·安全技术· 文章编号：1000-3428(2017)07-0170-05 文献标志码：A 中图分类号：TP391

互联网金融信息安全评估指标体系研究

梁 满，徐 御，李宏达，陈清明

（上海市信息安全测评认证中心，上海 200011）

摘 要： 针对互联网金融安全保障体系中的信息安全评估问题，基于《互联网金融网络与信息安全技术指引》的具体要求，参考 P2DR2 安全模型的构成要素，提出适用于互联网金融信息安全评估的指标体系。引入层次分析法确定指标结构和权重，并结合模糊综合评价法给出互联网金融信息的总体评价结果。实例应用结果表明，该指标体系可以有效地评估互联网金融的信息安全水平，具有较强的实用性。

关键词： 互联网金融；安全评估；P2DR2 安全模型；层次分析法；模糊综合评价法

中文引用格式： 梁 满，徐 御，李宏达，等. 互联网金融信息安全评估指标体系研究[J]. 计算机工程，2017，43(7)：170-174，181.

英文引用格式： Liang man，Xu Yu，Li Hongda，et al. Research on Internet Financial Information Security Evaluation Index System[J]. Computer Engineering，2017，43(7)：170-174，181.

Research on Internet Financial Information Security Evaluation Index System

LIANG Man，XU Yu，LI Hongda，CHEN Qingming

（Shanghai Information Security Testing Evaluation and Certification Center，Shanghai 200011，China）

【Abstract】 Aiming at the imformation security assessment problem of security protection system of Internet Finance，based on the specific requirements of《Internet Financial Networks and Information Security Technical Guidance》and the elements of P2DR2 security model，this paper puts forward an index system of information security evaluation for Internet Finance. Analytic Hierarchy Process（AHP） is adopted to determine index structure and weight. Combined with fuzzy comprehensive evaluation method，the overall evaluation results of Internet financial information are given. The example application results show that the proposed index system can effectively evaluate the information security level of Internet Finance，and it has stronger practicability.

【Key words】 Internet finance；security evaluation；P2DR2 security model；Analytic Hierarchy Process（AHP）；fuzzy comprehensive evaluation method

DOI： 10.3969/j.issn.1000-3428.2017.07.028

0 概述

互联网金融是传统金融与互联网相结合的新兴业务模式[1]。近几年，互联网金融以其高效便捷的服务方式和可展望的巨大经济效益得到了迅猛的发展。

随着互联网金融的快速发展，其信息安全保障问题显得越来越重要。2016 年 3 月，国内首个专门针对互联网金融行业的信息安全技术指引——《互联网金融网络与信息安全技术指引》[2]（简称《技术指引》）正式发布。为了确保互联网金融企业的业务连续性和可靠性，保证客户信息的保密性和完整性，《技术指引》认为互联网金融信息安全保障应至少包括信息安全合规性和信息安全动态保障 2 个主要方面。信息安全合规性是指互联网金融的从业机构至少要达到国家，行业发布的信息安全相关的技术标准和管理要求[3-6]，例如信息安全等级保护基本要求[3]、信息安全管理体系要求[4]、个人信息保护要求[5]等。信息安全动态保障是指要根据互联网金融各类信息系统的差异化保护要求，实现信息安全的动态保障。针对不同等级的互联网金融信息

基金项目： 2015 年度软件和集成电路产业发展专项（RX-RJJC-04-15-8601）。

作者简介： 梁 满（1979—），男，高级工程师、博士，主研方向为信息安全风险评估；徐 御、李宏达、陈清明，高级工程师、硕士。

收稿日期： 2016-06-17 **修回日期：** 2016-08-08 **E-mail：** liangman@shtec.org.cn

系统,采取不同要求的风险处理模型[6],定期开展针对互联网金融业务系统的风险评估工作,并根据评估结果制定切实有效的安全策略和措施,以消除、降低、转移高危安全风险,实现互联网金融信息安全风险管理的动态性与及时性。

互联网金融的安全评估方法概括起来可划分为定量评估和定性分析两类。前者主张用直观的数字描述评估要素和评估结果,然而完全量化的评估可能导致原本复杂的安全要素简单化、模糊化;后者主要依靠评价者的专业知识和经验做出判断分析,但评价的主观随意性较大,容易造成评价结果不够客观。在这种背景下,本文针对互联网金融风险评估的实际需要,基于最新发布的《技术指引》的具体要求,提出一种在定量评估的基础上再进行定性分析的综合评估指标体系。

1　指标体系的设计

1.1　P2DR2 安全模型

P2DR2 模型是一种典型的体现主动防御思想的安全模型[7]。《GB/Z 24364-2009 信息安全风险管理指南》[6]建议等级保护为三级以上的系统参考 P2DR2 模型。采用该模型可以帮助互联网金融机构选择合适的安全措施,避免安全保障体系设计上的漏洞。P2DR2 全模型的 5 种构成要素为指标项的设计提供了理论基础。

1.2　设计思路

《技术指引》把互联网金融信息安全保障分为安全合规性和动态保障 2 个方面。合规性要求互联网金融业务系统的技术安全防护能力不低于等级保护的技术要求,建议从业机构根据国家相关信息安全管理体系标准,结合自身安全需求制定安全策略,建立信息安全管理体系。同时,对于采集、处理、转移和使用的个人信息建议按照国家有关个人信息保护的标准进行保护。动态保障则建议互联网金融从业机构采用或者参考 P2DR2 模型进行风险控制,准确地控制和规避风险。

如表 1 所示,依据《技术指引》的具体要求,指标体系被设计为 3 个层次,把互联网金融信息安全评价分为合规安全和动态保障 2 个方面。指标项之间既相互独立,又彼此联系,满足了 P2DR2 安全模型的构成要素。

表 1　指标体系的层次结构

目标层(G)	准则层(C)	指标层(P)
互联网金融信息安全评估	合规安全(C_1)	安全策略(P_1)
		安全管理体系(P_2)
		等级保护(P_3)
		个人信息保护(P_4)
	动态保障(C_2)	漏洞扫描(P_5)
		威胁预警(P_6)
		在线监测(P_7)
		漏洞修补(P_8)
		应急响应(P_9)
		灾备恢复(P_{10})
		移动 APP 安全加固(P_{11})

2　指标体系的构造

互联网金融信息安全评估指标体系的构造使用了层次分析法和模糊综合评价法。

2.1　结构和权重

运用层次分析法[8](Analytic Hierarchy Process, AHP)确定指标结构和权重包含以下 4 个步骤:

1)建立递阶层次结构。指标体系共有 3 个层次。目标层(G):评估的总目标。准则层(C):影响安全评估实现的准则。指标层(P):评估实现的具体指标。各个层次的元素顺序以及元素间的隶属关系如表 1 所示。

2)构造判断矩阵并赋值。专家以某一层的支配元素为准则构造本层的判断矩阵,本层元素两两相比区分重要程度,并参照表 2 进行赋值[8]。

表 2　重要性标度含义

标度	重要性
1	i 与 j 重要性相同
3	i 稍微重要于 j
5	i 显著重要于 j
7	i 特别重要于 j
9	i 极度重要于 j
2,4,6,8	中间值

假定专家构造的判断矩阵 $\boldsymbol{A}=(a_{ij})_{n\times n}$,其主对角线为 1,且 $\forall i,j\in N=\{1,2,\cdots,n\}$,判断矩阵 $\boldsymbol{A}$ 满足:

$$a_{ij}>0,a_{ji}=1/a_{ij},a_{ii}=1 \tag{1}$$

3)层次单排序与一致性检验。对每一个判断矩阵 $\boldsymbol{A}$ 求解其最大特征根 $\lambda_{\max}$ 及其对应的最大特征向量 $\boldsymbol{V}=[v_1,v_2,\cdots,v_k]^{\mathrm{T}}$。对向量 $\boldsymbol{V}$ 进行列归一处理化后即为权重。假定权重向量 $\boldsymbol{W}=[w_1,w_2,\cdots,w_k]$,则对于权重向量 $\boldsymbol{W}$ 的每一个元素 $\forall i\in\{1,2,\cdots,k\}$ 都满足:

$$\boldsymbol{w}_i=\frac{v_i}{\sum_{i=1}^{k}v_i} \tag{2}$$

需要计算一致性指标 CI 来检查判断矩阵 $\boldsymbol{A}$ 是否存在不一致的情况,其计算公式如下:

$$CI=\frac{(\lambda_{\max}-n)}{(n-1)} \tag{3}$$

其中,n 为判断矩阵的阶数;$\lambda_{\max}$ 为判断矩阵的最大特征根。根据 CI 值与表 3 给出的一致性指标 RI 参考值($n=2,4,7$)计算一致性比率[8]:

$$CR=\frac{CI}{RI} \tag{4}$$

当 $CR<0.1$ 时,可认为所构造的判断矩阵 $\boldsymbol{A}$ 可用,否则需要重新构造判断矩阵 $\boldsymbol{A}$。

表 3 RI 参考值

矩阵的阶数 n	参考值
2	0.000
4	0.900
7	1.320

4)层次总排序与一致性检验。层次总排序的计算采用自上而下的方法,最终得到 P 层元素相对于 G 层的权重。假定已经获得 C 层 m 个元素相对于 G 层的权重向量 $\boldsymbol{W}^C=[w_1^C,w_2^C,\cdots,w_m^C]^{\mathrm{T}}$,且 P 层中的 n 个元素相对于 C 层第 j 个元素的层次单排序向量 $\bar{\boldsymbol{W}}_j^P=[\bar{w}_{1j}^P,\bar{w}_{2j}^P,\cdots,\bar{w}_{nj}^P]^{\mathrm{T}}$,则在向量 $\bar{\boldsymbol{W}}_j^P$ 中非隶属于 j 的元素都取值为 0。如果向量 $\bar{\boldsymbol{W}}^P=[\bar{w}_1^P,\bar{w}_2^P,\cdots,\bar{w}_n^P]$ 表示 P 层相对于 C 层的权重向量,那么 P 层相对于 G 层的权重向量为:

$$\bar{\boldsymbol{W}}_i^P=\sum_{j=1}^{m}\bar{\boldsymbol{W}}_{ij}^P\boldsymbol{W}_j^C,i=1,2,\cdots,n \tag{5}$$

假定已经获得 C 层的 j 个元素为准则的 CI_j^P,RI_j^P 和 CR_j^P,其中,$j=1,2,\cdots,m$,那么 P 层相对于 G 层的一致性指标 CI^P 可以计算为:

$$CI_j^P=(CI_1^P,CI_2^P,\cdots,CI_m^P)\cdot w^C \tag{6}$$

P 层相对于 G 层的平均随机一致性指标 RI^P 可以计算为:

$$RI_j^P=(RI_1^P,RI_2^P,\cdots,RI_m^P)\cdot w^C \tag{7}$$

P 层相对于 G 层的层次总排序的一致性比率 CR^P 可以计算为:

$$CR^P=\frac{CI^P}{RI^P} \tag{8}$$

当 $CR^P<0.1$ 时,可以认为层次总排序的结果具有较好的一致性[8]。

2.2 综合评价

模糊综合评价法[9]是借助模糊数学的隶属度理论[10]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评价对象做一个总体评价。运用该方法包含 4 个步骤:

1)确定评价对象的因素论域。假设被评价对象的 n 种评价因素表示为 $\boldsymbol{U}=\{u_1,u_2,\cdots,u_n\}$,即评价指标。根据建立的指标体系的层次结构,以准则层 C 的集合为评价对象的因素论域集合,则有 $\boldsymbol{U}=\{C_1,C_2\}$。根据指标的层次构造,每个 C_i 包含的评价因素子集分别为:

$$C_1=\{P_1,P_2,P_3,P_4\}$$
$$C_2=\{P_5,P_6,P_7,P_8,P_9,P_{10},P_{11}\} \tag{9}$$

2)确定评语结果集合。评语结果集合向量为 $\boldsymbol{V}=[v_1,v_2,\cdots,v_m]$,其中,元素 v_j 代表第 j 个评价结果。指标体系确定的评语结果集合为(即 $m=5$):

$$\boldsymbol{V}=[\text{“一星”},\text{“二星”},\text{“三星”},\text{“四星”},\text{“五星”}] \tag{10}$$

对应分数向量:

$$\boldsymbol{V}'=\{(0,20],(21,40],(41,60],(61,80],(81,100]\}$$

确定对应的评价等级标靶向量为:

$$\bar{\boldsymbol{V}}=[20,40,60,80,100]^{\mathrm{T}} \tag{11}$$

3)确定模糊关系矩阵。评价者根据指标项进行评价。统计评语结果可以得到模糊关系矩阵 $\boldsymbol{R}=(r_{ij})_{n\times m}$,其中,$r_{ij}$ 表示被评价对象从因素 u_i 来看对等级模糊子集 v_j 的隶属度;n 为因素集或者子因素集的数量;m 为评语等级集合的数量。需要对模糊关系矩阵 $\boldsymbol{R}$ 进行归一化处理,使之满足 $\sum_{j=1}^{m}r_{ij}=1$,以消除量纲的影响[9]。

4)合成模糊综合评价结果。把单因素权重向量 $\boldsymbol{W}_i$ 与单因素模糊关系矩阵 $\boldsymbol{R}_i$ 合成运算得到单因素评价结果向量:

$$\boldsymbol{B}_i=\boldsymbol{W}_i\cdot\boldsymbol{R}_i=[b_1,b_2,\cdots,b_m] \tag{12}$$

其中,元素 b_j 表示被评价对象相对于评价等级模糊子集元素 v_j 的隶属程度,需要对向量 $\boldsymbol{B}_i$ 进行归一化处理以消除量纲的影响,使之满足 $\sum_{j=1}^{m}b_{ij}=1$。如果重复使用式(12),则可以获得声明 U 中各因素子集的模糊关系矩阵 $\boldsymbol{R}_C=\begin{bmatrix}\boldsymbol{B}_1\\ \boldsymbol{B}_2\end{bmatrix}$,根据指标体系的层次结构逐层向上计算,最终可以得到 C 层相对于 G 层的综合评价结果向量 $\boldsymbol{B}_C=\boldsymbol{W}_{G-C}\cdot\boldsymbol{R}_C$。最后,把 C 层的模糊综合评价结果向量 $\boldsymbol{B}_C$ 与 $\bar{\boldsymbol{V}}$ 进行合成运算,计算互联网金融信息安全综合评价值:

$$S=\boldsymbol{B}_C\cdot\bar{\boldsymbol{V}} \tag{13}$$

根据 S 对应的等级分数区间向量 $\boldsymbol{V}'$,就可以确定被评估对象整体的信息安全水平等级。

3 实例应用

3.1 指标项权重

计算指标项权重,采用自上而下的顺序进行。首先邀请专家判断 C 层元素相对于 G 层的重要程

度。根据表 2 进行量化赋值,构造的一个 C 层元素相对于总目标层 G 层的判断矩阵:

$$\boldsymbol{A}=\begin{pmatrix}1 & 1/2\\ 2 & 1\end{pmatrix} \tag{14}$$

计算可得 $\lambda_{\max}=2$,对应的最大特征向量为:

$\boldsymbol{V}=[0.447\ 2,0.894\ 4]^{\mathrm{T}}$

由式(2)计算得到 $\boldsymbol{W}_{G-C}=[0.333\ 3,0.666\ 7]$。由式(3)和(4)可得 $CR=0$。

接下来,邀请专家判断 P 层元素 P_{1-4} 相对于 C 层元素 C_1 的重要性。根据表 2 进行量化赋值,构造一个 P 层元素 P_{1-4} 相对于 C 层元素 C_1 的判断矩阵:

$$\boldsymbol{A}=\begin{pmatrix}1 & 2 & 3 & 3\\ 1/2 & 1 & 2 & 2\\ 1/3 & 1/2 & 1 & 1\\ 1/3 & 1/2 & 1 & 1\end{pmatrix} \tag{15}$$

计算可得 $\lambda_{\max}=4.010\ 4$,对应的最大特征向量为:$\boldsymbol{V}=[0.809\ 9,0.467\ 4,0.250\ 5,0.250\ 5]^{\mathrm{T}}$。

由式(2)计算 P 层元素 P_{1-4} 相对于 C 层元素 C_1 的权重向量为 $\boldsymbol{W}_{C_1-P_{1-4}}=[0.455\ 4,0.262\ 8,0.140\ 9,0.140\ 9]$。由式(3)和式(4)计算 $CR=0.003\ 5/0.9=0.003\ 9<0.1$,可以认为所构造的判断矩阵式(15)具有较好的一致性。

同样地,邀请专家判断 P 层元素 P_{5-11} 相对于 C 层元素 C_2 的重要程度并构造判断矩阵如下:

$$\boldsymbol{A}=\begin{pmatrix}1 & 3 & 3 & 1 & 1/3 & 1/2 & 2\\ 1/3 & 1 & 1/2 & 1/3 & 1/4 & 1/4 & 2\\ 1/3 & 2 & 1 & 1/3 & 1/3 & 1/3 & 2\\ 1 & 3 & 3 & 1 & 1/3 & 1/3 & 3\\ 3 & 4 & 3 & 3 & 1 & 1 & 5\\ 2 & 4 & 3 & 3 & 1 & 1 & 5\\ 1/2 & 1/2 & 1/2 & 1/3 & 1/5 & 1/5 & 1\end{pmatrix} \tag{16}$$

计算可得 $\lambda_{\max}=7.273\ 3$,对应最大特征向量为:$\boldsymbol{V}=[0.306\ 7,0.171\ 9,0.307\ 4,0.635\ 0,0.592\ 8,0.103\ 9]^{\mathrm{T}}$。

由式(2)计算得到权重向量 $\boldsymbol{W}_{C_2-P_{5-11}}=[0.136\ 5,0.057\ 2,0.076\ 5,0.136\ 9,0.282\ 7,0.263\ 9,0.046\ 2]$。由式(3)和式(4)计算 $CR=0.045\ 6/1.32=0.003\ 9<0.1$,可以认为判断矩阵 $\boldsymbol{A}$ 具有较好的一致性。

接下来,需要确定所有指标项相对于评估总目标的层次总排序。也就是说,需要计算 P 的所有元素相对于总目标 G 层的层次总排序,由式(5)计算层次总排序的权重向量为:$\boldsymbol{W}_{G-P_{1-11}}=[0.151\ 8,0.087\ 6,0.047\ 0,0.047\ 0,0.091\ 0,0.038\ 1,0.051\ 0,0.091\ 3,0.188\ 5,0.175\ 9,0.030\ 8]$。

然后,需要对层次总排序的结果进行一致性检验。层次总排序的一致性检验参数值如表 4 所示。

表 4　总排序的一致性检验参数

参数名称	参数值
元素权重 W_i^C	$W_1^C=0.333\ 3$ $W_2^C=0.666\ 7$
一致性指标 CI_i^P	$CI_1^P=0.003\ 5$ $CI_2^P=0.045\ 6$
一致性比率 CR_i^P	$CR_1^P=0.003\ 9$ $CR_2^P=0.034\ 5$
随机一致性指标 RI_i^P	$RI_1^P=0.9$ $RI_2^P=1.32$

根据式(6),计算 $CI^P=\sum_{i=1}^{2}CI_i^PW_i^C=0.031\ 6$。根据式(7),计算 $RI^P=\sum_{j=1}^{2}RI_j^PW_j^C=1.180\ 0$。根据式(8),计算总排序 $CR^P=\dfrac{CI^P}{RI^P}=0.026\ 8<0.1$,可认为层次总排序结果具有较好的一致性,总排序权重结果合理。

3.2　定性评价与定量评价

邀请 6 名专业测评人员对某金融机构的信息安全整体水平进行综合评价,汇总评价结果如表 5 所示。

表 5　测评人员评价结果汇总统计

指标项	一星	二星	三星	四星	五星
P_1	0	0	0	1	5
P_2	0	0	0	1	5
P_3	0	0	0	2	4
P_4	0	0	1	3	2
P_5	0	0	1	2	3
P_6	0	0	1	3	2
P_7	0	0	0	2	4
P_8	0	0	0	1	5
P_9	0	0	0	1	5
P_{10}	0	0	0	3	3
P_{11}	0	0	0	2	4

根据式(12),把通过层次分析法得到的指标层元素 P_{1-4} 相对于目标层 G 的层次总排序权重 $\boldsymbol{W}_{G-P_{1-4}}$ 与单因素模糊关系矩阵 $\boldsymbol{R}_{C_1}$ 合成运算,得到单因素评价结果向量:

$$\begin{aligned}\boldsymbol{B}_{C_1}&=\boldsymbol{W}_{G-P_{1-4}}\cdot\boldsymbol{R}_{C_1}\\&=\begin{bmatrix}0.151\ 8\\ 0.087\ 6\\ 0.047\ 0\\ 0.047\ 0\end{bmatrix}^{\mathrm{T}}\cdot\begin{bmatrix}0 & 0 & 0 & 0.166\ 7 & 0.833\ 3\\ 0 & 0 & 0 & 0.166\ 7 & 0.833\ 3\\ 0 & 0 & 0 & 0.333\ 3 & 0.666\ 7\\ 0 & 0 & 0.166\ 7 & 0.500\ 0 & 0.333\ 3\end{bmatrix}\\&=[0\quad 0\quad 0.023\ 5\quad 0.237\ 2\quad 0.739\ 3]\end{aligned}$$

同理,把通过层次分析法得到的指标层元素 P_{5-11} 相对于目标层 G 的层次总排序权重 $\boldsymbol{W}_{G-P_{5-11}}$ 与单因素模糊关系矩阵 $\boldsymbol{R}_{C_2}$ 合成运算,得到 $\boldsymbol{B}_{C_2}$ 如下:

$$\boldsymbol{B}_{C_2}=\boldsymbol{W}_{G-P_{5-11}}\cdot\boldsymbol{R}_{C_2}$$

$$=\begin{bmatrix}0.091\,0\\0.038\,1\\0.051\,0\\0.091\,3\\0.188\,5\\0.175\,9\\0.030\,8\end{bmatrix}^{\mathrm{T}}\cdot\begin{bmatrix}0&0&0.166\,7&0.333\,3&0.500\,0\\0&0&0.166\,7&0.500\,0&0.333\,3\\0&0&0&0.333\,3&0.666\,7\\0&0&0&0.166\,7&0.833\,3\\0&0&0&0.166\,7&0.833\,3\\0&0&0&0.500\,0&0.500\,0\\0&0&0&0.333\,3&0.666\,7\end{bmatrix}$$

$$=[0\quad 0\quad 0.032\,3\quad 0.316\,9\quad 0.650\,8]$$

由 $\boldsymbol{B}_{C_1}$ 和 $\boldsymbol{B}_{C_2}$ 得到 C 层相对于 G 层的模糊关系矩阵：

$$\boldsymbol{R}_C=\begin{bmatrix}\boldsymbol{B}_{C_1}\\\boldsymbol{B}_{C_2}\end{bmatrix}=\begin{bmatrix}0&0&0.023\,5&0.237\,2&0.739\,3\\0&0&0.032\,3&0.316\,9&0.650\,8\end{bmatrix}$$

根据指标体系的层次结构逐层向上计算，最终得到 C 层相对于 G 层的模糊综合评价结果向量为：

$$\boldsymbol{B}_C=\boldsymbol{W}_{G-C}\cdot\boldsymbol{R}_C$$

$$=\begin{bmatrix}0.333\,3\\0.666\,7\end{bmatrix}^{\mathrm{T}}\cdot\begin{bmatrix}0&0&0.023\,5&0.237\,2&0.739\,3\\0&0&0.032\,3&0.316\,9&0.650\,8\end{bmatrix}$$

$$=[0\quad 0\quad 0.029\,4\quad 0.290\,3\quad 0.680\,3]$$

最后，根式(13)计算互联网金融信息安全综合评价值为：

$$S=\boldsymbol{B}_C\cdot\bar{\boldsymbol{V}}=\begin{bmatrix}0\\0\\0.029\,4\\0.290\,3\\0.680\,3\end{bmatrix}^{\mathrm{T}}\cdot\begin{bmatrix}20\\40\\60\\80\\100\end{bmatrix}=93.018\,0$$

4 相关讨论

可以发现 $S\in(81,100]$，即 $S\in V_5'$，对应的评语为“五星”，它反映某互联网金融机构的整体信息安全水平较高。本文所提出的指标体系使评估人员能够比较精确地分析安全存在的具体问题。例如，通过分析 C 层相对于 G 层的模糊综合评价结果向量 $\boldsymbol{B}_C$，可以发现评语为“三星”和“四星”的比重分别为 0.029 4 和 0.290 3，根据隶属度理论，这反映了约有 31.97% 评估指标项可以被改进。

值得注意的是，本文所提出的评估方法在实际应用中并不一定需要较多的专家人力介入，完全可以由一名专家独立完成权重计算和评价过程(此时等价于线性加权和法)。本文邀请多名专家参与，主要是为了使评价的结果更客观、更公正，最大程度上避免由一名专家单独评价时可能产生的主观偏差，这点在指标体系的实际实用中已经得到了证实。

5 相关研究对比分析

信息安全评估是信息系统安全的基础和前提[11]。目前，安全评估方法大致可以分为 2 类[12]：1)定量的评估，主要利用直观数字来表达评估结果，可以使评估结果更科学、更客观，然而互联网金融的安全因素十分复杂，有些安全因素难以被完全量化；2)定性的评估，主要依据评估者的经验和知识做出主观判断，可以弥补定量评估的缺点，使评估的结果更全面、更深入，然而该方法主要依赖评估者的主观性，对评估者的经验和能力要求较高。本文提出的评估方法结合了目前两种评估方法各自的优点，主张在定量分析的基础上，再进行定性的评价，这样可以充分利用到专家的经验和知识，同时最大程度上避免在评估过程中的主观随意性。

与文献[13]提出的基于等级保护的有效风险评估方法相比，本文提出的指标体系基于最新发布的《互联网金融网络与信息安全技术指引》，并参考了 P2DR2 模型的构成要素，因此更能反映互联网金融信息安全的特点。此外，前者对于所提出的评估方法的实际应用没有进行讨论，而本文对所提出的评估方法进行了实例验证。

文献[14]提出了一种利用风险矩阵进行操作系统风险等级评估的模型，主张将风险评估由定性分析完全转化为定量的评价。与完全定量的评估方法相比，本文提出的评估方法采用的是在定量分析的基础上再进行定性分析，可以有效避免有些安全风险因素被量化以后可能产生的误解和曲解。

文献[15]通过德尔菲法构建了一个云计算安全评估模型，可以针对云平台的安全能力进行量化和评估。然而，其评估指标的数量庞大，计算过程相对复杂，影响了实用性和对一般性应用环境的推广。与文献[15]评估方法相比，本文提出的指标体系建模过程简单，计算方便，评价效率高，可以很容易地被推广到一般的应用场景。

6 结束语

基于最新发布的《互联网金融网络与信息安全技术指引》的具体要求，本文提出一种定量评估与定性评估相结合的互联网金融信息安全指标体系。实例应用结果表明，该指标体系具有建模过程简单、计算方便、评价效率高等优点。下一步将改进评估模型，最大程度降低评估过程中的人为主观性对最终评估结果的影响。

(下转第 181 页)

参考文献

[1] 张　玲,白中英,罗守山,等. 基于粗糙集和人工免疫的集成入侵检测模型[J]. 通信学报,2013,34(9):166-176.

[2] Li M. Change Trend of Averaged Hurst Parameter of Traffic Under DDOS Flood Attacks[J]. Computers & Security,2006,25(3):213-220.

[3] Wang W, Guyet T, Quiniou R, et al. Autonomic Intrusion Detection: Adaptively Detecting Anomalies over Unlabeled Audit Data Streams in Computer Networks[J]. Knowledge-based Systems, 2014, 70: 103-117.

[4] 赵曦滨,井然哲,顾　明. 基于粗糙集的自适应入侵检测算法[J]. 清华大学学报(自然科学版),2008,48(7):1165-1168.

[5] 唐成华,刘鹏程,汤申生,等. 基于特征选择的模糊聚类异常入侵行为检测[J]. 计算机研究与发展,2015,52(3):718-728.

[6] Saxena H, Richariya V. Intrusion Detection in KDD99 Dataset Using SVM-PSO and Feature Reduction with Information Gain[J]. International Journal of Computer Applications,2014,98(6):25-29.

[7] 李丹丹,田春伟,李佰洋,等. 基于子空间聚类的网络流量分类方法[J]. 哈尔滨理工大学学报,2015,20(2):63-68.

[8] Lin W C, Ke S W, Tsai C F. CANN: An Intrusion Detection System Based on Combining Cluster Centers and NearestNeighbors[J]. Knowledge-based Systems, 2015,78(1):13-21.

[9] Reynolds R G. An Introduction to Cultural Algorithms[C]//Proceedings of the 3rd Annual Conference on Evolutionary Programming. San Diego, USA: World Scientific,1994:131-139.

[10] 郭一楠,巩敦卫. 双层进化交互式遗传算法的知识提取与利用[J]. 控制与决策,2007,22(12):1329-1334.

[11] Coello C A C, Becerra R L. Evolutionary Multiobjective Optimization Using a Cultural Algorithm [C]// Proceedings of IEEE Swarm Intelligence Symposium. Washington D. C., USA: IEEE Press,2003:6-13.

[12] 郭一楠,王　辉,程　建. 自适应免疫克隆选择文化算法[J]. 电子学报,2010,38(4):966-972.

[13] Sengupta N, Sen J, Sil J, et al. Designing of On-line Intrusion Detection System Using Rough Set Theory and Q-learning Algorithm [J]. Neurocomputing, 2013, 111(6):161-168.

[14] Lashin E F, Kozae A M, Khadra A A A, et al. Rough Set Theory for Topological Spaces[J]. International Journal of Approximate Reasoning,2005,40(12):35-43.

[15] Chang R K C. Defending Against Flooding-based Distributed Denial-of-Service Attacks: A Tutorial[J]. IEEE Communications Magazine,2002,40(10):42-51.

编辑　刘　冰　索书志

(上接第 174 页)

参考文献

[1] 谢　平,邹传伟. 互联网金融模式研究[J]. 金融研究,2012(12):11-22.

[2] 上海金融信息行业协会. 互联网金融网络与信息安全技术指引[EB/OL]. (2010-11-21). https://www.watchf.cn/.

[3] 公安部等级保护评估中心. 信息安全等级保护基本要求[EB/OL]. (2008-11-01). http://www.djbh.net/webdev/web/PolicyStandardsAction.do?p=getJcbz&id=402886e4353223cb013551fa78170050.

[4] 公安部等级保护评估中心. 信息系统安全管理要求[EB/OL]. (2006-05-31). http://www.djbh.net/webdev/web/PolicyStandardsAction.do?p=getJcbz&id=402886e4353223cb0135520045ce0055.

[5] 中国软件测评中心,中国电子技术标准化研究院,中国信息安全测评中心. 公共及商用服务信息系统个人信息保护指南[EB/OL]. (2012-11-05). http://www.pipa.gov.cn/NewsDetail.asp?ID=1002.

[6] 国家信息中心信息安全研究与服务中心,中国电信股份有限公司北京研究院. 信息安全风险管理指南[EB/OL]. (2009-12-01). https://wenku.baidu.com/view/52d4c724ccbff121dd368377.html.

[7] 康　维. 网络安全体系结构[M]. 田　果,刘丹宁,译. 北京:人民邮电出版社,2007.

[8] Satty T. L. How to Make a Decision: The Analytic Hierarchy Process [J]. European Journal of Operational Research,1990(48):9-26.

[9] 汪培庄. 模糊系统理论与模糊计算机[M]. 北京:科学出版社,1996.

[10] Zimmermann H J. Fuzzy Set Theory and its Applications[M]. Berlin, Germany: Springer,1996.

[11] 冯登国,张　阳,张玉清. 信息安全风险评估综述[J]. 通讯学报,2004,25(7):10-18.

[12] 范　红,冯登国,吴亚非. 信息安全风险评估方法与应用[M]. 北京:清华大学出版杜,2006.

[13] 李　杨,聂晓伟,杨鼎才. 一个基于等级保护的有效风险评估方法[J]. 计算机应用研究,2005,22(7):39-41.

[14] 邓　平,范科峰,张素兵,等. 一种安全操作系统风险评估模型[J]. 计算机工程,2011,37(9):57-58.

[15] 姜政伟,赵文瑞,刘　宇,等. 基于等级保护的云计算安全评估模型[J]. 计算机科学,2013,40(8):151-156.

编辑　刘　冰　陆燕菲