基于SecLA的云服务商选择方法研究

朱华旻 吴礼发 康红凯
(解放军理工大学指挥信息系统学院 南京 210007)

摘 要 云计算应用领域不断拓展,用户越来越关注云服务的安全性,现有云服务商选择方法主要考量性能和费用,缺乏有效的安全属性考评方法,为此提出了基于安全等级协议的云安全量化评比方法。基于云安全联盟的云控制矩阵及配套共识评估问卷,设计了云服务商安全指标体系及量化评分模型;对Web服务协议框架进行扩展,设计了云安全等级协议的模板框架;引入负提供参数来增强比较优势度法,实现了云安全等级的量化评比。实验检验了系列方法的可行性及有效性,与参数评估方法、简单线性加权方法等的对比表明,优先度排序更加合理,负提供参数对决策起到了良好的辅助效果。

关键词 云计算,云安全评估,云安全量化,安全等级协议,云服务商选择
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.5.019

Research of Cloud Provider Selection Method Based on SecLA

ZHU Hua-min WU Li-fa KANG Hong-kai
(Institute of Command Information System, PLA University of Science and Technology, Nanjing 210007, China)

Abstract As the range of cloud computing applications is gradually expanded, users become more and more concerned about the security of cloud services. Existing selection methods of cloud provider focus on performance and cost while seldom emphasize security. There is no effective method for evaluating the security services of cloud computing. Under this background, this paper presented a method for quantitative assessment of cloud security services based on security level agreement(SecLA). Firstly, it builds the cloud computing security index system and the quantitative evaluation model based on cloud control matrix(CCM) and accompanying consensus assessments initiative questionnaire(CAIQ), which are published by cloud security alliance(CSA). Secondly, it designs the template framework of SecLA by extending WS-Agreement. Finally, it introduces two underprovisioning parameters to enhance comparison method of alternatives advantage degree and realizes the quantitative comparison of SecLAs in cloud computing environment. The experimental results prove that the methods are feasible and effective. Compared with reference evaluation method(REM) and simple linear weighted method, the cloud providers sorting results in this paper are more reasonable, and underprovisioning parameters contribute a good auxiliary effect to decision making.

Keywords Cloud computing, Cloud security assessment, Cloud security quantification, Security level agreement(SecLA), Cloud provider selection

1 引言

云计算资源容量大、经济效益好、部署快速、弹性强,应用前景十分广阔,但面临着数据破坏、隐私泄漏、网络攻击、虚拟机入侵、灾难事件等诸多安全威胁,安全事件时有发生,例如2011年以来谷歌、亚马逊、微软等发生的一系列云安全事故,严重打击了云用户的消费信心,安全问题是云计算发展的主要阻碍[1]。用户在选择云服务商的过程中,越来越关注其安全保护质量,已有一些学者研究基于安全属性的云服务商选择方法[2-8],主要有如下两种解决思路:

1)通过创建云安全本体和提取安全供需信息,计算供需信息中本体术语语义匹配度对云服务商进行排序。Hale等[9]基于权威安全标准和框架例如NIST SP800-53、CCP2、CCM、DoD8500等,创建了云安全本体,其包含了一系列推荐安全控制的概念术语;利用该本体设计了云安全供需合规风险计算方法[7],但所创建本体术语及其关系的代表性和合理性无从检验,也较难取得业界共识。云安全联盟(CSA)倡议的云控制矩阵(CCM)是专家组深入研究IT领域权威安全标准和纲领,精心挑选归类综合,并经多次征求行业意见建议而推荐的一整套最佳云安全控制实践[10]。为评价云安全合规性,配套设计的云共识评估问卷(CAIQ)与CCM一一对应,就各控制条款对各服务商进行问卷调查[11]。Thaweejinda等[2]设计了基于CCM和CAIQ的云安全本体,以控制组、控制域为主要类,新建Product类统筹来证明控制域安全合规性的相关认证、报告、证书,Activity类统筹例如渗透测试、漏洞扫描等重要安全控制活动,利用这些类术语创建服务商和

到稿日期:2015-05-25 返修日期:2015-08-07 本文受江苏省自然科学基金项目(BK20131069)资助。
朱华旻(1978-),男,博士生,主要研究方向为网络安全,E-mail:zhuhuamin2001@163.com;吴礼发(1968-),男,教授,博士生导师,主要研究方向为网络安全;康红凯(1986-),男,硕士生,主要研究方向为网络安全。

用户特征库，进行供需语义特征匹配。Pumvarapruek 等[4]基于 CCM 和 CAIQ 创建了本体，从服务商网站提取相关安全术语建立服务商安全向量，计算该向量与本体各控制组向量的语义相似度，基于各服务商的控制组相似度列表进行综合选择，但安全术语提取的误差大。

2)基于安全指标及其评分模型的量化评估方法。姜政伟等[12]自定义了云安全指标体系，设计了改进 ELECTRE 多属性决策的云选择方法，但指标体系缺乏权威性和共识度，且未考虑用户个性化安全需求。Luna 等[5]直接基于云服务商 CAIQ 评估报告中安全条款 yes/no 的回答对各控制域安全等级计分，以用户需求为目标，通过对各控制域实际安全值与目标值之差进行线性加权来确定服务商效用。文献[6]采用与文献[5]相同的安全指标和计分标准，采用先聚合指标值后与用户需求相比较的方法。文献[5,6]均存在不足，因为 CAIQ 评估报告 yes/no 回答可能存在虚假成分，而且简单线性加权或者聚合的方法会导致优劣指标直接相互抵销，使所得效用值不可靠。Bhensook 等[3]只考查云服务商安全控制与 CMM 合规的证据，例如第三方审计报告、权威认证等，通过对相关证据质量打分，汇总计算各服务商安全得分。

总之，基于创建本体进行安全供需术语语义比较的方法存在以下问题：所创本体的合理性和完备性难以检验，其权威性和共识度很难被认可，样式和内容均尚未统一的云服务商安全描述使安全术语提取相当困难，提取误差通常较大。基于安全指标量化比较的方法可实现更高的精度和准确性，但需要权威而科学的指标和评分体系，以及有效的量化评价方法。考虑到 CCM 和 CAIQ 的权威性和已取得的广泛共识度，本文拟基于 CCM 和 CAIQ 设计云安全量化指标及评分模型，通过扩展 WS-Agreement[13]进行云安全等级协议(SecLA)描述模板的设计，通过引入负提供参数增强比较优势度法进行云服务商安全量化评比。

2 基本概念

2.1 安全等级协议(SecLA)

服务等级协议(SLA)源于电信领域，已广泛应用于通信和 Web 服务领域，是供求双方对服务质量属性进行描述和约束的模型/协议。云计算环境中，SLA 已经受到业界重视，例如 ENISA 已将云 SLA 列入欧盟云计算战略[6]。为了描述和量化服务的安全保护等级，1999 年 Henning 提出 SecLA 概念[14]，之后它被逐步推广应用于众多 IT 服务领域。目前，在云服务发现及使用过程中，通常仅能够评价和管理性能服务质量，缺乏安全保护质量度量和管理方法，这是在云计算中引入 SecLA 的主要动机。Karin 等[15]指出云 SecLA 全生命周期应包括发布、协商、签订、提供、监控和终止。

2.2 WS-Agreement

目前还没有创建 SLA offers 和契约的标准语言，但在 Web 服务及其它 SOA 环境中，Web 服务等级协议(WSLA)和 Web 服务协议规范(WS-Agreement)是最常用的 SLA 描述语言，WSLA[16]由 IBM 于 2001 年提出，提供了基于 XML 的 SLA 描述语言及 SLA 管理框架，但不开源、不易扩展。

WS-Agreement 是开放网格论坛(OGF)提出的一个基于 XML 的 Web 服务协议规范，其目标是提供标准化的 SLA 描述术语、模板框架，以及一套访问端口和包含创建、协商、签定、监控等环节的 SLA 操作，WSAG4J 框架已提供该协议规范的完整实现[17]。由于 WS-Agreement 应用广泛，相对简单且易于扩展，本文选择它作为 SecLA 模板的基础框架。WS-Agreement的主体结构如图 1 所示，它是创建 SLA offers、模板的基础。name 是可选项，SLA 协商可能使用不同的协议模板，所以用 Id 作为版本标识，wsag:Context 提供如协议相关各方、协议寿命等信息，核心部分是 wsag:Terms。

```
〈wsag:Agreement AgreementId="xs:string"〉
〈wsag:Name〉 xs:string 〈/wsag:Name〉?
〈wsag:Context〉 wsag:AgreementContextType 〈/wsag:Context〉
〈wsag:Terms〉
〈wsag:All〉
 {…
  〈wsag:All〉…〈/wsag:All〉
  〈wsag:ServiceDescriptionTerm wsag:Name="xs:string"
    wsag:ServiceName="xs:string"〉
  〈xs:any〉…〈/xs:any〉
  〈/wsag:ServiveDescriptionTerm〉
  〈wsag:ServiceProperties〉 wsag:ServicePropertiesType
  〈/wsag:ServiceProperties〉
  〈wsag:GuaranteeTerm〉 wsag:GuaranteeTermType
  〈/wsag:GuaranteeTerm〉...
  …}
〈/wsag:All〉
〈/wsag:Terms〉
〈/wsag:Agreement〉
```

图 1 WS-Agreement 主体结构

wsag:Terms 通过 wsag:All 可嵌套术语组合器来组织服务相关元素，主要包括服务描述术语和保证术语。服务描述术语实现对服务整体或部分的描述，包含该术语本身名称、所描述服务名称，以及一个可扩展的元素 xs:any，可利用它定义所需的各种领域描述术语，本文通过扩展 xs:any 定义了云计算环境下 SecLA 模板的主要结构。另外，可以通过服务属性元素定义服务属性及其相关变量，保证在术语部分通过定义服务属性条件约束确立服务质量目标。

2.3 比较优势度法

比较优势度法是林志明等[18]提出的一种多属性决策方法，主要原理是：首先备选方案两两间进行优劣比较，即通过计算方案间指标带权优势量和带权劣势量求取方案间优势度值；在此基础上建立方案优势度判别矩阵；最后基于判别矩阵进行方案优先度排序。比较优势度法的主要概念及计算流程如下所述。

假设有 m 个备选方案，n 个属性指标，经过无量纲规范化得到决策矩阵 $\boldsymbol{R}=(r_{ij})_{m\times n}$，$r_{ij}$ 是方案 x_i 的第 j 个指标，指标权重向量为 $w=(w_1,w_2,\cdots,w_n)$，令 $M=\{1,2,3,\cdots,m\}$，$N=\{1,2,3,\cdots,n\}$，指标集为 $U=\{u_1,u_2,u_3,\cdots,u_n\}$。

称 $J_{pq1}=\{u_j\mid r_{pj}>r_{qj},p,q\in M,j\in N\}$ 是方案 p 对 q 的优势指标集，$J_{pq2}=\{u_j\mid r_{pj}<r_{qj},p,q\in M,j\in N\}$ 是方案 p 对 q 的劣势指标集，$J_{pq3}=\{u_j\mid r_{pj}=r_{qj},p,q\in M,j\in N\}$ 是方案 p 对 q 的等势指标集。

称 $d^{+}_{pqk}=r_{pk}-r_{qk}(p、q\in M,u_k\in J_{pq1})$ 为方案 p 对方案 q 在 k 指标点的优势距离；称 $d^{-}_{pqk}=r_{qk}-r_{pk}(p、q\in M,u_k\in J_{pq2})$ 为方案 p 对方案 q 在 k 指标点的劣势距离。

称 $wd^{+}_{pq}=\sum d^{+}_{pqk}w_k(u_k\in J_{pq1},p、q\in M)$ 是方案 p 对方案

q 的带权优势量，它反映了方案 p 对方案 q 在优势指标上线性加权所得的绝对优势幅度；称 $wd_{pq}^{-}=\sum d_{pqk}^{-}w_k$（$u_k\in J_{pq2}$，$p$、$q\in M$）是方案 p 对方案 q 的带权劣势量，它反映了方案 p 对方案 q 在劣势指标上线性加权所得的绝对劣势幅度。

容易证明 $0\leqslant d_{pqk}^{+}\leqslant 1$，$0\leqslant d_{pqk}^{-}\leqslant 1$，$d_{pqk}^{+}=d_{qpk}^{-}$，按式(1)计算方案间相对优势度。

$$v_{pq}=\begin{cases} wd_{pq}^{+}/(wd_{pq}^{+}+wd_{pq}^{-}), & wd_{pq}^{+}\neq 0 \text{ 且 } wd_{pq}^{-}\neq 0 \\ 0.5\left(1+\dfrac{wd_{pq}^{+}}{\sum\limits_{u_k\in J_{pq1}}(\underset{i\in M}{\text{Max}}\, r_{ik}-\underset{i\in M}{\text{Min}}\, r_{ik})w_k}-\dfrac{wd_{pq}^{-}}{\sum\limits_{u_k\in J_{pq2}}(\underset{i\in M}{\text{Max}}\, r_{ik}-\underset{i\in M}{\text{Min}}\, r_{ik})w_k}\right), & \text{其它} \end{cases} \tag{1}$$

备选方案两两间优势度值构成优势度矩阵 $\boldsymbol{V}=(v_{pq})_{m\times m}$，已证明优势度矩阵是互补判别矩阵，即假定 v_{pq} 是方案 p 对 q 的优势度值，那么 v_{pq}、v_{qp} 均在 0 到 1 之间，$v_{pq}+v_{qp}=1$，且 $v_{pp}=v_{qq}=0.5$。基于矩阵 $\boldsymbol{V}$ 按式(2)求取各方案的总体优势度，按从大到小的顺序建立方案排序向量 $v=(v_1,v_2,\cdots,v_m)$，即为最终方案优劣排序结果。

$$v_i=\frac{\sum\limits_{j=1}^{m}v_{ij}}{\sum\limits_{k=1}^{m}\sum\limits_{j=1}^{m}v_{kj}}=\frac{\sum\limits_{i=1}^{m}v_{ij}+m/2-1}{m(m-1)},\ i=1,2,\cdots,m \tag{2}$$

3 云安全指标及评分模型

3.1 方法分析

定义安全指标是实现云安全等级量化评价的前提，也是一个复杂的系统工程。首先，作为 IT 服务的一个分支，云计算继承了传统 IT 领域权威的安全框架、标准和原则，同时也有其新特点；其次，指标体系须具有权威性，才能取得业界共识、推广使用；最后，指标要科学量化并便于实施度量。如引言所述，CSA 制订了 CCM 及配套 CAIQ，另外，还发起了云安全、信任与保证注册项目 STAR[19]，STAR 主要收录服务商安全评估报告及相关权威认证，同时推出基于 CCM 的 STAR 认证。CCM 的制订参考了许多相关 IT 服务领域权威的安全标准和框架，例如美国注册会计师协会的可信服务准则（AICPA TSC）、信息及相关技术控制目标框架（COBIT）、欧盟网络信息安全局信息保护框架（ENISA IAF）、联邦政府风险和授权管理计划（FedRAMP）、医疗电子交换法案（HIPAA/HI-TECH Act）、信息安全管理体系 ISO/IEC 27001、美国国家标准和技术研究院推荐的联邦信息系统和组织安全控制规范（NIST SP800-53 R3）、支付卡工业数据安全标准（PCI DSS）等。

CSA 作为云安全标准领导组织，由其提出的 CCM 及 CAIQ 已经获得了业界广泛共识和积极响应，广大云服务商正积极参加 STAR 项目，陆续向 STAR 库提交其 CAIQ 评估报告及相关认证，随着 CCM 及 CAIQ 的不断升级完善，其必将成为事实的云安全标准。鉴于此，本文拟基于 CCM 和 CAIQ 定义云安全等级量化指标及评分模型。

3.2 指标及评分模型

如图 2 所示，基于 CCM 的 CAIQ 采用分层结构，即控制组→控制域→问题的结构，为每个控制域精心设计了若干问题，调查该控制域是否遵循了 CCM 推荐的安全原则和最佳实践，服务商可以作出 yes/no 的回答，还可对问题作细节说明，佐证其合规性。例如对于问题 CO-02.1“是否允许云租户查看你的第三方审计报告，类似 SAS70 Type II 或 SSAE 16 SOC2 或 ISAE3402”，服务商可能回答 yes 并作细节说明“乐意与租户共享 SSAE16 审计报告”，SSAE16 审计报告即可作为该条款的合规性证据。仅依据 yes/no 的回答或仅依据合规证据来评价控制域安全等级均较为片面。CSA 发起创建的 STAR 平台本身具有较强的公信力，公开发布于 STAR 的 CAIQ 报告中所有安全陈述均可视为云服务商的一种安全承诺，可以作为安全协商或评估的依据，报告中 yes/no 的回答能够从总体上反映云服务商对 CCM 推荐安全控制的遵循情况，但不能排除存在虚假成分的可能。虽然合规性证据更加可靠，但有不少控制域往往很难提供这种证据。因此，拟将 CAIQ 中 yes/no 的回答与合规性证据结合起来，综合评价控制域安全等级，由于各控制域是相对独立的安全控制功能单元，本文基于各控制域安全等级定义云安全指标体系。

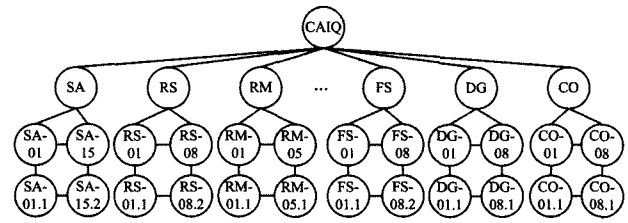

图 2 CAIQ 层次结构

首先，依据各控制域下安全条款 yes/no 回答计算其基础安全分，考虑控制域通常有 3－6 个问题，设置控制域满分为 5 分；其次，利用与文献[3]类似的方法，提取 CAIQ 报告中的 CCM 合规性证据，通过专家组对证据进行打分，综合各证据得分计算服务商合规性证据总分，将该值作为服务商合规性可信度；最后得到：控制域实际评分＝该控制域基础安全分×服务商合规性可信度。假设 g_i 是 CCM 下第 i 个控制组，d_{ij} 是控制组 g_i 下第 j 个控制域，在 CAIQ 报告中控制域 d_{ij} 包含 k 个问题 $q_{ij1},q_{ij2},\cdots,q_{ijk}$，得到肯定回答 l 个，该服务商合规性可信度为 t_p，则 d_{ij} 的最后评分等于 $5\times(l/k)\times t_p$。利用服务商 CAIQ 报告很容易计算各控制域基础安全分，以下主要介绍服务商合规性证据评分方法。

以 CSA 的 CCM 及 CAIQ 为依据，利用目标-问题-度量（Goal-Question-Metric，GQM）方式，定义服务商合规性证据评分模型。以各控制组为目标，基于 CCM 对控制组及组下控制域的相关控制规范，结合 CAIQ 对控制域制订的相关问题，设计各控制组与合规性证据相关的问题，最后针对每个问题设计具体度量指标，作为示例，表 1 展示了 Compliance 控制组的证据评分模型。

借鉴文献[2]将合规性证据分为两类：1）类似 SOC、SSAE16、ISO 27001、PCI DSS 等权威标准认证、报告、证书，称为 Product 类证据；2）类似漏洞扫描、渗透测试等重要安全活动，称为 Activity 类证据。通过考查证据合规性和完备性来评价证据质量，证据合规性指证据是否与 CAIQ 要求标准一致，是否符合权威标准，合规 1 分，部分合规 0.5 分，不合规 0 分，证据若虽属于问题范畴，但并不完全符合相关要求，则判定为部分合规；对于证据完备性，合规证据的产生通常有一个完整周期，例如 ISO 27001:2005 审计报告，最初可能只是安全纲领，进一步会制订审计规划，接下来明确活动细节，然

后执行审计、推荐校正、生成报告等，证据完备性评分模型如表 2 所列。

表 1　Compliance 控制组合规性证据评分模型示例

目标	问题	尺度
G-01 合规性	Q-01.1 有何证据表明使用了工业界接受的审计策略 CloudAudit/A6 URI Ontology、CloudTrust…等？	M-01.1.1 审计策略证据合规性、完备性
	Q-01.2 可提供哪些类似 SAS700 Type II/SSAE16 OC2/ISAE3402 等的第三方审计报告，其质量如何？	M-01.2.1 审计证据合规性及完备性。第三方陈述、书面证据、审计报告
	Q-01.3 周期性网络/应用脆弱点扫描、渗透测试是否与产业界最佳实践和指导一致，相关证据质量如何？	M-01.3.1 网络应用脆弱点扫描、渗透测试合规性、完备性
	Q-01.4 有什么证据证明你有能力为用户隔离和恢复数据？	M-01.4.1 实现用户数据隔离和恢复的证据合规性完备性
	Q-01.5 有什么证据证明你有能力保护用户信息资产？	M-01.5.1 信息资产保护证据合规性、完备性
…	…	…

表 2　证据完备性评分模型

完备性等级	相关证据类型	分值
无证据		0
初始阶段	初步项目说明、纲领	0.1
规划阶段	项目范围、工作分解、活动列表、项目时间表	0.3
执行阶段	项目管理计划、人员分配、团队表现评价	0.5
监控阶段	推荐校正动作、推荐预防动作	0.8
封闭	最后的 product、服务或结果	1

合规性证据评分方法：设 S_y 为第 y 个控制组证据得分，k 为控制组数目，则总分 $S_{total}=(\sum S_y)/k$，$y=1\rightarrow k$；设控制组 y 合规证据相关问题数目为 m，第 i 个问题证据实际得分为 $AutualS_{yi}$，分值上限为 $MaxS_{yi}$，则 $S_y=(\sum AutualS_{yi})/(\sum MaxS_{yi})$，$i=1\rightarrow m$；设 $AutualS_{yij}$ 表示控制组 y 第 i 个问题的第 j 个指标实际得分，$MaxS_{yij}$ 表示此指标得分上限，该问题共有 n 个指标，则 $AutualS_{yi}=(\sum AutualS_{yij})/(\sum MaxS_{yij})$，$j=1\rightarrow n$；设控制组 y 第 i 个问题的第 j 个指标的证据合规性得分为 v_{cpl}，完备性得分为 v_{cpt}，则 $AutualS_{yij}=(v_{cpl}+v_{cpt})/Max(v_{cpl}+v_{cpt})=(v_{cpl}+v_{cpt})/2$。

4　SecLA 的表示模板

设计的云安全指标及评分体系为描述用户安全需求和服务商安全能力提供了内容，下面基于 WS-Agreement 设计 SecLA 的表示模板，作为云安全需求和安全 offers 描述的载体。因目前云服务商普遍不支持安全协商，基于简单和易用原则，主要扩展 WS-Agreement 的服务描述术语 SDT 部分。如图 1 所示，SDT 包括两个属性和一个 xs:any 域，属性 wsag:Name 定义 SDT 的标识以方便对其引用，通常一个 SDT 对应描述一个服务方面或组件，属性 wsag:ServiceName 定义所描述服务的标识。xs:any 域允许自定义 SDT 相关的任何领域特别的 XML 描述规范。

基于 WS-Agreement 的 XML Schema 通过扩展 SDT 的〈xs:any〉域来表示云安全指标体系，以新的命名空间 secag 设计了 SecLA 表示模板。考虑 CAIQ 指标层次，定义了两个层级元素，分别为控制组元素和控制域元素，控制组元素主要实现指标分类，控制域元素对应于 CAIQ 的控制域安全指标。同时为两个元素定义了一些必要属性，为控制组定义了名称属性、ID 属性，控制组名称是控制组全名如 FacilitySecurity，ID 属性是 CAIQ 中赋予控制组的简写代码，作为该元素标识符，如 FacilitySecurity 简写为 FS。为控制域定义了名称、ID、权重和安全等级属性，名称是该控制域全名如 UserAccess，ID 是 CAIQ 赋予值，为其唯一标识，如 FS-02 就是 FacilitySecurity/UserAccess 的唯一标识。按本文安全指标评分模型，定义控制域安全等级为 0－5 之间的十进制数，为使用户定义控制域安全等级需求时不至于太随意，约定了安全需求可指定的 10 个安全等级值范围，即{0，0.5，1，1.5，2，2.5，3，3.5，4，4.5，5}，以 0.5 分进行步进。权重属性设置为 0－1 间十进制数，所有控制域权重之和必须等于 1。SecLA 模板主要元素的描述如图 3、图 4 所示，由于图 3 是元素层次结构的描述，图 4 是元素的具体定义，因此其命名空间不同。secag:SecurityDescriptionTerm 包含了一个或多个 secag:ControlGroup，而 secag:ControlGroup 则包含了一个或多个 secag:ControlDomain。控制组 secag:ControlGroup 既包含元素又包含属性，根据 XSD 是带混合内容的复杂类型，secag:ControlDomain 包含 4 个属性。另外，基于 wsag:SeriveDescriptionTerm 定义了 secag:SecurityDescriptionTerm，基于 xs:decimal 定义了两个简单类型 secag:SecLevelType 和 secag:WeightType，分别表示控制域安全指标值及其权重，篇幅所限不再详细列出。

```
〈secag:SecurityDescriptionTerm wsag:Name="xs:string"
  wsag:ServiceName="xs:string" 〉
〈secag:ControlGroup Name="xs:string" ID="xs:string"〉
〈secag:ControlDomain Name="xs:string" ID="xs:string"
  Weight="secag:WeightType" Level="secag:SecLevelType"/〉+
〈/secag:ControlGroup〉+〈xs:any〉…〈/xs:any〉
〈/secag:SecurityDescriptionTerm〉
```

图 3　secag:SecurityDescriptionTerm 元素

```
〈xs:element name = "ControlGroup" 〉
〈xs:complexType mixed = "true"〉
〈xs:sequence〉
〈xs:element ref= "ControlDomain" minOccurs ="1"/〉
〈/xs:sequence〉
〈xs:attribute name="Name" type="xs:string"/〉
〈xs:attribute name="ID" type="xs:string"/〉
〈/xs:complexType〉
〈/xs:element〉
…
〈xs:element name="ControlDomain" 〉
〈xs:complexType〉
〈xs:attribute name="Name" type="xs:string"/〉
〈xs:attribute name="ID" type="xs:string"/〉
〈xs:attribute name="Weight" type="secag:WeightType"/〉
〈xs:attribute name="Level" type="ecag:SecLevelType"/〉
〈/xs:complexType〉
〈/xs: element〉
```

图 4　secag:ControlGroup 及 secag:ControlDomain 元素

5　云服务商安全评价和决策

5.1　基本原理

基于量化安全指标进行云服务商选择是一个多属性决策问题，属性值为实数的多属性决策有 3 种解决思路：(1)通过集结属性值与权重获取方案评价值排序，如简单线性加权、层

次分析法[20]；(2)计算与目标方案的关系来评价方案优劣，如接近度、相似度、关联度[21]；(3)通过方案两两比较优劣进行排序，如 ELECTRE 法、PROMETHEE 法及比较优势度法[18]等。思路一基于总体效用排序，粒度较粗，优势指标与劣势指标会出现直接对冲；思路二能找到与目标最相似或接近的方案，但效益型指标通常越大越好，成本型指标越小越好，一些情况下此思路也并不理想；思路三在备选方案两两间比较每个属性优劣，粒度更细，且分别集结优势指标和劣势指标，避免了两者直接抵销。ELECTRE 法仅依据优劣指标个数比较方案优劣，忽视了属性值差距大小；PROMETHEE 法引入方案间属性优先函数表示属性优劣差距，但过于繁琐，2.3 节介绍的比较优势度法克服了 ELECTRE 的缺陷且简单易行，因此，本文基于比较优势度法进行服务商安全性评价和决策，并对其进行进一步改进。

比较优势度法仅在备选方案间两两比较，反映不了各方案对用户指定安全目标(指标心理阈值)的满足程度，无从得知哪些方案达到或优于用户目标；另外，尽管避免了优势指标与劣势指标直接对冲，但依据式(1) 特别突出的带权优势量仍可一定程度平衡掉较大带权劣势量的坏影响，即劣势指标突出的方案仍有可能排序靠前。为此，本文对比较优势度法进行两点改进：(1)将用户需求视为目标方案，加入备选方案序列参与比较，依据排序结果便知哪些备选方案达到或优于用户需求目标值；(2)新增 2 个负提供参数作为决策依据，包括负提供指标百分比、负提供指标偏移幅度，用户可从方案排序结果过滤掉负提供参数太大的方案，使决策结果符合用户心理预期，决策更加合理。

5.2 基于 Broker 的云选择框架

设计了基于第三方 Broker 的云选择框架，如图 5 所示，Broker 作为用户和云服务商的中介，承担了云选择的主要职能，包括：

(1)专家评分，基于 CCM 合规性证据评分系统，组织专家组对 STAR 库中服务商 CAIQ 评估报告中的相关证据进行评分，结合 CAIQ 报告 yes/no 的回答计算得到服务商各控制域实际安全等级值，并将它保存到数据库；

(2)创建 SecLA 的描述模板；

(3)生成云服务商 $SecLA_{PS}$：基于服务商安全评分数据库和步骤(2)创建的 SecLA 模板，生成服务商 $SecLA_{PS}$；

(4)协助用户定义 $SecLA_R$：为用户提供控制域平均安全值 LSL 作为参照，基于用户指定的安全域及其值，利用 SecLA 模板定义用户需求 $SecLA_R$；

(5)评价和比较云服务商：将 $SecLA_R$、$SecLA_{PS}$ 提交到安全评价和比较模块，主要利用改进的比较优势度法计算获取方案优先排序向量及备选方案负提供参数，反馈给用户进行最终决策。

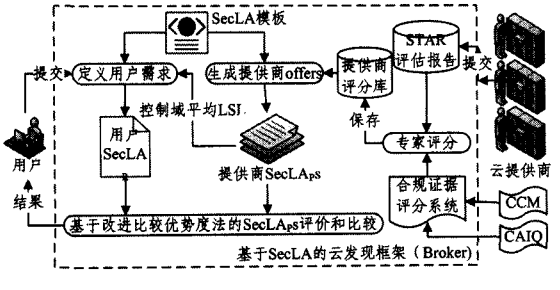

图 5 基于 Broker 的云选择框架

5.3 基于改进比较优势度法的云服务商评价和决策

基于改进比较优势度法的云服务商安全评价和决策流程如图 6 所示，具体如下：

(1)基于用户安全需求和服务商安全 offers 的标准描述 $SecLA_R$、$SecLA_{PS}$，提取用户关注的控制域需求目标值，以及各备选云服务商相应控制域的实际安全等级值，创建决策矩阵 $\boldsymbol{X}(x_{ij})_{(m+1)\times n}$。$\boldsymbol{X}$ 前 m 行代表备选云服务商，第 $m+1$ 行代表用户目标，每列代表用户关注的控制域，均为效益型指标，可利用公式 $r_{ij}=(x_{ij}-\min x_{kj})/(\max x_{kj}-\min x_{kj})$，$k=1\rightarrow m+1$ 进行归一化处理，得到无量纲归一决策矩阵 $\boldsymbol{R}(r_{ij})_{(m+1)\times n}$。

(2)对 $m+1$ 个方案进行两两比较，依据 2.3 节介绍的方法分别计算方案间带权优势量 wd^+ 和带权劣势量 wd^-，利用式(1)计算方案间的比较优势度，建立比较优势度矩阵 $\boldsymbol{V}=(v_{pq})_{(m+1)\times(m+1)}$。

(3)基于步骤(2)所得比较优势度矩阵 $\boldsymbol{V}$，利用式(2)计算各方案总优势度，基于总优势度进行方案优先度排序，建立包括目标方案在内的方案排序向量 v'。

(4)基于决策矩阵 $\boldsymbol{R}$，计算各方案负提供指标百分比及负提供幅度，用二维数组 $SLO[i][0]$ 保存方案 i 的负提供指标百分比，$SLO[i][1]$ 保存方案 i 的负提供幅度。此步骤可与步骤(2)、步骤(3)同时进行。

(5)输出 v' 及服务商负提供参数，供用户最终决策。

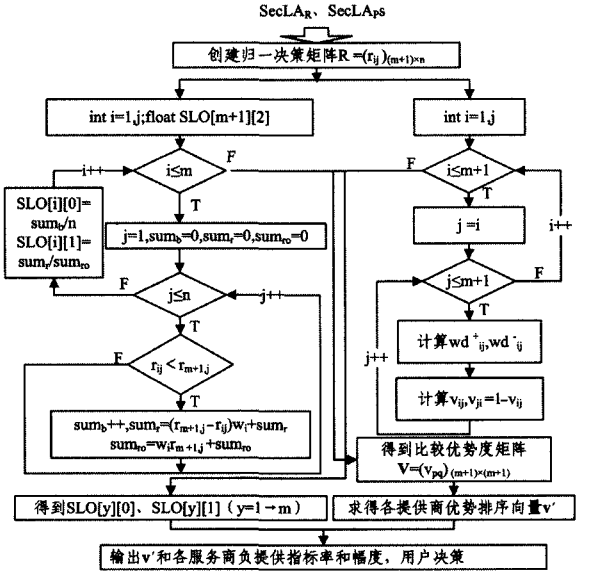

图 6 云服务商安全评价和决策流程

6 实验及分析

6.1 实验验证

云安全联盟 STAR 注册库[19]已收录世界范围内近 200 个主要云服务商的 CAIQ 评估报告，CAIQ 报告以工业界接受的方式记录了云服务商的安全控制[6]，本文基于这些真实报告数据对提出的方法进行验证。

假定某用户欲选择最安全的云存储商，重点关注 10 个控制域的安全等级，分别为："合规性"控制组下的审计规划、独立审计、第三方审计；"设施安全"控制组下的策略、用户访问、资产管理；"信息安全"控制组下的策略、职责分离、加密密钥管理、事件管理，同时平均分配重要性权重。STAR 库中云存

储商较多，在能够有效验证本文方法的情况下为简化计算，随机下载了8个云存储服务商的CAIQ评估报告进行实验，因主要考查云服务商安全属性，故暂不考虑其费用、性能等。按照CSA的要求，对8个云服务商作匿名处理，分别以SP1→SP8代替。具体过程如下：

(1)基于本文云安全合规性证据评分模型，针对备选云服务商CAIQ评估报告中的合规性证据，模拟专家评分，计算各服务商合规性可信度。

篇幅所限，表3仅部分列出SP1→SP3针对"合规性"控制组的合规性证据评分情况作为示范。例如，SP1的审计策略指标项M-01.1.1描述为"执行工业认证和第三方审计"，依据表1中Q-01.1所要求的审计策略"CloudAudit/A6 URI Ontology、CloudTrust…等"，只能算部分合规，记0.5分；但SP1能提供SSAE16等审计报告，证明审计流程是完整的，因此M-01.1.1项的完备性记1分，而SP3明确采用CloudAudit审计策略，所以M-01.1.1项合规性记1分，对第三方审计指标项M-01.2.1，SP1→SP3提供的审计报告均满足表1中Q-01.2所要求的标准，因此合规性及完备性均记1分。

表3　服务商关于云控制矩阵的合规性证据评分示例

指标M-	SP1			SP2			SP3		
	product/activity	合规性	完备性	product/activity	合规性	完备性	product/activity	合规性	完备性
01.1.1	执行工业认证和第三方审计	0.5	1	2次内部审计、1次SOC外部审计/年	0.5	1	CloudAudit、ISO27001：2005	1	1
01.2.1	SSAE16报告PCI DSS、ISO 27001证书	1	1	SSAE16、SOC 1报告	1	1	ISO27001：2005证书	1	1
01.3.1	渗透测试	1	0.3	Rapid7渗透测试、Qualys脆弱点扫描1次/周	1	0.5	风险评估系统	0.5	0.3
…	…	…	…	…	…	…	…	…	…

按此方法为SP1→SP8的所有控制组相关合规性证据打分，依据3.2节所述的服务商合规性证据总分方法，计算得到SP1→SP8的合规性证据分即为其合规性可信度值，最后表示为百分数形式。经计算，SP1→SP8的合规性可信度值分别为：71%、82%、83%、80%、58%、67%、74%、65%。

(2)利用(1)的计算结果对SP1→SP8 CAIQ报告记录的控制域安全等级进行修正，分别定义表示服务商安全offers和用户安全需求的标准描述$SecLA_{P}$s、$SecLA_{R}$，基于$SecLA_{P}$s、$SecLA_{R}$建立决策矩阵并归一化处理。

首先，对SP1→SP8 CAIQ报告中用户需求所关注10个控制域的安全等级进行修正，并计算修正后的平均值，如表4所列。在此基础上，利用SecLA模板建立SP1→SP8安全offers的标准描述$SecLA_{P1}$→$SecLA_{P8}$。其次，为使用户$SecLA_{R}$定义的控制域安全值更贴近实际，将控制域修正后平均值提供给用户参考，定义安全需求标准描述$SecLA_{R}$，其主要内容如图7所示。最后，基于$SecLA_{P}$s和$SecLA_{R}$建立决策矩阵$X=(x_{ij})_{9\times10}$，前8行表示SP1→SP8，第9行表示用户需求，各列分别代表10个控制域安全等级值，基于$\boldsymbol{X}$计算归一化决策矩阵$\boldsymbol{R}=(r_{ij})_{9\times10}$，如图8所示。

表4　SP1→SP8各控制域安全等级及平均值

指标	SP1× 0.71	SP2× 0.82	SP3× 0.83	SP4× 0.80	SP5× 0.58	SP6× 0.67	SP7× 0.74	SP8× 0.65	平均
CO-02	4.3→3.05	3.6→2.95	5.0→4.15	4.3→3.44	5.0→2.90	5.0→3.35	4.3→3.18	3.6→2.34	3.17
…	…	…	…	…	…	…	…	…	…
FS-01	5.0→3.55	5.0→4.10	5.0→4.15	5.0→4.00	5.0→2.90	5.0→3.35	5.0→3.70	5.0→3.25	3.63
…	…	…	…	…	…	…	…	…	…
IS-19	3.8→2.70	3.8→3.12	2.5→2.08	3.8→3.04	2.5→1.45	5.0→3.35	3.8→2.81	3.8→2.47	2.63
…	…	…	…	…	…	…	…	…	…

```
〈secag:SecurityDescriptionTerm wsag:Name="FileServer"
 wsag:ServiceName="FileShareService"〉
〈secag:ControlGroup Name="Compliance" ID="CO"〉
〈secag: ControlDomain Name = "AuditPlanning" ID = "CO-01"
 Weight="0.1" Level="4"/〉…
〈/secag:ControlGroup〉
〈secag:ControlGroup Name="FacilitySecurity" ID="FS"〉
〈secag:ControlDomain Name="Policy" ID="FS-01" Weight="0.1"
 Level="3.5"/〉…
〈/secag:ControlGroup〉
〈secag:ControlGroup Name="InformationSecurity" ID="IS"〉
〈secag:ControlDomain Name="Policy" ID="IS-03" Weight="0.1"
 Level="3.5"/〉…
〈/secag:ControlGroup〉
〈/secag:SecurityDescriptionTerm〉
```

图7　$SecLA_{R}$的部分描述

$$\mathbf{R}=\begin{bmatrix}
0.52 & 0.39 & 0.43 & 0.52 & 0.52 & 0.52 & 0.71 & 0.52 & 0.66 & 0.07\\
0.96 & 0.34 & 1.00 & 0.96 & 0.96 & 0.96 & 1.00 & 0.96 & 0.88 & 0.26\\
1.00 & 1.00 & 0 & 1.00 & 1.00 & 1.00 & 0.28 & 1.00 & 0.33 & 1.00\\
0.88 & 0.61 & 0.49 & 0.88 & 0.88 & 0.88 & 0.95 & 0.88 & 0.84 & 0.92\\
0 & 0.31 & 0.35 & 0 & 0 & 0 & 0.37 & 0 & 0 & 0.36\\
0.36 & 0.56 & 0.41 & 0.36 & 0.36 & 0.36 & 0 & 0.36 & 1.00 & 0\\
0.64 & 0.46 & 0.90 & 0.64 & 0.64 & 0.64 & 0.79 & 0.64 & 0.72 & 0.12\\
0.28 & 0 & 0.40 & 0.28 & 0.28 & 0.28 & 0.55 & 0.28 & 0.54 & 0.54\\
0.88 & 0.64 & 0.61 & 0.48 & 0.88 & 0.48 & 0.68 & 0.88 & 0.82 & 0.66
\end{bmatrix}$$

图8　归一化决策矩阵$\boldsymbol{R}$

(3)基于$\boldsymbol{R}$和式(1)计算方案两两间优势度值，建立比较优势度矩阵$\boldsymbol{V}$，如图9所示，利用$\boldsymbol{V}$根据式(2)计算各方案总优势度为$v_1=0.1049$、$v_2=0.1478$、$v_3=0.1307$、$v_4=0.1396$、$v_5=0.0677$、$v_6=0.0843$、$v_7=0.1134$、$v_8=0.0890$、$v_9=0.1227$，得到优先排序向量为$v'=(v_2,v_4,v_3,v_9,v_7,v_1,v_8,v_6,v_5)$；按图6所示算法流程，计算得各服务商负提供参数如表5所列。

$$\mathbf{V}=\begin{bmatrix}
0.5000 & 0.0156 & 0.2318 & 0.3329 & 0.9287 & 0.7590 & 0.4336 & 0.8028 & 0.0448\\
0.9844 & 0.5000 & 0.5857 & 0.5183 & 0.9862 & 0.9341 & 0.9457 & 0.9486 & 0.7349\\
0.7682 & 0.4143 & 0.5000 & 0.3919 & 0.9384 & 0.8203 & 0.6419 & 0.8530 & 0.5833\\
0.6671 & 0.4817 & 0.6081 & 0.5000 & 0.8409 & 0.9658 & 0.8540 & 0.7391 & 0.8965\\
0.0713 & 0.0138 & 0.0616 & 0.1591 & 0.5000 & 0.1884 & 0.0449 & 0.1164 & 0.2185\\
0.2410 & 0.0660 & 0.1797 & 0.0342 & 0.8116 & 0.5000 & 0.1189 & 0.5689 & 0.0509\\
0.5664 & 0.0540 & 0.3581 & 0.1460 & 0.9551 & 0.8811 & 0.5000 & 0.8840 & 0.3179\\
0.1972 & 0.0514 & 0.1470 & 0.2609 & 0.8836 & 0.4311 & 0.1160 & 0.5000 & 0.3204\\
0.9552 & 0.2651 & 0.4167 & 0.1035 & 0.7815 & 0.9491 & 0.6821 & 0.6796 & 0.5000
\end{bmatrix}$$

图9　比较优势度矩阵$\boldsymbol{V}$

表 5　服务商负提供参数

SLO	SP2	SP4	SP3	SP7	SP1	SP8	SP6	SP5
SLO_b	20%	20%	30%	60%	70%	100%	90%	100%
SLO_r	54%	12%	71%	32%	42%	51%	55%	82%

(4)依据 v'和各服务商负提供参数进行决策。通过排序向量 v'可知 v_2、v_4、v_3 总体上优于用户需求 v_9，如果仅依据 v'，应该选择 SP2，但通常情况下用户倾向于安全控制总体上有效而均衡，避免各控制域良莠不齐的情形，SP2 与 SP4 负提供指标率虽都为 20%，但 SP2 的负提供指标偏离幅度高达 54%，SP4 只有 12%，SP3 的两个负提供参数分别为 30%、71%，由此来看 SP4 的安全控制总体上更加协调均衡，并且优势度排序仅次于 SP2，$v4=0.1396$ 与 $v_2=0.1478$ 相差很小，因此决策选择 SP4 更加满足用户需求。

6.2　对比分析

(1)与 REM 方法[8]进行比较。REM 方法通过计算各服务商与用户需求目标值的欧氏距离进行决策，欧氏距离 $d(\boldsymbol{a},\boldsymbol{b})=\sqrt{Tr((\boldsymbol{a}-\boldsymbol{b})(\boldsymbol{a}-\boldsymbol{b})^{T}}$，基于决策矩阵 $\boldsymbol{R}=(r_{ij})_{9\times10}$ 计算结果如表 6 所列，按欧氏距离由小到大排序：

SP4<SP7<SP1<SP2<SP3<SP8<SP6<SP5

表 6　REM 方法排序结果

SP	SP4	SP7	SP1	SP2	SP3	SP8	SP6	SP5
d	0.6876	0.8128	0.9316	0.9976	1.2622	1.3144	1.3523	1.9548

虽然决策结果都是 SP4，但其排序存在明显问题，决策结果偶然性较大，SP7、SP1 负提供率分别是 60%、70%，一半以上指标低于用户需求，而 SP2、SP3 只有不到 30%的负提供率，但上述排序结果显示 SP7、SP1 比 SP2 、SP3 更好。由于指标是效益型，用户乐见指标正偏移，因此基于与用户指定值接近度进行决策的 REM 方法存在缺陷，本文方法克服了该缺陷。

(2)与简单线性加权方法比较。按备选方案与目标方案指标差简单线性加权[5]计算得排序结果，如表 7 所列，效用值由大到小排序：

SP2>SP4>SP3>SP7>SP1>SP6>SP8>SP5

决策结果为 SP2，未得到最理想结果。虽然排列顺序与本文相差不大，但该方法在指标差集结中会出现指标差正负直接对冲的情形，尤其当各指标权重差别较大、指标值波动很大时，正负指标差的相互抵销使得集结结果很难准确反映方案优劣。

表 7　简单线性加权方法排序结果

SP	SP2	SP4	SP3	SP7	SP1	SP6	SP8	SP5
值	0.1260	0.1188	0.0598	−0.0825	−0.2154	−0.3246	−0.3593	−0.5630

6.3　实验小结

实验表明，利用本文设计的云安全指标及评分模型，能够有效对各服务商安全属性进行量化，通过综合评价各服务商安全控制的 CCM 合规性证据及其质量，对其提交的安全等级指标进行校正，有效减小了所提交值可能存在虚假成分的影响，使其更贴近真实；基于所定义安全指标的层次结构设计的 SecLA 模板简洁实用，可以有效地描述用户安全需求及云服务商的安全 offers；基于实例数据的云服务商优劣比较、决策演算过程以及实验对比分析证明，改进后的比较优势度法不仅能较客观地反映各服务商安全控制的优劣，还能够就用户安全需求的满足情况进行量化评价。

结束语　本文研究了安全云服务商的选择问题。首先，基于云安全联盟的 CCM 及 CAIQ，定义了云安全量化指标及评分模型，已经取得了业界较广泛共识且颇具权威性的 CCM 及 CAIQ 为云安全指标建设提供了可靠基础。其次，设计了简洁的 SecLA 描述模板，为安全描述提供了载体。最后，提出了基于改进比较优势度法的云安全量化评价及决策方法，综合考虑指标重要性及其优劣幅度，分别计算优势与劣势，避免了优劣指标直接对冲，并乐见各指标与目标值的正偏移，增设负提供参数作为决策依据，使结果更符合用户预期。现实中选择云服务商时需要综合考虑功能、费用、性能和安全等因素，这是下一步的工作重点。

参 考 文 献

[1] Feng Deng-guo, Zhang Min, Zhang Yan, et al. Study on Cloud Computing Security[J]. Journal of Software, 2011, 22(1): 71-83 (in Chinese)
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] Thaweejinda J, Senivongse T. Semantic search for cloud providers with security conformance to cloud controls matrix[C]// Proceedings of the 2014 11th International Joint Conference on Computer Science and Software Engineering. IEEE, 2014: 286-291

[3] Bhensook N, Senivongse T. An assessment of security requirements compliance of cloud providers[C]// Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science(CloudCom). IEEE, 2012: 520-525

[4] Pumvarapruek N, Senivongse T. Classifying cloud provider security conformance to cloud controls matrix[C]// Proceedings of the 2014 11th International Joint Conference on Computer Science and Software Engineering. IEEE, 2014: 268-273

[5] Luna J, Vateva-Gurova T, Suri N, et al. SecLA-Based Negotiation and Brokering of Cloud Resources[M]// Helfert M. Cloud Computing and Services Science. Berlin: Springer International Publishing, 2014: 1-18

[6] Luna J, Langenberg R, Suri N. Benchmarking Cloud Security Level Agreements Using Quantitative Policy Trees[C]// Proceedings of the 2012 ACM Workshop on Cloud Computing Security Workshop. ACM, 2012: 103-112

[7] Hale M L, Gamble R. Secagreement: advancing security risk calculations in cloud services[C]// Procee-dings of the 2012 IEEE 8th World Congress on Services. IEEE, 2012: 133-140

[8] Luna J, Ghani H, Vateva T, et al. Quantitative Assessment of Cloud Security Level Agreements: A Case Study[C]// Proceedings of the 2012 International Conference on Security and Gryptography. Scitepress, 2012: 64-73

[9] Hale M L, Gamble R. Building a Compliance Vocabulary to Embed Security Controls in Cloud SLAs[C]// Proceedings of the 2013 IEEE 9th World Congress on Services. IEEE, 2013: 118-125

[10] Cloud Security Alliance. Cloud Controls Matrix [EB/OL]. (2015-04-25). https://cloudsecurityalliance.org/research/ccm

[11] Cloud Security Alliance. Consensus Assessments Initiative Questionnaire[EB/OL]. https://cloudsecurityalliance.org/research/cai

[12] Jiang Zheng-wei, Wu Xi-hong, Yang Pei-an, et al. Cloud Provider Selection Method Based on SecSLA[J]. Computer Engineering, 2013, 39(10): 1-5(in Chinese)
姜政伟，巫锡洪，杨沛安，等. 基于 SecSLA 的云供应商选择方法[J]. 计算机工程，2013，39(10)：1-5

[13] Andrieux A, Czajkowski K, Dan A, et al. Web services agreement specification (WS-Agreement) [EB/OL]. http://www.ogf.org/documents/GFD.107.pdf

[14] Henning R R. Security service level agreements: quantifiable security for the enterprise[C]// Proceedings of the 1999 workshop on New Security Paradigms. ACM, 1999: 54-60

[15] Bernsmed K, Jaatun M G, Meland P H, et al. Security SLAs for federated cloud services[C]// 2011 6th International Conference on Availability, Reliability and Security. IEEE, 2011: 202-209

[16] Ludwig H, Keller A, Dan A, et al. Web service level agreement (WSLA) language specification[R]. IBM, 2003: 815-824

[17] Lawrence A, Djemame K, Wäldrich O, et al. Using Service Level Agreements for Optimising Cloud Infrastructure Services[M]// Cezon M, Wolfsthal Y. Towards a Service-Based Internet. Berlin: Springer, 2011: 38-49

[18] Lin Zhi-ming, Mao Zheng-yuan. Comparison Method of Alternatives Advantage Degree for Multiple Attribute Decision-making [J]. Statistics and Decision, 2015(2): 44-47(in Chinese)
林志明，毛政元. 多属性决策的方案比较优势度法[J]. 统计与决策，2015(2)：44-47

[19] Cloud Security Alliance. Security, Trust and Assurance Registry (STAR)[EB/OL]. https://cloudsecurityalliance.org/star

[20] Chen Ai-zu, Tang Wen, Zhang Dong-li. Research on performance evaluation of system operation[M]. Beijing: Science Press, 2009: 56-60(in Chinese)
陈爱祖，唐雯，张冬丽. 系统运行绩效评价研究[M]. 北京：科学出版社，2009：56-60

[21] Li Xiao-lin, Zhang Li-na. Service Selection Strategies Based on Multi-Attribute Group Decision-Making Considering QoS Preference[J]. Computer Systems & pplications, 2014, 23(12): 249-252(in Chinese)
李小林，张力娜. 考虑 QoS 偏好的多属性群决策服务选择策略[J]. 计算机系统应用，2014，23(12)：249-252

(上接第 79 页)

此体系下无法得到准确的定义，如表 4 中第 2 类和第 7 类缺陷的表现形式项为空白。因此，如何进一步细化分类属性将是下一步研究工作的重点。

参 考 文 献

[1] Mei Hong, Wang Qian-xiang, Zhang lu, et al. Software Analysis: A Road Map[J]. Chinese Journal of Compters, 2009, 32(9): 1697-1710(in Chinese)
梅宏，王千祥，张路，等. 软件分析技术进展[J]. 计算机学报，2009，32(9)：1697-1710

[2] Piessens F. A Taxonomy of Causes of Software Vulnerabilities in Internet Software[C]// Proceedings of the 13th International Symposium on Software Reliability Engineering (ISSR'02). 2002: 47-52

[3] Aslam T. A Taxonomy of Security Faults in the Unix Operating System[R]. Technique Report TR-95-09, Department of Computer Science, Purdue University, West Lafayette, USA, 1995

[4] Jiwnani K, Zelkowitz M. Susceptibility Matrix: A New Aid to Software Auditing[J]. IEEE Security and Privacy, 2004, 2(2): 16-21

[5] Landwehr C E, Bull A R, McDermott J P. A Taxonomy of Computer Program Security Flaws with Examples[J]. ACM Computing Surveys, 1994, 26(3): 211-254

[6] Weber S, Karger P A, Paradkar A. A Software Flaw Taxonomy: Aiming Tools at Security[C]// Proceedings of the 2005 Software Engineering for Secure Systems(SESS'05). 2005: 274-281

[7] Tsipenyuk K, Chess B, McGraw G. Seven Pernicious Kingdoms [J]. A Taxonomy of Software Security Errors. IEEE Security & Privacy, 2005, 3(6): 81-84

[8] Power R. Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare[M]. Computer Security Institute, 1998

[9] Krsul I, Spafford E, Tripunitara M. Computer Vulnerability Analysis[R]. Technique Report TR-47909-1398, Department of Computer Science, Purdue University, West Lafayette, USA, 1998

[10] Wenliang D, Mathur A P. Categorization of Software Errors that Lead to Security Breaches[C]// Proceedings of the 21st National Information Systems Security Conference. 1998: 603-612

[11] Bishop M. A Taxonomy of Unix System and Network Vulnerabilities[R]. Technical Report CSE-95-8, Dept. of Computer Science, University of California at Davis, Davis, 1995

[12] Cohen F B. Information System Attacks: A Preliminary Classification Scheme[J]. Computers and Security, 1997, 16(1): 26-49

[13] Howared J D. An Analysis of Security Incidents on the Internet 1989-1995[R]. Pittsburgh, USA: Carnegie Mellon University, 1997

[14] Killourhy K S, Maxion R A, Tan K M. A Defense-centric Taxonomy Based on Attack Manifestations[C]// 2004 International Conference on Dependable Systems and Networks. IEEE, 2004: 102-111

[15] Hansman S, Hunt R. A Taxonomy of Network and Computer Attack[J]. Computers and Security, 2005, 24(1): 31-43

[16] DeMillo R A, Mathur A P. A Grammar-based Fault Classification Scheme and Its Application to the Classification of the Errors of Tex[R]. Technique Report, Department of Computer Science, Purdue University, West Lafayette, USA, 1995

[17] Bazaz A, Arthur J D. Towards a taxonomy of vulnerabilities [C]// Proceedings of the 40th Annual Hawaii International Conference on System Sciences. IEEE, 2007: 163

[18] CWE[OL]. http://cwe.mitre.org

[19] Fortify Software[OL]. http://www.fortify.com

[20] Huang Ming, Zeng Qing-kai. Research on Classification Attributes of Software Vulnerability [J]. Computer Engineering, 2010, 36(1): 184-186(in Chinese)
黄明，曾庆凯. 软件脆弱性分类属性研究[J]. 计算机工程，2010，36(1)：184-186