偏联系数隐私风险态势评估方法

晏 燕[1,2],王万军[3]
YAN Yan[1,2], WANG Wanjun[3]

1.兰州理工大学 电气工程与信息工程学院,兰州 730050
2.兰州理工大学 计算机与通信学院,兰州 730050
3.兰州文理学院 数字媒体学院,兰州 730000
1.School of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China
2.School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China
3.College of Digital Media, Lanzhou University of Arts and Science, Lanzhou 730000, China

YAN Yan, WANG Wanjun. Privacy risk situation assessment method based on partial connection numbers. Computer Engineering and Applications, 2018, 54(10):143-148.

Abstract: In view of the problem of privacy risk situation assessment, a set pair analysis assessment system is set up for privacy risk indicators based on the theory of five-element partial connection numbers. The weights of assessment indicators are determined by the method of least squares partial weighting. Partial differential processes are carried out on different stages by using the theory of five-element connection numbers. Potential values and trends are calculated and analyzed for partial connection numbers on different stages in order to realize situation assessment of privacy risk. The proposed method can dynamically reflect privacy risk assessment indicators and effectively eliminate interference and adverse effects caused by uncertainty, vagueness and randomness during the process of privacy risk assessment. Finally, some examples are given to analyze the feasibility and effectiveness of the proposed method.
Key words: privacy risk; situation assessment; five-element partial connection numbers; least squares partial weighting

摘 要:针对数据隐私保护风险评估问题,利用集对分析的五元偏联系数理论,为隐私风险待评估指标建立了集对分析评估系统。采用最小二偏赋权方法确定评估指标的权重,并运用五元联系数对隐私评估指标进行分阶偏处理,对各阶偏联系数进行势态计算并分析趋势走向,实现对隐私风险态势的评估。该方法能够对隐私风险评估指标进行动态的体现,有效消除了隐私风险评估过程中不确定、模糊、随机等误差因素的干扰和不良影响。通过实例分析了该方法的可行性和有效性。
关键词:隐私风险;态势评估;五元偏联系数;最小二偏赋权
文献标志码:A **中图分类号:**TP309 doi:10.3778/j.issn.1002-8331.1612-0444

1 引言

随着互联网与移动通信技术的迅猛发展,云计算、大数据、物联网、车联网、智慧城市、智能家居等新兴技术层出不穷,用户能够随时、随地、随身的对信息进行访问、查询和跟踪。同时,大量的数字化信息存在于网络空间、云平台和移动终端,使得用户的隐私信息面临威胁[1]。隐私信息的泄露不仅影响到人们的财产和生命安全,甚至威胁社会稳定与国家安全。因此,如何有效防止用户隐私信息的泄露已经成为全社会共同关注的焦点和亟待解决的重要问题[2]。进行隐私信息风险评估、降低隐私信息泄露发生率,对提高隐私信息的安全性具有重要而现实的意义。

目前,国内外关于隐私保护规则和相关算法的研究已经取得不少成果[3-8]。但是,对隐私风险评估的研究相

基金项目:国家自然科学基金(No.61762059,No.61363078);甘肃省青年科技基金计划项目(No.1310RJYA004)。
作者简介:晏燕(1980—),女,副教授,硕士生导师,主要研究方向为隐私保护技术和多媒体信息安全,E-mail:yanyan@lut.cn;王万军(1974—),男,副教授,主要研究方向为智能信息处理技术。
收稿日期:2016-12-27 **修回日期:**2017-02-17 **文章编号:**1002-8331(2018)10-0143-06
CNKI **网络出版:**2017-05-16, http://kns.cnki.net/kcms/detail/11.2127.TP.20170516.1757.014.html

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

对较少。文献[9]总结了国内外信息系统安全风险评估的常用方法,研究了信息系统安全风险的分布规律,提出了适用于信息系统安全风险评估的一般方法。文献[10]使用模糊集理论对信息系统的风险因素进行分析,构造了各种因素所对应的隶属度矩阵,采用熵权系数法确定因素权重以减少传统权重确定方法的主观偏差。Saripaui等[11]采用Delphi法将搜集到的信息进行归纳、修改、汇总,并对隐私风险进行定量评估研究。任丹丹等[12]研究了车载自组织网络中的位置隐私风险,通过布尔函数对隐私泄露攻击目标建立攻击树模型,并对各攻击树节点多属性赋值进行分析。张秋瑾[13]和Wang等[14]研究并建立了云计算隐私评估的指标体系,运用信息熵、模糊集和马尔科夫链等理论对云计算的隐私风险进行评估建模。文献[15]将多元联系数集对分析理论应用于航空维修风险评估,运用不确定层次分析法确定各评估指标的权重区间。综合分析目前已经报道的各种评估方法,定量方法大多是建立在Fuzzy数学、Vague理论、灰理论、贝叶斯理论、粗糙集理论或直觉模糊理论等基础上的。虽然这些方法起到了一定的评估效果,但仍然存在诸多缺陷和不足[14]。例如,对评估指标中信息临界边值的指派、确定-不确定信息的集成、不同评估方法中权重的取值等,都直接影响评估结果的准确与否。

本文在分析隐私风险评估指标的基础上,提出新的隐私风险态势评估方法。利用集对分析理论中的偏联系数[16-17]方法,对风险指标计算偏阶联系数的态势并分析趋势变化,从而实现隐私风险的评估。为了克服人为因素对评估结果的影响,风险指标的权重采用最小二偏方法进行科学计算,从而有效消除了评估过程中不确定因素对结果的干扰和影响。

2　隐私风险评估

隐私风险评估是对隐私系统风险进行的全面、系统的估计和衡量。导致隐私风险的因素包罗万象,其中既有人为因素,亦有客观原因;既有技术因素,亦有设备原因;既有内因,亦有外因;既有系统自身的脆弱性因素,亦有保密泄露的原因;既有系统的不完备性因素,亦有人为蓄意攻击的可能。总而言之,隐私风险就是隐私数据泄露发生的可能性及其负面影响。隐私风险评估就是对隐私风险发生的可能性及其负面影响进行识别和评价。

本文在研究国内外大量隐私泄露事件风险评估方法的基础上,通过详细总结、分类和筛选,并结合ITSEC(Information Technology Security Evaluation Criteria)的定义[18]及文献[10]和文献[13]建立了如表1所示的隐私风险评估指标体系。

表1　隐私风险评估指标体系

隐私风险评估目标	一级指标	二级指标	三级指标
隐私风险评估	隐私风险资产 B_1	保密性 C_1	数据加密 T_{11}
			数据隔离 T_{12}
			密钥管理 T_{13}
			数据保密 T_{14}
		完整性 C_2	数据备份 T_{21}
			数据销毁 T_{22}
			软件升级 T_{23}
		可用性 C_3	数据迁移 T_{31}
			风险识别 T_{32}
	隐私风险威胁 B_2	技术风险 C_4	恶意攻击 T_{41}
			网络监控 T_{42}
			漏洞处理 T_{43}
		个人风险 C_5	内部人员 T_{51}
			身份验证 T_{52}
			操作失误 T_{53}
	隐私风险脆弱性 B_3	组织脆弱性 C_6	审查支持 T_{61}
			法律遵守 T_{62}
			责任权益 T_{63}
		技术脆弱性 C_7	服务锁定 T_{71}
			访问控制 T_{72}
		其他 C_8	规章制度 T_{81}
			隐私处理 T_{82}
			风险申报 T_{83}

3　基于偏联系数的隐私风险态势评估方法

3.1　联系数

联系数[16]是集对分析理论(Set Pair Analysis,SPA)中刻画两个集合之间相互联系、制约、影响并反映属性的同(同一、肯定或支持)、异(不确定)、反(对立、否定或反对)关系的表达式。

定义1　设 X 为非空集合,则 $A=\{<x,a_A(x),b_A(x),c_A(x)>|x\in X\}$ 的联系数为:

$$\mu_A(x)=a_A(x)+b_A(x)i+c_A(x)j \tag{1}$$

其中 $a_A(x),b_A(x),c_A(x)$ 分别表示 X 中元素 x 属于 A 的支持(同)度,不确定(异)度和对立(反)度。$a_A(x):x\to[0,1]$,$b_A(x):x\to[0,1]$,$c_A(x):x\to[0,1]$ 满足归一化条件 $a_A(x)+b_A(x)+c_A(x)=1$。其中 $i\in[-1,1]$,称为不确定度系数;j 为对立度系数,通常情况可取 $j=-1$。

3.1.1　偏联系数

式(1)中含有同、异、反三个元素,因此又称为同异反联系数或三元联系数。多元联系数是将三元联系数中的不确定项 b_i 进一步拓展得到的一般形式:

$$\mu=a+b_1i_1+b_2i_2+\cdots+b_ni_n+cj \tag{2}$$

当 $n=3$ 时,称式(2)为五元联系数,记为:

$$\mu=a+bi+cj+dk+el \tag{3}$$

式(3)中 a 为同一度,b 为同差异偏同分量,c 为同差异中立分量,d 为同差异偏反分量,e 为对立度,

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

i,j,k,l 分别为 $b,c,d,e\in[0,1]$ 的系数，且满足归一化条件：$a+b+c+d+e=1$。

定义2[15,19] 在五元联系数 μ 中，一阶偏联系数为：

$$\partial\mu=\partial a+\partial bi+\partial cj+\partial dk \tag{4}$$

其中，$\partial a=\frac{a}{a+b}$，$\partial b=\frac{b}{b+c}$，$\partial c=\frac{c}{c+d}$，$\partial d=\frac{d}{d+e}$。

定义3 在五元联系数 μ 中，二阶偏联系数为：

$$\partial^2\mu=\partial(\partial\mu)=\partial^2 a+\partial^2 bi+\partial^2 cj \tag{5}$$

其中，$\partial^2 a=\frac{\partial a}{\partial a+\partial b}$，$\partial^2 b=\frac{\partial b}{\partial b+\partial c}$，$\partial^2 c=\frac{\partial c}{\partial c+\partial d}$。二阶偏联系数是在一阶偏联系数上进行的偏离趋向变化。

定义4 在五元联系数 μ 中，三阶偏联系数为：

$$\partial^3\mu=\partial^2(\partial\mu)=\partial^3 a+\partial^3 bi \tag{6}$$

其中，$\partial^3 a=\frac{\partial^2 a}{\partial^2 a+\partial^2 b}$，$\partial^3 b=\frac{\partial^2 b}{\partial^2 b+\partial^2 c}$。

定义5 在五元联系数 μ 中，四阶偏联系数为：

$$\partial^4\mu=\partial^3(\partial\mu)=\partial^4 a \tag{7}$$

其中，$\partial^4 a=\frac{\partial^3 a}{\partial^3 a+\partial^3 b}$。

偏联系数是描述偏离趋向变化高低的函数，它反映了同异反联系状态的发展趋势和变化。在 r 阶偏联系数中，当 $\partial^{(r)}\mu>0$ 时，本次联系分量相对上次联系分量而言，朝正方向层次迁移，呈现提高趋势；当 $\partial^{(r)}\mu<0$ 时，本次联系分量相对上次联系分量而言，朝负方向层次迁移，呈现下降趋势；当 $\partial^{(r)}\mu=0$ 时，本次联系分量相对上次联系分量而言，朝不确定方向层次迁移，呈现中介不确定趋势。

3.1.2　势与偏势

定义6[15] 在三元联系数 $\mu=a+bi+cj$ 中，当 $c\neq0$ 时，联系数的势为：

$$shi(\mu)=a/c \tag{8}$$

$shi(\mu)>1$ 时称为同势；$shi(\mu)=1$ 时称为均势；$shi(\mu)<1$ 时称为反势。

当 $c=0$ 时，三元联系数降为二元联系数，其势值可以用同一度 a 进行度量。当 $a>b$ 时，称为不确定同一势；当 $a\leqslant b$ 时，称为不确定-不确定势。

定义7 五元联系数 μ 的势为：

$$shi(\mu)=(a+b)/(d+e) \tag{9}$$

其对应的一阶、二阶、三阶偏联系数分别为：

$$shi(\partial\mu)=(\partial a+\partial b)/\partial d \tag{10}$$

$$shi(\partial^2\mu)=\partial^2 a/\partial^2 c \tag{11}$$

$$shi(\partial^3\mu)=\partial^3 a \tag{12}$$

在隐私风险评估中，“同势”表明隐私风险评估与理想标准风险趋于同一变化状态，即处于隐私评估的“低风险”；“均势”表明隐私风险评估与理想标准风险趋于势均力敌状态，即处于隐私评估的“中等风险”；“反势”表明隐私风险评估与理想标准风险趋于反向状态，即处于隐私评估的“高风险”。进一步而言，“一阶同偏联系数势”表明隐私风险评估与理想标准风险趋于低风险发展趋势，继续发展仍然处于低风险发展趋势；“一阶均偏联系数势”表明隐私风险评估与理想标准风险趋于中间风险发展趋势，继续发展仍然处于中间风险发展趋势；“一阶反偏联系数势”表明隐私风险评估与理想标准风险趋于高风险发展趋势，继续发展仍然处于高风险发展趋势。二阶和三阶偏联系数势的同、均、反偏联系数含义与一阶偏联系数势类似，反映了上一阶发展趋势进一步继续发展以后风险趋势的变化。

3.1.3　记分函数与精确函数

定义8 五元联系数 μ 的记分函数为：

$$S(\mu)=(a+b)-(d+e) \tag{13}$$

其对应的一阶、二阶、三阶偏联系数记分函数分别为：

$$S(\partial\mu)=(\partial a+\partial b)-\partial d \tag{14}$$

$$S(\partial^2\mu)=\partial^2 a-\partial^2 c \tag{15}$$

$$S(\partial^3\mu)=\partial^3 a \tag{16}$$

定义9 五元联系数 μ 的精确函数为：

$$H(\mu)=a+b+d+e \tag{17}$$

其对应的一阶、二阶、三阶偏联系数精确函数分别为：

$$H(\partial\mu)=\partial a+\partial b+\partial d \tag{18}$$

$$H(\partial^2\mu)=\partial^2 a+\partial^2 c \tag{19}$$

$$H(\partial^3\mu)=\partial^3 a \tag{20}$$

在隐私风险评估中，记分函数 $S(\mu)$ 和精确函数 $H(\mu)$ 相当于数理统计中的均值和方差[20]，记分函数越大，隐私潜在风险越高；记分函数越小，隐私潜在风险越低。当记分函数相同时，精确函数越大，隐私潜在风险越高；精确函数越小，隐私潜在风险越低。因此，利用记分函数和精确函数可以对隐私潜在风险进行等级排序评估和预测分析。表2给出了9标度语义与记分函数的关系。

表2　9标度语义与记分函数关系

模糊语义	联系数	记分函数值
极大(极高)	1+0i+0j	1.000
很大(很高)	0.9+0.05i+0.05j	0.923
较大(较高)	0.8+0.1i+0.1j	0.839
大(高)	0.7+0.15i+0.15j	0.748
一般(中等)	0.5+0i+0.5j	0.500
小(低)	0.3+0.15i+0.55j	0.278
较小(较低)	0.2+0.1i+0.7j	0.172
很小(很低)	0.1+0.05i+0.85j	0.081
极小(极低)	0+0i+1j	0

3.2　最小二偏赋权

权重是隐私风险评估中对各待评指标影响程度的反映和体现，权重系数的确定直接决定评估结果的优劣。权重的确定方法主要有三类[13]：主观赋权法、客观赋权法和综合赋权法。主观赋权通常根据决策者的经

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

验方法进行给定,评估的科学性和有效性很大程度上受到主观人为因素和个人偏好程度的影响。客观赋权根据待评估指标信息计算权重系数,但有时客观赋权过于强调计算而脱离实际,无法给出合理的解释。综合赋权是将各种赋权方法根据实际问题结合的一种方法。本文结合主观赋权和客观赋权的方法,提出一种五元偏联系数势的最小二偏赋权方法。

对隐私风险属性 G_i,其 r 阶偏联系数势矩阵为:

$$\boldsymbol{P}_i^{(r)}=\begin{pmatrix} p_{11}^{(r)} & p_{12}^{(r)} & \cdots & p_{1n}^{(r)} \\ p_{21}^{(r)} & p_{22}^{(r)} & \cdots & p_{2n}^{(r)} \\ \vdots & \vdots & & \vdots \\ p_{m1}^{(r)} & p_{m2}^{(r)} & \cdots & p_{mn}^{(r)} \end{pmatrix}=(p_{lj})_{nm} \tag{21}$$

对于两个不同的 r 阶偏联系数势矩阵 $\boldsymbol{P}_j^{(r)}$ 和 $\boldsymbol{P}_k^{(r)}$,其偏差用 $D_i^{(r)}(\omega)$ 表示:

$$D_i^{(r)}(\omega)=\left(\sum_{i=1}^{n}\sqrt{(p_{ij}^{(r)}-p_{ik}^{(r)})^2}\right)^{\frac{1}{2}} \tag{22}$$

式(22)只是权重重要程度相同时的情况,但在多数情况下,隐私风险指标的权重重要程度是不同的。在不同权重向量 $\boldsymbol{W}_i=(w_{1i},w_{2i},\cdots,w_{mi})^{\mathrm{T}}$ 构成的评估指标中,为了评估结果的合理,构建最小二偏函数:

$$\min\ D^{(r)}(\omega)=\sum_{i=1}^{m}D_i^{(r)}(\omega)=\sum_{j=1}^{n}\left(\sum_{i=1}^{n}\omega_j^{(r)}\sqrt{(p_{ij}^{(r)}-p_{ik}^{(r)})^2}\right)^{\frac{1}{2}} \tag{23}$$

为了求解式(23),建立如下最小二偏目标函数:

$$\min\ D^{(r)}(\omega)=\sum_{i=1}^{m}D_i^{(r)}(\omega)=\sum_{j=1}^{n}\left(\sum_{i=1}^{n}\omega_j^{(r)}\sqrt{(p_{ij}^{(r)}-p_{ik}^{(r)})^2}\right)^{\frac{1}{2}}$$

$$\text{s.t.}\ \sum_{j=1}^{n}\omega_j^{(r)}=1,\omega_j^{(r)}\geqslant 0,j=1,2,\cdots,n \tag{24}$$

构造Lagrange函数对式(24)进行求解,最后得到一般的最小 h 偏赋权公式:

$$\omega_j^{(r)}=\frac{\left[\sum_{i=1}^{m}\left(\sqrt{(p_{ij}^{(r)}-p_{ik}^{(r)})^2}\right)^h\right]^{\frac{1}{h}}}{\sum_{j=1}^{n}\left[\sum_{i=1}^{m}\left(\sqrt{(p_{ij}^{(r)}-p_{ik}^{(r)})^2}\right)^h\right]^{\frac{1}{h}}} \tag{25}$$

在实际问题中,通常采用二偏赋权 $(h=2)$ 求权重即可。

4　应用分析

根据表1构建的隐私风险评估指标体系,由专家对隐私风险资产、隐私风险威胁和隐私风险脆弱性等指标给出如表3所示的评估意见。

隐私风险评估的步骤如下:

步骤1　计算隐私风险指标的权重。将表3中定性的隐私风险指标转化为对应的偏联系数势矩阵,结合式(21)~(25)计算得到各风险指标的权重为:

表3　隐私风险评估表

风险指标	隐私风险因素	隐私风险资产 B_1	隐私风险威胁 B_2	隐私风险脆弱性 B_3
C_1	T_{11}	高	中等	高
	T_{12}	低	较低	较高
	T_{13}	高	较高	高
	T_{14}	较低	高	高
C_2	T_{21}	高	较高	较低
	T_{22}	低	中等	高
	T_{23}	高	高	低
C_3	T_{31}	高	低	高
	T_{32}	较高	高	较低
C_4	T_{41}	很高	高	高
	T_{42}	高	低	很低
	T_{43}	低	高	较高
C_5	T_{51}	低	低	高
	T_{52}	很低	低	较高
	T_{53}	高	低	低
C_6	T_{61}	高	高	低
	T_{62}	低	低	高
	T_{63}	较高	高	高
C_7	T_{71}	高	较高	低
	T_{72}	高	高	较低
C_8	T_{81}	低	较低	高
	T_{82}	高	高	较低
	T_{83}	高	高	低

$$w(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8)=[0.171\,8,0.126\,1,0.086\,5,0.168\,9,0.129\,1,0.152\,2,0.016\,1,0.149\,3]$$

步骤2　隐私风险态势计算分析。根据式(3)~(20)计算结果如表4所示。

对表4分析可知:在三级指标中,除了数据隔离 T_{12}、网络监控 T_{42}、身份验证 T_{52},规章制度 T_{81} 的态势为“反势”外,其他指标的态势均为“同势”。整个三级指标中的隐私风险态势基本处于“同势”级别,这表明系统处于隐私泄露的低风险状态。如果要提高防范,可以考虑从上述四个“反势”指标着手处理。

为了对相同级别的态势进行有效区分,采用联系数势值、记分函数和精确度函数反映各态势的变化情况。势值越大,隐私风险越小;势值越小,隐私风险越大。一般情况下,当势值大于1时,隐私风险处于安全状态,可以不考虑防范处理;当势值等于1时,隐私风险处于临界状态,隐私安全需要进一步观察分析;当势值小于1时,隐私风险处于危险状态,必须考虑采取防范手段进行处理。当势值相同时,采用记分函数和精确函数进一步区分。同势值记分函数值越大,隐私风险越小,反之亦然。当势值和记分函数均相同时,通过精确函数来区分态势大小,此时精确函数值越大,隐私风险就越小;反之,精确函数值越小,隐私风险就越大。

进一步分析隐私系统的风险发展趋势,从表4中得知:在一阶潜在发展趋势上,各隐私趋势走向状态为“提

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

表4　隐私风险计算结果

风险指标	权重	隐私风险因素	五元联系数	态势	一阶偏联系数					
					一阶偏联系数	趋势	势值	风险态势	记分函数	精度函数
C_1	0.171 8	T_{11}	0.633+0.086i+0.011j+0.073k+0.267 1	同势	0.880+0.887i+0.131j+0.215k	提高	8.219	同势	1.552	1.982
		T_{12}	0.433+0.092i+0.016j+0.093k+0.450 1	反势	0.825+0.852i+0.147j+0.171k	提高	9.807	同势	1.506	1.848
		T_{13}	0.733+0.113i+0.020j+0.065k+0.133 1	同势	0.866+0.983i+0.235j+0.328k	提高	5.637	同势	1.521	2.177
		T_{14}	0.533+0.106i+0.027j+0.062k+0.333 1	同势	0.834+0.797i+0.303j+0.157k	提高	10.389	同势	1.474	1.788
C_2	0.126 1	T_{21}	0.567+0.097i+0.015j+0.085k+0.317 1	同势	0.854+0.866i+0.150j+0.211k	提高	8.152	同势	1.509	1.931
		T_{22}	0.500+0.083i+0.011j+0.080k+0.400 1	同势	0.858+0.883i+0.121j+0.167k	提高	10.425	同势	1.574	1.858
		T_{23}	0.566+0.119i+0.027j+0.098k+0.283 1	同势	0.826+0.815i+0.216j+0.257k	提高	6.385	同势	1.384	1.898
C_3	0.086 5	T_{31}	0.566+0.119i+0.027j+0.098k+0.283 1	同势	0.826+0.815i+0.216j+0.257k	提高	6.385	同势	1.384	1.898
		T_{32}	0.567+0.097i+0.015j+0.085k+0.317 1	同势	0.854+0.866i+0.150j+0.211k	提高	8.152	同势	1.509	1.931
C_4	0.168 9	T_{41}	0.767+0.102i+0.015j+0.059k+0.117 1	同势	0.883+0.872i+0.203j+0.337k	提高	5.208	同势	1.418	2.092
		T_{42}	0.367+0.088i+0.015j+0.095k+0.516 1	反势	0.807+0.854i+0.136j+0.157k	提高	10.647	同势	1.505	1.817
		T_{43}	0.600+0.109i+0.115j+0.089k+0.267 1	同势	0.846+0.487i+0.564j+0.250k	提高	5.332	同势	1.083	1.583
C_5	0.129 1	T_{51}	0.433+0.252i+0.128j+0.085k+0.417 1	同势	0.634+0.663i+0.601j+0.169k	提高	7.675	同势	1.128	1.466
		T_{52}	0.400+0.080i+0.011j+0.083k+0.500 1	反势	0.833+0.879i+0.117j+0.142k	提高	12.056	同势	1.570	1.854
		T_{53}	0.433+0.252i+0.128j+0.085k+0.417 1	同势	0.634+0.663i+0.601j+0.169k	提高	7.675	同势	1.128	1.466
C_6	0.152 2	T_{61}	0.566+0.119i+0.027j+0.098k+0.283 1	同势	0.826+0.815i+0.216j+0.257k	提高	6.385	同势	1.384	1.898
		T_{62}	0.433+0.252i+0.128j+0.085k+0.417 1	同势	0.634+0.663i+0.601j+0.169k	提高	7.675	同势	1.128	1.466
		T_{63}	0.733+0.113i+0.020j+0.065k+0.133 1	同势	0.866+0.983i+0.235j+0.328k	提高	5.637	同势	1.521	2.177
C_7	0.016 1	T_{71}	0.600+0.109i+0.115j+0.089k+0.267 1	同势	0.846+0.487i+0.564j+0.250k	提高	5.332	同势	1.083	1.583
		T_{72}	0.533+0.106i+0.027j+0.062k+0.333 1	同势	0.834+0.797i+0.303j+0.157k	提高	10.389	同势	1.474	1.788
C_8	0.149 3	T_{81}	0.400+0.010i+0.115j+0.104k+0.467 1	反势	0.976+0.080i+0.525j+0.182k	提高	5.802	同势	0.874	1.238
		T_{82}	0.533+0.106i+0.027j+0.062k+0.333 1	同势	0.834+0.797i+0.303j+0.157k	提高	10.389	同势	1.474	1.788
		T_{83}	0.566+0.119i+0.027j+0.098k+0.283 1	同势	0.826+0.815i+0.216j+0.257k	提高	6.385	同势	1.384	1.898

续表4

二阶偏联系数						三阶偏联系数				
二阶偏联系数	趋势	势值	态势	记分函数	精度函数	三阶偏联系数	趋势	势值	态势	记分函数
0.498+0.871i+0.379j	提高	1.314	微同势	0.119	0.877	0.364+0.697i	下降	0.364	反势	0.364
0.492+0.853i+0.462j	提高	1.065	微同势	0.030	0.954	0.366+0.649i	下降	0.366	反势	0.366
0.468+0.807i+0.417j	提高	1.122	微同势	0.051	0.885	0.367+0.659i	下降	0.367	反势	0.367
0.511+0.725i+0.659j	下降	0.775	微反势	−0.148	1.170	0.413+0.524i	下降	0.413	反势	0.413
0.497+0.852i+0.584j	下降	0.851	微反势	−0.087	1.081	0.368+0.593i	下降	0.368	反势	0.368
0.507+0.879i+0.580j	下降	0.874	微反势	−0.073	1.087	0.366+0.602i	下降	0.366	反势	0.366
0.503+0.791i+0.457j	提高	1.100	微同势	0.046	0.960	0.389+0.634i	下降	0.389	反势	0.389
0.503+0.791i+0.457j	提高	1.100	微同势	0.046	0.960	0.389+0.634i	下降	0.389	反势	0.389
0.497+0.852i+0.584j	下降	0.851	微反势	−0.087	1.081	0.368+0.593i	下降	0.368	反势	0.368
0.503+0.811i+0.376j	下降	1.338	微同势	0.127	0.879	0.383+0.683i	下降	0.383	反势	0.383
0.486+0.863i+0.466j	提高	1.043	微同势	0.020	0.952	0.360+0.649i	下降	0.360	反势	0.360
0.635+0.463i+0.693j	下降	0.916	强反势	−0.058	1.328	0.578+0.401i	提高	0.578	同势	0.578
0.489+0.525i+0.781j	下降	0.626	弱反势	−0.292	1.270	0.482+0.402i	提高	0.482	反势	0.482
0.487+0.883i+0.452j	提高	1.077	微同势	0.035	0.938	0.355+0.661i	下降	0.355	反势	0.355
0.489+0.525i+0.781j	下降	0.626	弱反势	−0.292	1.270	0.482+0.402i	提高	0.482	反势	0.482
0.503+0.791i+0.457j	提高	1.100	微同势	0.046	0.960	0.389+0.634i	下降	0.389	反势	0.389
0.489+0.525i+0.781j	下降	0.626	弱反势	−0.292	1.270	0.482+0.402i	提高	0.482	反势	0.482
0.468+0.807i+0.417j	提高	1.122	微同势	0.051	0.885	0.367+0.659i	下降	0.367	反势	0.367
0.635+0.463i+0.693j	下降	0.916	强反势	−0.058	1.328	0.578+0.401i	提高	0.578	同势	0.578
0.511+0.725i+0.659j	下降	0.775	微反势	−0.148	1.170	0.413+0.524i	下降	0.413	反势	0.413
0.929+0.132i+0.743j	提高	1.250	强同势	0.186	1.672	0.876+0.151i	提高	0.876	同势	0.876
0.511+0.725i+0.659j	下降	0.775	微反势	−0.148	1.170	0.413+0.624i	下降	0.413	反势	0.413
0.503+0.791i+0.457j	提高	1.100	微同势	0.046	0.960	0.389+0.634i	下降	0.389	反势	0.389

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

高",风险态势均处于"同势",这表明隐私系统风险情况良好,而且最小同势值为5.208(恶意攻击 T_{41}),其值大于1,隐私风险处于安全状态,因此不需要考虑防范处理风险问题。

对二阶潜在发展趋势分析可知:数据保密 T_{14}、数据备份 T_{21}、数据销毁 T_{22}、风险识别 T_{32}、恶意攻击 T_{41}、漏洞处理 T_{43}、内部人员 T_{51}、操作失误 T_{53}、法律遵守 T_{62}、服务锁定 T_{71}、访问控制 T_{72}、隐私处理 T_{82} 等指标趋势走向为"下降"。这表明隐私系统的风险由上一层良好状态开始逐渐减弱。而且除恶意攻击 T_{41} 的势态保持"同势"外,其余均为"反势",且势态值均小于1,说明隐私系统的风险处于危险状态。因此对恶意攻击 T_{41} 进行关注而不采取保护措施,对其他指标进行保护。保护的优先级别根据势值大小进行,由高到低依次为:漏洞处理 T_{43}、服务锁定 T_{71}(势值0.916)→数据销毁 T_{22}(势值0.875)→数据备份 T_{21}(势值0.851)→风险识别 T_{32}(势值0.850)→数据保密 T_{14}、访问控制 T_{72}、隐私处理 T_{82}(势值0.775)→内部人员 T_{51}、操作失误 T_{53}、法律遵守 T_{62}(势值0.626)。

对三阶潜在发展趋势分析可知:漏洞处理 T_{43}、内部人员 T_{51}、操作失误 T_{53}、法律遵守 T_{62}、服务锁定 T_{71}、规章制度 T_{81} 趋势走向为"提升",表明这些指标的隐私风险由上一层状态开始逐渐增强。虽然状态有所好转,但内部人员 T_{51}、操作失误 T_{53}、法律遵守 T_{62} 态势为"反势",说明趋势好转的同时这些指标处于危险状态,仍需对这些指标采取保护措施。而漏洞处理 T_{43}、服务锁定 T_{71}、规章制度 T_{81} 的态势为"同态",处于安全状态,可以关注但无需保护。

通过对上述态势、势值、记分函数、精确函数的计算和分析,说明本文提出的隐私风险态势评估方法能够科学有效地对风险指标和趋向变化进行动态预测,大大降低了隐私风险的发生。

5 结束语

本文针对隐私保护风险评估问题,采用集对分析五元偏联系数中的势值、记分函数、精确函数和态势概念及赋权理论,建立了一种最小二偏赋权的五元联系数隐私风险评估方法。该方法能够较好地对隐私风险评估指标进行动态描述,消除了隐私风险评估过程中随机、模糊、不确定等因素的干扰和影响。本文研究中采用加权平均值方法对风险指标进行处理,在完全未知的条件下对权重信息进行隐私风险评估模型的建立和求解,这给实际问题的解决带来一定局限性。如何建立多指标情况下的权重不完全问题的求解,是下一步研究的重点。

参考文献:

[1] 王元卓,范乐君,程学旗.隐私数据泄露行为分析-模型、工具与案例[M].北京:清华大学出版社,2014.

[2] 晏燕,郝晓弘,王万军.一种隐私保护度量的集对分析方法[J].武汉大学学报:工学版,2015,48(6):884-891.

[3] 方滨兴,贾焰,李爱.大数据隐私保护技术综述[J].大数据,2016(1):1-18.

[4] 王璐,孟小峰.位置大数据隐私保护研究综述[J].软件学报,2014,25(4):693-712.

[5] Jiang Qi,Khurram K M,Lu Xiang.A privacy preserving three-factor authentication protocol for e-health clouds[J].Journal of Supercomputing,2016,72(10):3826-3849.

[6] Kairouz P,Oh S,Viswanath P.The composition theorem for differential privacy[J].Computer Science,2015:1376-1385.

[7] Seidl D E,Jankowski P,Tsou M H.Privacy and spatial pattern preservation in masked GPS trajectory data[J].International Journal of Geographical Information Science,2016,30(4):785-800.

[8] Soohyung K,Hyukki L,Dohn C Y.Privacy-preserving data cube for electronic medical records:an experimental evaluation[J].International Journal of Medical Informatics,2017,97:33-42.

[9] 吴晓平,付钰.信息系统安全风险评估理论与方法[M].北京:科学出版社,2011.

[10] 付钰,吴晓平,叶清,等.基于模糊集与熵权理论的信息系统安全风险评估研究[J].电子学报,2010,38(7):1489-1494.

[11] Saripalli P,Walters B.QUIRC:a quantitative impact and risk assessment framework for cloud security[C]//IEEE International Conference on Cloud Computing,2010.

[12] 任丹丹,杜素果.一种基于攻击树的VANET位置隐私安全风险评估的新方法[J].计算机应用研究,2011,28(2):728-731.

[13] 张秋瑾.云计算隐私安全风险评估[D].昆明:云南大学,2015.

[14] Wang H,Liu F,Liu H.A method of the cloud computing security management risk assessment[M]//Advances in computer science and engineering.[S.l.]:Springer,2012:609-618.

[15] 施志坚,王华伟,王祥.基于多元联系数集对分析的航空维修风险态势评估[J].系统工程与电子技术,2016,38(3):588-593.

[16] 赵克勤.集对分析及其初步应用[M].杭州:浙江科学技术出版社,2000.

[17] 王万军.一种基于集对决策的偏联系数方法[J].甘肃联合大学学报:自然科学版,2009,23(3):43-45.

[18] ITSEC.Information technology security evaluation criteria,version1.2[S].Office for Official Publications of the European Communities,1991-06.

[19] 吴亭.五元联系数在学生成绩发展趋势分析中的应用[J].数学的实践与认识,2009,39(5):53-59.

[20] 徐泽水.直觉模糊信息集成理论及应用[M].北京:科学出版社,2008.

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net