the proposal, user behavior trust evaluation based on one control target was extended to include two control target modules which were historical access behavior and current access environment. At the same time, the historical access behavior module was divided into two aspects: conventional behavior and gray behavior, and the current access environment module was divided into two directions: information integrity and access security. The corresponding control criteria was divided to construct the analytic network process (ANP) model under different control objectives. The limit hypermatrix under each target module was calculated to obtain the final stability weight of each element with the help of network analytic hierarchy process software. And the real user behavior data under the development platform was selected to comprehensively calculate the trust degree under different modules as the final behavior evaluation result. The expansion of the user behavior evaluation module refined the evaluation granularity, which makes the evaluation results more objective and accurate. In the cloud environment with the same malicious ratio, the optimization mechanism has better recognition effect, and it can identify cloud users with low trust efficiently and effectively, so as to improve the security and legitimacy of the cloud. At the same time, it also provides new research direction for solving the problem of user security and credibility, and effective risk control in the cloud environment.

Keywords: cloud computing, user behavior, fuzzy analytic network process, degree of trust

0 引言

在信息技术迅速发展的时代下,云计算的广泛运用给用户带来诸多服务和网络资源的同时,显现出一系列的网络安全问题。云环境下的用户规模日益扩大,用户行为变得越来越复杂^[1]。对于云安全来说,仅凭身份认证技术的成熟已无法保证云计算环境的信息安全^[2]。云安全中的信任、稳定等特性都被视为需要攻克的难点^[3]。针对用户行为的信任评估是解决云环境中安全问题的核心技术^[5],也是当今网络时代下云计算研究中的一个重要方向^[6]。

信任在理论上是一种社会学,通常情况下人与人之间的相互联系被视为实体之间或者机器之间的交互,因此信任被引入计算机范畴内^[6-7]。用户行为信任评估方面取得了研究成果。毋泽南等^[8]运用机器学习的方法让计算机对用户的历史行为证据进行学习生成信任评估模型。王超等^[5]提出了基于相对熵的组合赋权法(RE-CWA, relative entropy-combined weighting approach)来确定用户行为权重的贴适度,进而对用户信用度进行了模糊综合评价,构建了适用于云环境的信任评估模型。Huang等^[9]采用加权主观逻辑对系

统中的信任值进行更新从而提出了一种分布式声誉管理方法。谢晓兰等^[10]在用户行为数据的基础上,结合马尔可夫链与层次分析法提出了新的可信度计算方法来提高云端的安全性。胡园园等^[11]在模糊层次分析法的基础上进行改进,采用网络层次分析法构建知识链动态信任评价体系,为知识链企业中的信任评估环节提供了新的思路。

本文在以上研究成果的基础上,提出了云环境下基于模糊网络分析法(FANP, fuzzy analytic network process)的信任评估优化机制。该机制从历史访问行为与当前访问环境两方面扩展用户行为信任评估模块,采用模糊网络分析法构造不同模块下的网络分析法模型进而计算出稳定的行为证据权重,将其与处理好的初始证据矩阵相结合获取用户在不同控制目标模块下的信任度。该优化机制一方面弱化了传统信任评估的主观性,另一方面评估模块的扩展细化了评估粒度,使决策结果的客观性更强。

1 基于 FANP 的云用户行为信任评估

1.1 用户行为的 ANP 评估模型

本文将用户行为信任的一个控制目标扩展为

云用户的历史访问行为与访问环境两个控制目标模块，对不同的模块构建相对应的网络层次分析模型，分别如图 1 和图 2 所示。每个 ANP 结构包含控制层与网络层两个层次。在网络层中包含控制目标与准则，如在图 1 历史访问行为的 ANP 结构中，控制目标为云用户的历史访问行为，准则从常规行为与灰色行为两个角度来构建。所有受控制层支配的元素构成网络层^[12]，各个元素之间都是相互关联的，如用户密码的错误次数越多，用户的登录次数就会越少。

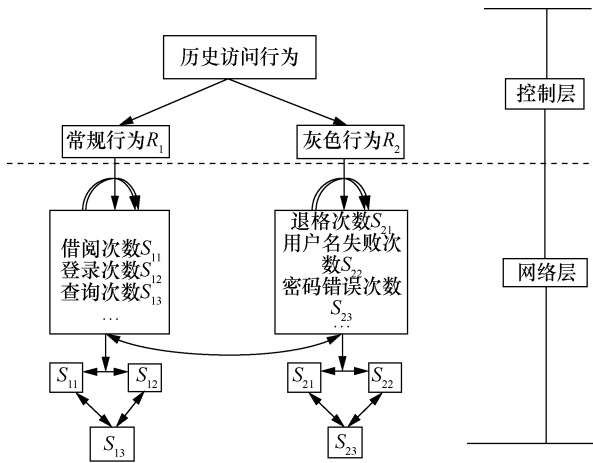


图 1 云用户历史访问行为的 ANP 结构
Figure 1 ANP structure of historical access behavior of cloud

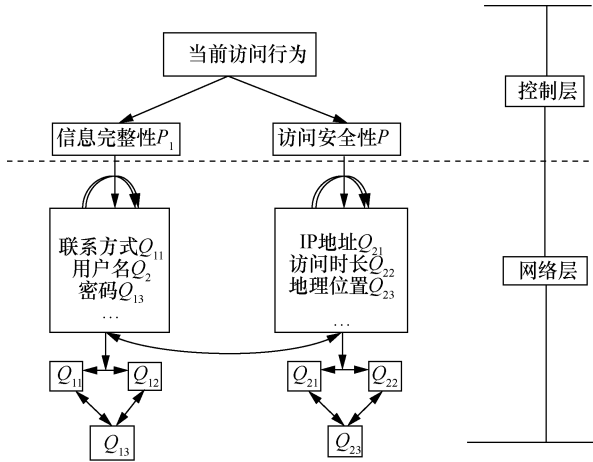


图 2 云用户访问环境的 ANP 结构
Figure 2 ANP structure of cloud user access environment

1.2 构造三角模糊判别矩阵

FANP 采用三角模糊数取代 1~9 Saaty 标度法，一方面能够体现信任不确定性与模糊性的特点，另一方面有效避免了传统 ANP 方法的主观随意性。通过专家打分对网络层的各元素进行两两

比较判断，得到三角模糊判别矩阵。1~9 Saaty 的具体标度方法如表 1 所示。

表 1 判断矩阵标度
Table 1 Scale of judgment matrix

标度值	内容
1	两元素同等重要
3	一元素比另一元素稍重要
5	一元素比另一元素明显重要
7	一元素比另一元素强烈重要
9	一元素比另一元素极端重要
2,4,6,8	上述元素比较的折中值

根据表 1 的判别标度构造三角模糊判别矩阵，采用三角模糊数对元素进行两两比较后同样需要进行一致性检验。

定义 1 设 $M = (a, b, c)$ 为一个模糊数， $0 < a \leq b \leq c$ 则称其为三角模糊数，其隶属度函数为^[2]

$$\mu_M(x) = \begin{cases} \frac{x-a}{b-a}, & a \leq x \leq b \\ \frac{x-c}{b-c}, & b \leq x \leq c \\ 0, & \text{其他} \end{cases} \quad (1)$$

其中，参数 a , b , c 分别表示下界、中间值与上界，用来描述信任的不确定性与模糊性。

定义 2 设 $M_1 = (a_1, b_1, c_1)$ 和 $M_2 = (a_2, b_2, c_2)$ 为两个三角模糊数，有关其计算法则如下。

1) $M_1 \oplus M_2 = (a_1, b_1, c_1) \oplus (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$ 。

2) $M_1 \otimes M_2 = (a_1, b_1, c_1) \otimes (a_2, b_2, c_2) = (a_1 a_2, b_1 b_2, c_1 c_2)$ 。

3) $1/M_1 = (a_1, b_1, c_1)^{-1} \approx (1/c_1, 1/b_1, 1/a_1)$ 。

1.3 构造超矩阵

构造模糊判断矩阵后，需要得到相对权重。首先进行模糊综合度的计算。设 M_{g_i} 为模糊判断矩阵中的模糊数，则模糊综合度 S_i 为

$$S_i = \sum_{j=1}^m M_{g_i}^j \otimes \left[\sum_{i=1}^n \sum_{j=1}^m M_{g_i}^j \right]^{-1} \quad (2)$$

其中， m 为矩阵的列数， n 为矩阵的行数。

其次计算 M_i 大于 M_j 的可能性程度，设 $M_1 = (a_1, b_1, c_1)$ 和 $M_2 = (a_2, b_2, c_2)$ 为两个三角模糊

数, 则 $M_1 \geq M_2$ 的可能性程度定义为

$$V(M_1 \geq M_2) = \begin{cases} 1, b_1 \geq b_2 \\ \frac{a_2 - c_1}{(b_1 - c_1) - (b_2 - a_2)}, b_1 \leq b_2, c_1 \geq a_2 \\ 0, \text{其他} \end{cases} \quad (3)$$

将求出的若干个可能性程度中的最小值记为该元素重要于其他元素的可能度^[2], 如式(4)所示。

$$d(A_i) = d(M \geq M_1, M_2, \dots, M_k) = \min d(M \geq M_i), i = 1, 2, \dots, k \quad (4)$$

设 $w' = [d(A_1), d(A_2), \dots, d(A_n)]^T$, 将其进行归一化后得到非模糊权重向量 $w = [d'(A_1), d'(A_2), \dots, d'(A_n)]^T$ 。按照此方法计算出其他的判断矩阵 w_{ij} 。

$$w_{ij} = \begin{bmatrix} w_{i1}^{(j1)} & \dots & w_{i1}^{(jn)} \\ \vdots & \ddots & \vdots \\ w_{in}^{(j1)} & \dots & w_{in}^{(jn)} \end{bmatrix} \quad (5)$$

矩阵 $w_{ij} = 0$ 中的列向量是网络层中元素之间影响力大小的排序向量^[5]。若网络层元素之间互相不受影响, 则 $w_{ij} = 0$, 以此得到 ANP 结构的超矩阵 w 。

$$w = \begin{bmatrix} w_{11} & \dots & w_{1N} \\ \vdots & \ddots & \vdots \\ w_{N1} & \dots & w_{NN} \end{bmatrix} \quad (6)$$

由上述矩阵可以观察到, 超矩阵是由若干个归一化的列分块组成, 但超矩阵本身并非归一化。因此需要获取控制准则下的加权矩阵 A 。

$$A = \begin{bmatrix} a_{11} & \dots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \dots & a_{NN} \end{bmatrix} \quad (7)$$

最后结合矩阵 A 与超矩阵的相应元素块即可获得加权超矩阵 w' 。在加权超矩阵中, 每一列的和为 1, 也称其为列随机矩阵^[2]。

1.4 用户行为证据的获取

云用户的行为证据是指云服务提供商的用户行为信任评价指标经过一定的处理得到的具体化

数值^[13]。获取用户行为证据的流程如下:

1) 利用 Bandwidthd 等网络流量分析工具来查看数据包的传送速率, 获取网关的各种协议^[14];

2) 利用计算机上的入侵检测系统, 如 RealSecure 等对网络安全进行分析, 获取实时的事件活动以及用户的访问次数等^[15];

3) 利用 Ajax 的点击流捕获工具获取用户的一系列动作信息;

4) 利用如 Cisco 的 NetFlow Monitor 等专门的数据采集工具^[15]获取数据。

为了让本文提出的信任评估机制的优化效果更真实, 本文所用的用户行为数据来源于开发的云用户行为监测、评估与控制示范平台, 平台包括图书的查询、购买、借阅、下载以及信息设置等功能。该平台是由 JSP 页面和后台控制程序组成的基于 Java 的 Web 系统。通过在 JSP 页面嵌入 JavaScript 代码可以获取用户的行为数据, 如用户名、密码以及用户键盘输入的退格次数等, 此外, 通过 JavaScript 可以获取到用户的地理位置以及 IP 地址等信息; 当用户切换页面时, 系统根据 JSP 页面提交的表单还可以获取用户的查询以及借阅次数等信息。当退出平台时, 用户在该系统平台所操作的一系列动作被记录在数据库中。

1.5 用户行为信任度

(1) 用户行为评估矩阵

评估矩阵由 FANP 方法获取的行为证据权重与初始证据矩阵计算得到。本文通过开发的平台获取用户不同模块下的行为证据, 依据用户行为证据规则库^[16]将行为证据划分为相应的信任等级。将信任等级构成初始证据矩阵进行后续的计算。

设初始证据矩阵为 $U = (u_{ij})_{mn}$, 行为证据权重矩阵为 $W = (w_{ij})_{mn}$, 根据 $U \times w^T$ 获得的矩阵对角线即用户行为评估矩阵 $E = (e_1, e_2, \dots, e_n)$ 。将评估矩阵与相应模块下的控制层指标权重相结合即该模块下的用户行为信任度。

(2) 综合行为信任度计算

云用户的综合行为信任度包括访问环境信任度 $F(u_i)$ 与历史访问行为信任度 $L(u_i)$ 两部分。计算方式如下。

$$T(u_i) = \alpha L(u_i) + \beta F(u_i) \quad (8)$$

其中, α 和 β 分别表示历史访问行为与当前访问环境行为所占的比重, 且 $\alpha + \beta = 1$ 。它们的值随着云服务提供商侧重程度的增加而增大, 如在某个云环境下, 云服务商更看重用户的历史访问行为, 那么应该提高 α 的值, 减小 β 的值。

(3) 用户行为信任等级

本文根据实际应用需求将用户行为信任等级划分为 5 个等级, 即 L_1 :不可信; L_2 :一般可信; L_3 :基本可信; L_4 :中等可信; L_5 :高度可信。信任等级划分情况如表 2 所示。

表 2 信任等级划分 Table 2 Trust level division table	
信任值	信任等级
[0, 0.2]	L_1
(0.2, 0.3]	L_2
(0.3, 0.6]	L_3
(0.6, 0.8]	L_4
(0.8, 1]	L_5

2 实验结果与分析

本文实验运行在一个用户行为监测、评估与控制示范的平台上, 该平台可以获取到历史访问行为以及当前访问环境两方面的用户行为数据。将最近 7 天的用户行为数据作为行为证据, 实验部分所选取的用户行为证据与 1.1 节中 ANP 模型所列出的行为数据一一对应。

2.1 信任评估实例计算

(1) 建立模糊判断矩阵

将历史访问行为方面下的常规行为与灰色行为为两个指标进行比较, 利用三角模糊数列出两两比较矩阵。一级指标模糊判断矩阵如图 3 所示。

	常规行为(R_1)	灰色行为(R_2)
常规行为(R_1)	(1,1,1)	(1,2,4)
灰色行为(R_2)	(1/4,1/2,1)	(1,1,1)

图 3 一级指标模糊判断矩阵
Figure 3 Fuzzy judgment matrix of primary index

根据式 (2) 计算综合模糊度为: $S_{R_1} = (0.29, 0.67, 1.54)$; $S_{R_2} = (0.18, 0.33, 0.62)$ 。

根据式(3)得出各准则重要于其他准则的重要性程度为: $d(S_{R_1}) = 1$; $d(S_{R_2}) = 1.33$ 。

将其归一化获得加权矩阵为: $A_1 = (0.43, 0.57)^T$ 。

按照相同的方法计算访问环境方面下的加权矩阵为: $A_2 = (0.4, 0.6)^T$ 。

本文分别构建了历史访问行为与访问环境两方面的 ANP 结构模型, 以历史访问行为方面的计算为例, 分别构建不同准则下常规行为与灰色行为下不同元素之间的两两判断模糊矩阵, 如在用户名失败次数(S_{22})一定的准则下, 常规访问行为下的各元素之间的模糊判断矩阵如图 4 所示。

S_{22}	S_{11}	S_{12}	S_{13}
S_{11}	(1,1,1)	(1/3,2/5,1/2)	(1,2,4)
S_{12}	(2,5/2,3)	(1,1,1)	(1/6,1/4,1/2)
S_{13}	(1/4,1/2,1)	(2,4,6)	(1,1,1)

图 4 两两比较矩阵
Figure 4 Pairwise comparison matrix

通过式(2)~式(4)的计算方法得到归一化的权重向量为 $w = (0.33, 0.27, 0.40)^T$ 。

(2) 建立超矩阵

按照上述同样的方法求出不同准则下的相应权重, 所有权重组成历史访问行为下的超矩阵。按照相同的原理求得访问环境下的超矩阵。上述过程采用手工运算计算量过大, 本文借助计算 ANP 的专属工具 yaanp 来获取结果, 计算结果分别如图 5、图 6 所示。

	S_{11}	S_{12}	S_{13}	S_{21}	S_{22}	S_{23}
S_{11}	0	0.75	0.21	0.12	0.33	0.23
S_{12}	0.69	0	0.79	0.61	0.27	0.55
S_{13}	0.31	0.25	0	0.27	0.40	0.22
S_{21}	0.34	0.33	0.13	0	0.68	0.74
S_{22}	0.21	0.28	0.33	0.61	0	0.26
S_{23}	0.45	0.38	0.54	0.39	0.32	0

图 5 历史访问行为下的超矩阵
Figure 5 Hypermatrix under historical access behavior

(3) 计算极限超矩阵

对超矩阵进行加权获取加权超矩阵, 将加权超矩阵不断进行自乘直到得到一个稳定的极限矩阵, 任取极限矩阵中的一列数据就是各个元素最终的稳定权重。此过程同样借助专属计算软件 yaanp 来完成, 计算结果如图 7 和图 8 所示。

	Q_{11}	Q_{12}	Q_{13}	Q_{21}	Q_{22}	Q_{23}
Q_{11}	0	0.34	0.27	0.13	0.36	0.59
Q_{12}	0.31	0	0.73	0.28	0.23	0.13
Q_{13}	0.69	0.66	0	0.59	0.41	0.28
Q_{21}	0.34	0.28	0.22	0	0.69	0.72
Q_{22}	0.07	0.34	0.25	0.16	0	0.29
Q_{23}	0.59	0.38	0.53	0.84	0.31	0

图 6 访问环境下的超矩阵
Figure 6 Hypermatrix in access environment

	S_{11}	S_{12}	S_{13}	S_{21}	S_{22}	S_{23}
S_{11}	0.1523	0.1523	0.1523	0.1523	0.1523	0.1523
S_{12}	0.2092	0.2092	0.2092	0.2092	0.2092	0.2092
S_{13}	0.1123	0.1123	0.1123	0.1123	0.1123	0.1123
S_{21}	0.2045	0.2045	0.2045	0.2045	0.2045	0.2045
S_{22}	0.1600	0.1600	0.1600	0.1600	0.1600	0.1600
S_{23}	0.1617	0.1617	0.1617	0.1617	0.1617	0.1617

图 7 历史访问行为下的极限超矩阵
Figure 7 Limit hypermatrix under historical access behavior

	Q_{11}	Q_{12}	Q_{13}	Q_{21}	Q_{22}	Q_{23}
Q_{11}	0.1014	0.1014	0.1014	0.1014	0.1014	0.1014
Q_{12}	0.0941	0.0941	0.0941	0.0941	0.0941	0.0941
Q_{13}	0.1378	0.1378	0.1378	0.1378	0.1378	0.1378
Q_{21}	0.2572	0.2572	0.2572	0.2572	0.2572	0.2572
Q_{22}	0.1289	0.1289	0.1289	0.1289	0.1289	0.1289
Q_{23}	0.2806	0.2806	0.2806	0.2806	0.2806	0.2806

图 8 访问环境下的极限超矩阵
Figure 8 Limit hypermatrix in access environment

(4) 用户行为信任度计算

通过开发的平台获取的用户历史访问行为与访问环境两方面的证据值经过规范化处理后^[17], 参考用户行为证据规则库^[16]查看得到的历史访问行为初始证据值为: $u_1 = \begin{bmatrix} 3 & 4 & 2 \\ 2 & 3 & 4 \end{bmatrix}$,

$$u_2 = \begin{bmatrix} 6 & 5 & 7 \\ 4 & 6 & 5 \end{bmatrix}, u_3 = \begin{bmatrix} 3 & 4 & 7 \\ 6 & 5 & 4 \end{bmatrix}。$$

云用户的访问环境初始证据值为:

$$u_1 = \begin{bmatrix} 3 & 7 & 3 \\ 7 & 4 & 4 \end{bmatrix}, u_2 = \begin{bmatrix} 7 & 7 & 3 \\ 7 & 6 & 3 \end{bmatrix}, u_3 = \begin{bmatrix} 3 & 4 & 6 \\ 7 & 6 & 5 \end{bmatrix}。$$

求得云用户特性层的评估矩阵:

$$E_1 = \begin{bmatrix} 1.5183 & 1.5358 \\ 1.3763 & 3.4384 \end{bmatrix}, E_2 = \begin{bmatrix} 2.7459 & 4.863 \\ 1.7819 & 3.4156 \end{bmatrix},$$

$$E_3 = \begin{bmatrix} 2.0798 & 2.6738 \\ 1.5074 & 3.9768 \end{bmatrix}。$$

根据云用户历史访问行为与访问环境两方面评估特性层的权重与特性层的评估矩阵求得云用户历史访问行为与访问环境的信任度为: $E_{u_1} = [1.5283 \quad 2.6136]$, $E_{u_2} = [3.9526 \quad 2.7621]$, $E_{u_3} = [2.4184 \quad 2.9890]$ 。

假设本文实验中 $\alpha = 0.4$, $\beta = 0.6$, 根据式(8)求得用户综合信任度。根据规范化处理, 最终的用户信任值与所对应的信任等级如表 3 所示。

表 3 信任值与信任等级
Table 3 Trust degree and trust level table

信任值	信任等级
0.2180	L_2
0.3238	L_3
0.2761	L_2

2.2 实验对比

为了验证本文提出的信任评估机制的性能优化效果, 对基于本文的 FANP 优化评估机制与传统的 AHP 信任评估机制进行实验对比。

采用 Python 语言模拟某云端用户在与云服务商进行交互的过程中, 如用户密码错误次数、退格次数等损坏信任值的行为比例增加时的信任度变化情况。本文实验中将损坏信任值的行为称为恶意行为。图 9 给出了两种评估机制在不同的恶意用户行为比率下的信任度变化情况。

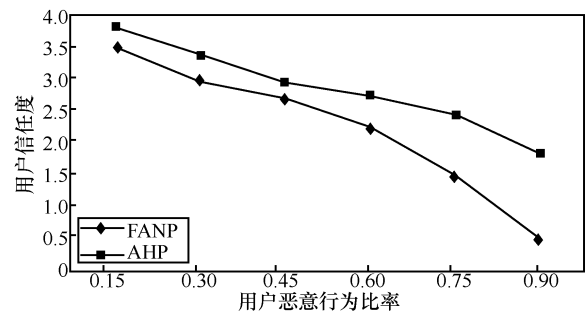


图 9 用户信任度随用户恶意行为比率的变化
Figure 9 The change of user trust with the ratio of malicious behavior

从图 9 可以看出, 随着用户恶意行为比率的增加, 两种行为信任评估机制中的用户信任度都

呈现下降趋势, 但本文提出的优化机制比传统的 AHP 评估机制下降更为显著, 且在不同的恶意行为比率下, 本文机制中用户的行为信任度始终低于 AHP 机制中的信任度, 这说明本文的优化机制能够更早更快地识别出信任度低的用户, 从而降低云端的风险。

3 结束语

云计算环境安全面临着严峻的考验, 设计有效的机制对云端用户展开信任评估是有效提升云安全的方法之一。本文引入模糊网络分析法, 体现了信任的不确定性, 弱化了传统评估方法普遍存在的主观性; 扩展了用户行为管理模块, 分别构造云用户历史访问行为和访问环境两个角度下的网络层次模型, 细化了评估粒度。实验结果证明所提出的优化机制可以更好地识别出恶意用户, 提高云环境的安全性。下一步会根据本文的信任评估优化机制研究相对应的访问控制策略, 从而打造一个安全性更高的云环境。

参考文献:

- [1] 陈红松, 王钢, 宋建林. 基于云计算入侵检测数据集的内网用户异常行为分类算法研究[J]. 信息网络安全, 2018(3): 1-7.
CHEN H S, WANG G, SONG J L. Research on anomaly behavior classification algorithm of internal network user based on cloud computing intrusion detection data set[J]. Netinfo Security, 2018(3): 1-7.
- [2] 王国峰, 刘川意, 潘鹤中, 等. 云计算模式内部威胁综述[J]. 计算机学报, 2017, 40(2): 296-316.
WANG G F, LIU C Y, PAN H Z, et al. Survey on insider threats to cloud computing[J]. Chinese Journal of Computers, 2017, 40(2): 296-316.
- [3] 王晶. 基于属性的云服务访问控制技术研究[D]. 保定: 河北大学, 2016.
WANG J. Study of the technology on attribute based access control in cloud computing services[D]. Baoding: Hebei University, 2016.
- [4] 王燕, 周建涛. 云环境下的信任研究方法与技术[J]. 小型微型计算机系统, 2015, 36(10): 2334-2339.
WANG Y, ZHOU J T. Trust research methods and technology in cloud computing[J]. Journal of Chinese Computer Systems, 2015, 36(10): 2334-2339.
- [5] 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.
WANG C. The research of trust evaluation based on user behavior in cloud computing[D]. Baotou: Inner Mongolia University of Science & Technology, 2015.
- [6] 王晋东, 卫波, 张恒巍, 等. 云计算环境下服务信任评估方法研究[J]. 计算机科学, 2014, 41(12): 38-42, 66.
WANG J D, WEI B, ZHANG H W, et al. Research on service trust evaluation approach under cloud computing environment[J]. Computer Science, 2014, 41(12): 38-42, 66.
- [7] 田立业, 詹静, 姜伟, 等. 量化的云计算信任模型研究[J]. 计算机工程与设计, 2013, 34(1): 13-17.
TIAN L Y, ZHAN J, JIANG W, et al. Research on quantified cloud computing trust model[J]. Computer Engineering and Design, 2013, 34(1): 13-17.
- [8] 毋泽南, 田立勤, 王志刚. 基于机器学习的 Web 用户行为认证[J]. 网络与信息安全学报, 2018, 4(1): 45-51.
WU Z N, TIAN L Q, WANG Z G. Behavior authentication of Web users based on machine learning[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 45-51.
- [9] HUANG X M, YU R, KANG J W, et al. Distributed reputation management for secure and efficient vehicular edge computing and networks[J]. IEEE Access, 2017, 5: 25408-25420.
- [10] 谢晓兰, 李鑫融, 陈超泉. 云环境中用户可信度计算方法[J]. 桂林理工大学学报, 2020, 40(1): 122-130.
XIE X L, LI X R, CHEN C Q. Research on calculation method of user trust in cloud environment[J]. Journal of Guilin University of Technology, 2020, 40(1): 122-130.
- [11] 胡园园, 顾新, 王涛. 基于网络层次分析法的知识链信任评估研究[J]. 情报科学, 2015, 33(12): 40-45.
HU Y Y, GU X, WANG T. Research on trust evaluation of knowledge chain based on the analytic network process[J]. Information Science, 2015, 33(12): 40-45.
- [12] 许永平, 朱延广, 杨峰, 等. 基于 ANP 和模糊积分的多准则决策方法及其应用[J]. 系统工程理论与实践, 2010, 30(6): 1099-1105.
XU Y P, ZHU Y G, YANG F, et al. New multi criteria decision making approach based on ANP and fuzzy integral with its application[J]. Systems Engineering-Theory & Practice, 2010, 30(6): 1099-1105.
- [13] 肖传奇, 陈明志. 云环境下基于 IFAHP 的用户行为信任模型研究[J]. 信息网络安全, 2015(12): 14-20.
XIAO C Q, CHEN M Z. Research on user behavior trust model based on IFAHP in cloud computing environment[J]. Netinfo Security, 2015(12): 14-20.
- [14] 毋泽南, 田立勤, 王志刚. 一种结合滑动窗口和推荐信任的用户行为信任评估[J]. 山东大学学报(理学版), 2019, 54(1): 53-59.
WU Z N, TIAN L Q, WANG Z G. A user behavior trust evaluation combined with sliding window and recommended trust[J]. Journal of Shandong University (Natural Science), 2019, 54(1): 53-59.
- [15] 王卫强. 基于动态反馈的云安全访问控制机制研究[D]. 沈阳: 东北大学, 2013.
WANG W Q. The research of security access control based on dynamic feedback on cloud computing platform[D]. Shenyang: Northeastern University, 2013.
- [16] 田立勤. 网络用户行为的安全可信分析与控制[M]. 北京: 清华大学出版社, 北京交通大学出版社, 2011.
TIAN L Q. Security and trust analysis and control of network user behavior [M]. Beijing: Tsinghua University Press, Beijing Jiaotong University Press, 2011.
- [17] 马佳乐, 郭银章. 云计算用户行为信任评估与访问控制策略研究[J]. 计算机应用研究, 2020, 37(S2): 260-262.
MA J L, GUO Y Z. Research on cloud computing user behavior trust evaluation and access control strategy[J]. Application Research of Computers, 2020, 37(S2): 260-262.

[作者简介]



张艺（1995-），女，山东威海，华北科技学院硕士生，主要研究方向为网络安全评价与用户行为认证。



毋泽南（1991-），男，河南焦作，青海师范大学博士，主要研究方向为信任安全、用户行为认证。



田立勤（1970-），男，陕西定边，博士，华北科技学院教授、博士生导师，主要研究方向为物联网远程信息监控、大数据有效性审核、网络安全评价与用户行为认证、网络性能评价与优化。



武文星（1996-），男，山西吕梁人，华北科技学院硕士生，主要研究方向为算法优化。