基于等级保护的云计算安全评估模型

姜政伟[1,2] 赵文瑞[1,2] 刘 宇[1,2] 刘宝旭[2]

(中国科学院研究生院 北京 100049)[1] (中国科学院高能物理研究所计算中心 北京 100049)[2]

摘 要 云计算应用与发展中最受关注的问题之一是安全。针对云计算服务安全水平量化的需求,以我国等级保护测评要求为基础,借鉴欧美相关机构的云计算风险控制与安全评估框架,通过德尔菲法构建云计算安全评估指标体系,使用层次化分析法计算出各指标项的权重。根据设计的指标体系,将模糊综合评判引入对云计算实例的分析。实际应用表明模型能为云平台安全提供有效的量化和与评估。

关键词 云计算,安全评估,等级保护,层次分析法,模糊综合评价

中图法分类号 TP393 **文献标识码** A

Model for Cloud Computing Security Assessment Based on Classified Protection

JIANG Zheng-wei[1,2] ZHAO Wen-rui[1,2] LIU Yu[1,2] LIU Bao-xu[2]

(Graduate University, Chinese Academy of Sciences, Beijing 100049, China)[1]

(Computing Center of Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, China)[2]

Abstract The security topic in application and development of cloud computing is one of the greatest concerns. Aiming at the requirement of security level quantification in cloud computing service, based on classified protection in our country and learned from the cloud computing risk control and security assessment frameworks designed by European and American institutions, a cloud computing security assessment indexes system was built up through Delphi method, and the weight of each index was calculated with analytic hierarchy process. According to this indexes system, fuzzy comprehensive analysis method was introduced to the evaluation of a cloud computing instance. The case study shows that this model can effectively quantify and assess the security level of cloud platform.

Keywords Cloud computing, Security assessment, Classified protection, Analytic hierarchy process, Fuzzy comprehensive evaluation

1 引言

云计算作为一种对基于网络的、可配置的共享计算资源池进行方便、随需访问的服务模式,具有诸多优点,如能获得规模化的效益,实现快速、智能的资源扩展。目前,云计算得到了广泛的应用,国内外已有不少较为成熟的云计算平台,基础设施即服务如亚马逊公司的弹性计算云,平台即服务如谷歌的 App Engine、微软的 Azure,软件即服务如 Salesforce 公司的 Sales Cloud 等;国内也有些公司在提供商业化的云计算服务,如盛大云、阿里云、新浪云等。

云计算的发展与应用存在众多挑战,而安全一直是首当其冲的问题。近年来,亚马逊、谷歌、微软等大型云服务商发生了各种安全事故,更增加了人们的疑虑。因此,要大规模地应用云计算技术,必须解决云计算的安全问题。

云计算面临的安全挑战之一是建立以安全目标验证、安全服务等级测评为核心的云计算安全标准及其测评体系[1]。研究、设计适合云计算平台的安全评估指标体系,使之既为云服务商的安全建设提供重要参考,也有利于第三方机构的评估与审计。根据指标体系进行科学的量化评估,能合理地评价平台的安全服务水平,为云用户提供直观的平台选择依据。

本文基于《GB/T 22239-2008 信息安全等级保护基本要求》[2]的指标体系,借鉴欧美信息安全或标准化机构对云计算风险控制与安全评估的框架设计,使用德尔菲法构建适用于云平台的安全评估指标体系,通过层次化分析法确定各指标项的权重,最后以模糊综合评价法计算云计算实例的安全指数,验证提出的评估模型的有效性。

2 相关研究

文献[3,4]讨论了基于等级保护的风险评估方法,但缺乏实例分析。类似于文献[5]的一些学位论文研究了信息安全等级保护体系及其应用,但对指标体系的裁剪与思考较少。文献[6,7]将层次分析与模糊综合评价应用于信息安全的量

到稿日期:2012-10-25 返修日期:2013-03-01 本文受国家科技支撑计划项目(2012BAH14B02),国家发改委信息安全专项项目(发改办高技[2012]1424号)资助。

姜政伟(1985-),男,博士生,主要研究方向为云计算安全与风险评估,E-mail:jiangzw@ihep.ac.cn;赵文瑞(1988-),女,硕士生,主要研究方向为云计算;刘 宇(1984-),男,博士生,主要研究方向为信息安全;刘宝旭(1972-),男,研究员,博士生导师,主要研究方向为计算机网络与信息安全。

化评估，针对性很强。

在指标体系的设计方面，文献[8]提出了一个多维的信息安全指标体系，但构造的度量指标相对简单、模糊。具体到云计算，欧盟网络与信息安全局 ENISA 于 2009 年提出了云计算中的信息安全保障框架 IAF[9]，以 10 个一级指标、69 个二级指标、130 多个三级指标来保障云计算平台的安全。美国 2010 年开始的联邦政府风险和授权管理项目 FedRAMP[10]，通过 17 个大类、158 个二级指标规定了对云计算安全控制措施的要求，目的是为云计算服务和产品提供标准的评估和授权方法。云安全联盟 CSA 于 2010 年发布了云控制矩阵 CCM[11]，提供了要求云服务商满足的基本安全原则，帮助客户评价供应商的安全性，同时 CSA 还设计了云计算一致性评估问卷 CAIQ[12]，把评估分为 11 类一级指标、103 个二级指标、212 个三级指标，以表格的形式提供大量的是/否问题，帮助审查供应商的资质。

关于云计算中的安全风险评估研究，文献[13]把典型的攻击与事件映射到 6 个关键的安全对象，使用德尔菲法收集风险评估所需信息，建立对应的风险评估知识库，提出一个云计算平台中风险与影响的量化评估框架，但文中使用的指标项云计算特点不显著，没有真实的云计算平台实例分析。文献[14]与文献[15]设计和实现了一个能识别、评估、削减、监控云计算平台风险的框架，其识别的风险包括法律、技术、策略及一般 4 类，但未实现对各类风险的分析与分步评估。

除了文献[9-12]对云计算中安全风险评估的指标框架设计之外，针对云平台安全评估的指标体系研究还很少，尚未发现基于云计算特色的指标体系对云服务的安全水平进行量化评估的研究。

3 云计算安全评估指标体系设计

指标是评估的工具，是反映对象属性的指示标志。指标体系则是根据评估目标与评估内容的要求构建的一组相关指标，据此搜集评估对象的有关信息资料，反映评估对象的基本面貌、特征和水平。指标体系是对云计算进行安全评估的重要依据，其设计是本文的重要工作之一。

3.1 指标设计原则

建立云计算安全评估指标体系是一项相当复杂的工作，一方面，选取的指标应能涵盖云计算的各个安全因素，使最终评估结果能全面反映真实状况；另一方面，云计算涉及的因素纷繁复杂，指标项越多，确定评估指标的重要性顺序就越难，处理和建模的过程就越复杂，扭曲系统本质特性的可能性就越大。为提高效率，保证可行性，建立云计算安全评估指标体系应遵守下述设计原则[16]：

1)科学性与系统性。指标的选取应建立在对云计算安全的科学研究基础之上，符合国家有关信息和信息系统安全的法律和法规，综合考虑影响平台的诸多因素，定性与定量分析相结合，以正确反映系统整体和内部相互关系的数量特征。

2)层次性和独立性。指标体系应按照属性的不同，进行综合与分解，将其分为不同的层次。而每层次的指标应是相互独立的，尽量避免指标间的交叉、包含关系，使得每个指标可以独立地评估系统的某项内容，从而从不同方面反映云计算安全的实际情况。

3)可比性与可操作性。指标体系的可比性越强，评价结果的可信度就越大。云计算安全具有多重属性，有些因素难以量化。因此指标的设计要客观实际，保持同标准，以保证指标间的可比性。此外，指标体系要符合实际评测工作的需要，易于操作和测评，数据资料应便于收集与计算机处理。

3.2 以等级保护测评准则为指标基础

信息安全等级保护是指对国家安全、法人和其它组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置[17]。

云计算平台具有信息系统的共性，仍可使用等级保护来保障平台的安全[18]。作为特殊的信息系统，云计算平台的安全可以分为技术与管理两方面，前者可包括物理环境、网络、主机系统、应用与数据，后者可包括制度、机构、人员、系统建设与运维等。云计算的安全既是复杂的技术过程，也是综合性的社会系统过程，可通过一系列的技术手段，按照社会化的组织、管理原则，实现云计算平台安全的设计、防护与评估。而我国的信息系统等级保护体系分为管理与技术两部分，发展较为成熟，规范较全面，对云计算有较好的适用性。

3.3 安全评估指标体系结构

由于云计算安全评估涉及面很广，不确定因素很多，仅凭几名决策者无法完成分析与设计任务，必须借助各方面专家的知识与经验完成。因此，本文利用德尔菲法来建立云计算安全评估指标体系[19]。基本流程如下：

第 1 步　选择风险评估、分布式与云计算研究、社会管理等领域的多名专家。以《GB/T 22239－2008 信息安全等级保护基本要求》为基础，借鉴 ENISA 的 IAF[9]、美国 FedRAMP[10]以及 CSA 的 CAIQ[11]中对风险控制与安全评估的指标设计，结合我国国情与云计算实践经验，设计第一轮云计算安全评估指标体系调查表，收集专家认为影响云平台安全的因素。

第 2 步　回收第一轮调查表，汇总制定第二轮调查表。从第一轮调查表反馈的信息可知专家认可的云计算中更重要的安全技术评估项是隔离机制、虚拟机保护机制、身份鉴别机制、数据移植方案，安全管理评估项是供应链管理、应急预案管理、法规需求管理、服务水平协议 SLA 管理。

第 3 步　重复第 2 步工作，进行多轮的信息收集与框架修改，直到大多数专家反映所构建的指标体系符合 3.1 节的指标设计原则。

基于等级保护的云计算安全评估指标体系的最终结构如图 1 所示。

该指标体系共有 4 层，把云计算安全评估分为技术要求与管理要求两大类：技术要求包括物理安全、网络安全、主机系统安全、应用安全、数据安全、备份恢复与数据移植；管理要求包括安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理、服务水平协议管理。第 4 层共有 72 个指标项，比较全面地涵盖了云平台安全评估的主要因素。

这个指标体系以等级保护为基础，进行了裁剪、增删、修改以满足云计算安全评估的需要。图 1 中粗斜体字所示为具有云计算特色或者云计算中更重要的评估项，这些项目主要分析文献[9,10,12]和专家的总结。例如，虚拟机技术是云平

台的关键技术，所以在主机系统安全下添加虚拟机保护项；平台的对外接口或 API 函数存在漏洞，数据被特定云平台锁定，法规遵从是云计算中的主要风险[20,21]，所以对应地添加了代码与接口安全，数据移植，法律、规范需求管理项；云计算平台中资源共享的风险，可能存在有恶意企图的内部人员，计算资源被不法分子利用，容易成为黑客攻击特别是拒绝服务的目标，云计算平台涉及多个供应商[21,22]，所以着重强调了结构安全与隔离、人员录用、安全意识教育与培训、应用资源鉴别、安全应急预案管理、外包商开发管理项的评估；服务水平协议是云服务商与租户互通以及服务保障的关键依据，所以在管理要求下专门增添了服务水平协议管理项，并从 5 个方面评估 SLA 的管理[23]。

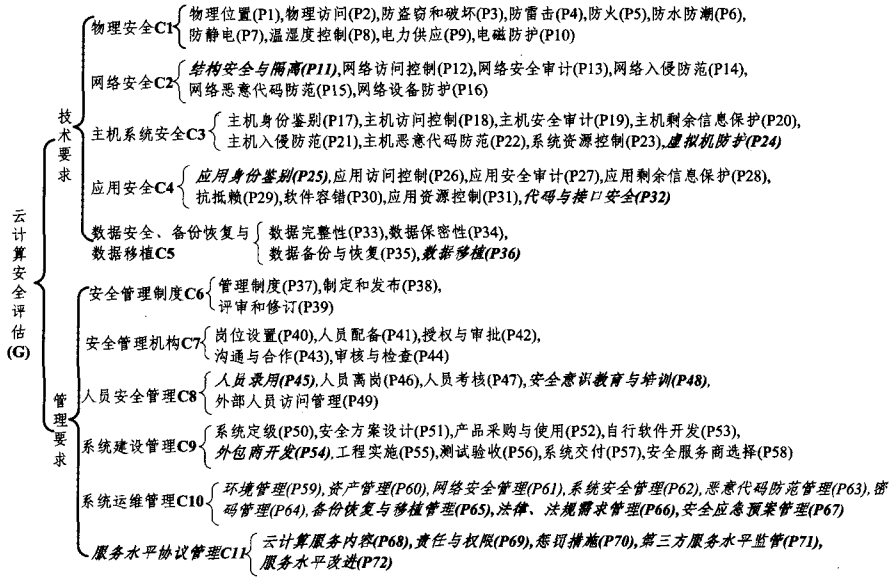

图 1　云计算安全评估指标体系示意图

4　基于 AHP 的模糊综合评价算法

4.1　层次分析法

AHP(Analytic Hierarchy Process)层次分析法[24]是美国运筹学家 T. L. Satty 教授提出的一种定性与定量相结合的多目标、层次化权重决策分析方法。AHP 为相互关联、相互制约、难于完全定量处理的复杂问题提供了一种简单实用的分析方法。AHP 算法基本步骤如下：

1)构造递阶层次结构模型 G-C-P。把 3.3 节设计的云计算安全评估指标体系分为 3 层，其中，最高层是目标层 G(Goal)-云计算安全评估的总体目标；中间层是准则层 C(Criterion)，共 11 项；各准则下是方案层 P(Plan)或指标层，即进行安全评估的具体方案，是影响目标实现的 72 类最底层因素。

表 1　Satty 9 级分制

标度	含义
1	两因素相比，同等重要
3	两因素相比，前者比后者稍重要
5	两因素相比，前者比后者明显重要
7	两因素相比，前者比后者强烈重要
9	两因素相比，前者比后者极端重要
2,4,6,8	表示上述判断的中间值
倒数	相应两因素交换次序比较的重要性

2)建立判断矩阵。对于同一层次的各元素，以相邻上一层支配元素为准则，使用德尔菲法，请专家参照表 1 的 Satty 9 级分制两两比较相对重要性，得出相对权值的比值 ω_i/ω_j，以此建立一个判断矩阵 A，如式(1)所示：

$$A=\begin{pmatrix} 1 & \omega_1/\omega_2 & \cdots & \omega_1/\omega_n \\ \omega_2/\omega_1 & 1 & \cdots & \omega_2/\omega_n \\ \vdots & \vdots & \ddots & \vdots \\ \omega_n/\omega_1 & \omega_n/\omega_1 & \cdots & 1 \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_m \end{pmatrix} \quad (1)$$

A 为 $n\times n$ 方阵，主对角线为 1，具有如下性质：

$\forall i,j\in N\triangleq\{1,2,\cdots,n\}$，有

$$a_{ij}>0,a_{ij}=1/a_{ji},a_{ii}=1 \quad (2)$$

3)层次单排序及一致性检验。对每一个判断矩阵求解最大特征根 λ_{max} 及对应的最大特征向量 W，进而得出针对上层某一准则的各元素相对权重，之后做一致性检验。根据需要，本文采用和积法计算 λ_{max} 与 W 的近似值。

a)对 A 按列规范化：

$$\overline{a_{ij}}=a_{ij}/\sum_{i=1}^{n}a_{ij}\ (i,j=1,2,\cdots,n) \quad (3)$$

b)将规范化后的判断矩阵按行相加：

$$\bar{\omega}_i=\sum_{j=1}^{n}\overline{a_{ij}}\ (i=1,2,\cdots,n) \quad (4)$$

c)对向量 $W=\{\bar{\omega}_1,\bar{\omega}_2,\cdots,\bar{\omega}_n\}^T$ 规范化：

$$\omega_i=\bar{\omega}_i/\sum_{i=1}^{n}\bar{\omega}_i \quad (5)$$

则 $W=\{\omega_1,\omega_2,\cdots,\omega_n\}^T$ 即为最大特征向量的近似值。

d)利用最大特征向量求最大特征根的近似值：

$$\lambda_{max}=\frac{1}{n}(AW)_i/\omega_i \quad (6)$$

式中，$(AW)_i$ 为矩阵 A 与 W 乘积向量的第 i 个元素。

当因素较多时，由专家经验给出的两两比较的主观判断矩阵计算最大特征向量与最大特征根可能发生不一致的情况，这需要由 λ_{max} 检验 A 是否存在严重的非一致性。为此，使用 Satty 定义的一致性检验指标 CI：

$$CI=(\lambda_{max}-n)/(n-1) \quad (7)$$

式中，n 为 A 的阶数，CI 越小，说明一致性越高。为判断矩阵是否具有满意的一致性，可将 CI 与平均随机一致性指标 RI 相比，得到随机一致性比率 CR：

$$CR=CI/RI \quad (8)$$

本文使用 Satty 给出的 1－12 阶 RI 参考值，如表 2 所列。

表 2　随机一致性指标 RI 参考值

n	1	2	3	4	5	6
RI	0	0	0.58	0.90	1.12	1.24
n	7	8	9	10	11	12
RI	1.32	1.41	1.45	1.49	1.51	1.54

一致性检验中，当 $CR<0.1$ 时，可认为判断矩阵具有满意的一致性，求得的权重可用，否则就需要对判断矩阵进行合理调整后再做上述处理。

4)层次总排序及一致性检验。通过第 3)步得到的是某一层元素对于其上一层中某支配元素的权重向量，为得到最底层各方案指标 P_k 对于总目标 G 的重要性排序，根据 AHP 理论，需要自上而下依次计算同一层次中所有因素对于最高层目标的排序权重值。对于 GCP 层次结构，准则层 C 的 m 个元素：$C_1,C_2,\cdots,C_m$ 对目标 G 的排序为 $c_1,c_2,\cdots,c_m$。方案指标层 P 的 n 个元素对上层 C 中某个因素为 C_j 的单准则排序为 $p_{1j},p_{2j},\cdots,p_{nj}$ $(j=1,2,\cdots,m)$，若 P_j 与 C_j 无关，$p_{kj}=0$ $(1\leqslant k\leqslant n)$。计算 P 层第 i 个元素对 G 的层次总排序权值：

$$p_i=\sum_{j=1}^{m}c_j p_{ij}\ (i=1,2,\cdots,n) \tag{9}$$

P 层元素对于总目标 G 的排序权重向量为：

$$W_{G-P}=(p_1,p_2,\cdots,p_n)^{\mathrm{T}} \tag{10}$$

层次总排序也需要通过下式进行一致性检验：

$$CR=\sum_{j=1}^{m}p_j CI_j/\sum_{j=1}^{m}p_j RI_j \tag{11}$$

式中，CI_j 为 P 层各元素对上层 C 层的元素 C_j 的层次单排序一致性指标，RI_j 为对应阶的随机一致性指标，CR 为最底层 P 对目标 G 的总排序随机一致性比率。当 $CR<0.1$ 时，通过一致性检验，组合权重可以作为最终决策的依据，否则要重新考虑层次模型或者重新构造一致性 CR 较小的成对比较矩阵。

4.2　模糊综合评价法

模糊综合评价法源于美国控制论专家 Zadeh L. A. 的模糊集理论(Fuzzy sets)[25]，它使用模糊关系合成原理，对具有多种属性、属性间边界不清、难以定量的事物进行合理综合与总体评判。

为表示某一元素与模糊子集的关系，模糊综合评价法引入隶属度概念。隶属度用闭区间[0,1]中的一个数字表示，隶属度值越接近 1，则表示当前元素对模糊子集的隶属程度越高，反之亦然。

模糊综合评价的基本步骤如下：

1)建立因素集。本文以层次分析法识别的安全评估的准则层集合为因素集 $U=\{C_1,C_2,\cdots,C_m\}$，其中各单因素子集 C_i 分别为：

$$\begin{aligned}&C_1=\{P_1,P_2,\cdots,P_{10}\}\\&C_2=\{P_{11},P_{12},\cdots,P_{16}\}\\&\quad\vdots\\&C_{11}=\{P_{68},P_{69},\cdots,P_{72}\}\end{aligned} \tag{12}$$

2)建立评价集。评判者对评价对象作出评价结果集合 $V=\{V_1,V_2,\cdots,V_k\}$，一般根据实际情况可以将评价等级划分为 4～5 级，取各区间的中值作为等级参数，则对应的评价等级参数列向量为：

$$\bar{V}=(v_1,v_2,\cdots,v_n) \tag{13}$$

3)指标评判与建立模糊关系矩阵。由不同专家根据本领域专业知识对各指标进行评价，将定性指标定量化，然后统计专家对各指标的不同级别评语的频数，即得出各子集 C_i 的单因素评价矩阵 R_i。

4)单因素评价。将已通过层次分析法算出的各单因素 C_i 的权重系数向量 W_i 与单因素评价矩阵 R_i 进行合成运算：

$$B=W_i\cdot R_i \tag{14}$$

5)多因素综合评判。基于第 4)步，可得到 U 中各子集的综合评价矩阵：

$$R=(B_1,B_2,\cdots,B_m)^{\mathrm{T}} \tag{15}$$

如此，逐层向上，直到求出准则层 C 相对于目标 G 的模糊综合评价结果：

$$E=W_C\cdot R_C=(e_1,e_2,\cdots,e_n) \tag{16}$$

E 是因素集 U 的一个隶属度结果向量，而最终评价结果是 E 和评价等级参数列向量 $\bar{V}$ 相乘得到的代数值：

$$Z=E\cdot\bar{V}=(e_1,e_2,\cdots,e_n)\cdot(v_1,v_2,\cdots,v_n) \tag{17}$$

式中，Z 是整个评估对象的一个安全指数结果。

至此，可总结本文使用的云计算安全评估模型，如图 2 所示。

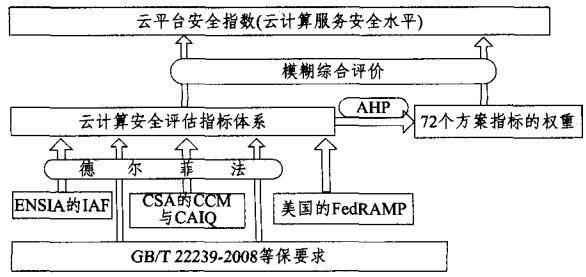

图 2　云计算安全评估模型

5　实例计算与讨论

第 3 节构建的指标体系需要确定权重，通过德尔菲法收集多位专家对指标体系中各指标相对重要性的数据，使用 AHP 计算出 72 个指标项的权重。

根据构建的指标体系，对作者所在的研究所——中国科学院高能物理研究所的科学云[26]进行实例分析。

为提高评估效率，保证数据精确性，本文对采集到的数据使用 Matlab 编程计算。

5.1　确定各指标项权重

根据图 1 所示的 G-C-P 层次模型，建立各级判断矩阵并分别计算单层排序向量、最大特征值 λ_{max}、一致性比率 CR。

准则层 C 相对于目标层 G 的数据如表 3 所列。

计算出 $\lambda_{max}=11.1616$，由式(7)得 $CI=0.0106<0.1$，该判断矩阵通过一致性检验，可接受，结果有效，其最大特征值对应的单位特征向量即准则层因素的权重为：

$$W_{G\text{-}C}=(0.0683,0.1114,0.1326,0.1114,0.0449,0.0352,0.0783,0.0783,0.1412,0.1380,0.0601)^{\mathrm{T}}$$

按照同样的理论与方法计算方案指标层 P_1-P_{10} 对准则层 C_1，$P_{11}-P_{16}$ 对准则层 C_2，$P_{17}-P_{24}$ 对准则层 C_3，$P_{25}-P_{32}$ 对准则层 C_4，$P_{33}-P_{36}$ 对准则层 $C5$，$P_{37}-P_{39}$ 对准则层 C_6，$P_{40}-P_{44}$ 对准则层 C_7，$P_{45}-P_{49}$ 对准则层 C_8，$P_{50}-P_{58}$ 对准则

层 C_9，$P_{59}-P_{67}$ 对准则层 C_{10}，$P_{68}-P_{72}$ 对准则层 C_{11} 的数据，各自进行层次单排序与一致性检验。

表 3 准则层 C 的判断矩阵与权重

G	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	$W_{G\text{-}C}$
C1	1	1/2	1/2	1/2	2	2	1	1	1/2	1/2	1	0.0683
C2	2	1	1	1	2	3	1	1	1	1	2	0.1114
C3	2	1	1	1	3	4	2	2	1	1	2	0.1326
C4	2	1	1	1	2	3	1	1	1	1	2	0.1114
C5	1/2	1/2	1/3	1/2	1	1	1/2	1/2	1/3	1/3	1	0.0449
C6	1/2	1/3	1/4	1/3	1	1	1/2	1/2	1/5	1/4	1/2	0.0352
C7	1	1	1/2	1	2	2	1	1	1/2	1/2	1	0.0783
C8	1	1	1/2	1	2	2	1	1	1/2	1/2	1	0.0783
C9	2	1	1	1	3	5	2	2	1	1	3	0.1412
C10	2	1	1	1	3	4	2	2	1	1	3	0.1380
C11	1	1/2	1/2	1/2	1	2	1	1	1/3	1/3	1	0.0601

最后进行层次总排序，计算出方案指标层中 72 个安全评估项对整个云平台安全评估的组合多元权重，即求出方案指标层 P 相对于目标层 G 的总排序权重 $W_{G\text{-}P}=(0.0051, 0.0089, 0.0103, 0.0052, 0.0065, 0.0087, 0.0051, 0.0019, 0.0087, 0.0080, 0.0264, 0.0290, 0.0165, 0.0079, 0.0079, 0.0237, 0.0204, 0.0263, 0.0263, 0.0108, 0.0131, 0.0108, 0.0118, 0.0131, 0.0160, 0.0206, 0.0160, 0.0083, 0.0079, 0.0076, 0.0275, 0.0076, 0.0091, 0.0091, 0.0156, 0.0111, 0.0156, 0.0136, 0.0060, 0.0119, 0.0154, 0.0154, 0.0178, 0.0178, 0.0174, 0.0174, 0.0174, 0.0174, 0.0087, 0.0162, 0.0189, 0.0121, 0.0189, 0.0199, 0.0128, 0.0155, 0.0176, 0.0091, 0.0093, 0.0096, 0.0224, 0.0200, 0.0109, 0.0051, 0.0195, 0.0167, 0.0245, 0.0258, 0.0086, 0.0086, 0.0086, 0.0086)^T$。

为验证该排序的有效性，进行总排序的一致性检验。检验用到的准则层与方案指标层一致性参数如表 4 所列。

表 4 准则层 C 判断矩阵与权重

准则层	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
准则权重 Wi	0.0683	0.1114	0.1326	0.1114	0.0449	0.0352	0.0783	0.0783	0.1412	0.1380	0.0601
单指标层 CI	0.0329	0.0100	0.0168	0.0077	0.0202	0.0091	0.0194	0	0.0329	0.0169	0
RI	1.49	1.24	1.41	1.41	1.12	0.58	1.12	1.12	1.45	1.45	1.12

总排序的 $CI=\sum_{i=1}^{11}CI_iW_i=0.0162$

$RI=\sum_{i=1}^{11}RI_iW_i=1.3022$

$CR=CI/RI=0.01244<0.1$

可知总排序结果具有满意的一致性，可以接受该分析结果，即层次分析所得的 72 个方案指标项对云计算安全评估总目标的权重分配合理。

5.2 云平台安全指数计算

以 G-C-P 层次模型中的准则层因素构造云计算安全模糊集 $U_1=\{C_1, C_2, \cdots, C_{11}\}$，该模糊集单因素子集中共有 72 个元素；确定云计算安全评语集 $V=\{$很差，差，一般，好，很好$\}=\{v_1, v_2, v_3, v_4, v_5\}$；评语集与分数对照依次为：[0,30)，[30,60)，[60,70)，[70,90)，[90,100)，对应的评价等级参数列向量为 $\overline{V}=(15,40,65,80,95)$。

邀请 8 名具有相关经验的专业人员，根据云计算安全模糊集中的 11 个子集对高能物理研究所云平台进行评价，统计 72 个元素的评价等级频数分布表，如表 5(局部)所列。

表 5 评价等级频数分布表($N=8$)

评估项	很差	差	一般	好	很好
P1	0	0	2	5	1
P2	0	1	3	4	0
P3	0	0	1	5	2
…	…	…	…	…	…
P10	0	1	2	5	0
…	…	…	…	…	…
P71	0	1	3	4	0
P72	0	1	5	2	0

对准则项 C_1 所关联的 P_1-P_{10} 频数分布归一化处理，可得模糊关系矩阵 R_{C1}：

$$R_{C1}=\begin{pmatrix}0 & 0 & 0.25 & 0.625 & 0.125\\ 0 & 0 & 0.375 & 0.5 & 0.125\\ 0 & 0 & 0 & 0.625 & 0.375\\ 0 & 0 & 0.125 & 0.625 & 0.25\\ 0 & 0 & 0.25 & 0.625 & 0.125\\ 0 & 0 & 0.25 & 0.75 & 0\\ 0 & 0.125 & 0.625 & 0.125 & 0.125\\ 0 & 0 & 0.625 & 0.25 & 0.125\\ 0 & 0 & 0.125 & 0.625 & 0.25\\ 0 & 0 & 0.25 & 0.625 & 0.125\end{pmatrix}$$

由式(14)得 C_1 的单因素评价结果 B_{C1}：

$B_{C1}=W_{G\text{-}C}\cdot R_{C1}=(0,0093, 0.2415, 0.5771, 0.1722)$

同理可得 B_{C2}，B_{C3}，B_{C4}，B_{C5}，B_{C6}，B_{C7}，B_{C8}，B_{C9}，B_{C10}，B_{C11}。将单因素评价结果综合起来，构成总的模糊关系矩阵：

$$R=\begin{pmatrix}0 & 0.0093 & 0.2415 & 0.5771 & 0.1722\\ 0 & 0.0877 & 0.3240 & 0.5873 & 0\\ 0 & 0.1295 & 0.4133 & 0.4571 & 0\\ 0 & 0.1295 & 0.2816 & 0.5890 & 0\\ 0 & 0.1250 & 0.3317 & 0.5433 & 0\\ 0 & 0.1039 & 0.3750 & 0.4657 & 0.0554\\ 0 & 0.1004 & 0.3313 & 0.5682 & 0\\ 0 & 0.0278 & 0.3611 & 0.5287 & 0.0833\\ 0 & 0 & 0.2530 & 0.6642 & 0.0829\\ 0 & 0.0688 & 0.3312 & 0.5817 & 0.0183\\ 0 & 0.1250 & 0.5537 & 0.3215 & 0\end{pmatrix}$$

因此，云平台综合评价向量为：

$E = W_{GC} \cdot R = (0, 0.0784, 0.3358, 0.5510, 0.0345)$

由式(17)得到高能所云平台的整体安全评估指数：

$$Z = E \cdot \overline{V}$$
$$= (0, 0.0784, 0.3358, 0.5510, 0.0345) \cdot (15, 45, 65, 80, 95)^T$$
$$= 72.7125$$

Z 数值落在评语集中 v_4 的区间内，评分结果反映云平台的安全级别为“好”，而向量 E 中评语为“一般”的比例也达到了 0.3358，根据隶属度概念，说明仍存在不小的安全改进空间。

计算与分析显示，提出的评估模型完成了对云计算实例的安全水平量化，评估结果与该平台通过其它方案评测得到的综合结论相符，表明使用的评估方法是有效的。

5.3 讨论

与规范类文献[9-12]所提出的云计算安全保障或安全控制体系相比，本文构建的评估准则以我国推行较广的等级保护指标体系为基础，使用德尔菲法进行了适合云计算的指标项裁剪、修订与增加，符合中国的具体情况，实践证明其操作性也更强，并在一定程度上消除了层次的复杂性与指标项的冗余，可较大地减少工作量。

与文献[13]的云安全风险量化评估框架相比，本文设计的评估指标体系更具体，更能反映云计算的特点。前者笼统地提出云计算安全的六点，无细节化的评估项，本文集中在16项底层指标上体现了云计算安全的需求，如“虚拟机防护”、“第三方服务水平监管”、“数据移植”；另一方面，前者的实例分析比较零散，本文则以实际云平台为例，从全局、整体的角度验证了提出模型的有效性。

与文献[14]云服务风险评估框架相比，本文首次将德尔菲法、AHP与模糊综合评判引入云计算安全评估的指标体系构建与实施过程，以量化的方法给用户或审计人员提供了直观的服务安全水平结果。

结束语 云计算已经得到比较广泛的应用，其很多安全问题却一直待解决。其中，云计算安全的建设、评估与审计、服务水平的量化，都需要有适用的指标体系；建立云计算安全评估指标体系后，需要采用科学的算法确定各指标项的权重；对获取的评估信息使用恰当的计算方法，从而得出有效的评估结果。这些是本文已初步完成的工作。下一步的计划是，对设计的指标体系进行修改，以便适用于更多典型的云平台，增强评估过程的自动化功能。

参 考 文 献

[1] 冯登国，张敏，张妍，等. 云计算安全研究[J]. 软件学报，2011，22(1)：71-83

[2] GB/T 22239-2008 信息安全等级保护基本要求[S]. 2008

[3] 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

[4] 周元德，董凤翔，胡波. 基于等级保护的信息安全风险评估方法[J]. 铁道工程学报，2006，99(9)：89-92

[5] 王升保. 信息安全等级保护体系研究及应用[D]. 合肥：合肥工业大学，2009

[6] 李鑫，李京春，郑雪峰，等. 一种基于层次分析法的信息系统漏洞量化评估方法[J]. 计算机科学，2012，39(7)：58-63

[7] 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

[8] 周焕盛，江建慧. 一个多维信息安全指标体系及等级保护量化模型[J]. 中国科学技术大学学报，2012，42(1)：67-76

[9] ENISA. Cloud Computing Information Assurance Framework [R]. 2009

[10] Coucil U S C. Proposed Security Assessment and Authorization for Cloud Computing[R]. 2010

[11] CSA. CloudControlMatrix [EB/OL]. https://cloudsecurityalliance.org/research/ccm/

[12] CSA. CloudConsensusAssessmentInitiative [EB/OL]. https://cloudsecurityalliance.org/research/cai/

[13] Saripalli P, Walters B. A Quantitative Impact and Risk Assessment Framework for Cloud Security[C]// Proceedings of IEEE 3rd International Conference on Cloud Computing. 2010：280-288

[14] Djemame K, Armstrong D J, Kiran M, et al. A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems [C]// Proceedings of 2nd International Conference on Cloud Computing, GRIDs, and Virtualization. 2011：119-126

[15] Kiran M, Jiang Ming, Armstorng D J, et al. Towards a Service Life-cycle based Methodology for Risk Assessment in Cloud Computing[C]// Proceedings of 9th International Conference on Dependable, Autonomic and Secure Computing. 2011：449-456

[16] 陈晓剑，梁梁. 系统评价方法及应用[M]. 合肥：中国科学技术大学出版社，1993：24-25

[17] 公安部. 信息安全等级保护管理办法(试行). 2006

[18] 沈昌祥. 云计算安全与等级保护[J]. 信息安全与通信保密，2012(1)：16-17

[19] Linstone H A. The Delphi Method：Techniques and Applications [M]. Addison-Wesley，1975：25-30

[20] Brodkin. Gartner：seven cloud-computing security risks [DB/OL]. http://www.networkworld.com/news/2008/070208-cloud.html，2008-07-02

[21] ENISA. Cloud computing-benefits risks and recommendations for information security[R]. 2009

[22] ENISA. Top Threats to Cloud Computing [R]. 2009

[23] ENISA. A guide to monitoring of security service levels in cloud contracts[R]. 2012

[24] Saaty T L. How to make a decision：The Analytic Hierarchy Process[J]. European Journal of Operational Research，1990(48)：9-26

[25] Zimmermann H-J. Fuzzy Set Theory and its Applications [M]. Springer，1996：47-91

[26] 程耀东，刘宝旭，孙功星，等. 高能物理与云计算[J]. 核电子学与探测技术，2011，31(11)：1189-1194