一种可量化的云计算平台安全评估模型

许剑，靳莉
（北京中电飞华通信有限公司，北京 100029）

摘　要：提出一种基于一致的 API 访问不同云的可量化安全评估模型。评估系统包括安全扫描引擎模块、安全恢复引擎模块、安全量化评估模块、可视化显示模块等。介绍了安全评估过程及修复过程，并基于 G-Cloud 平台进行了仿真验证。结果显示，所提模型可以通过可视化图形显示一个或多个云的动态安全扫描评分，能够引导用电用户修改配置、改进操作、修复漏洞，提高云用电资源的安全性。

关键词：云计算；可视化；可量化评估；安全可视
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020185

A quantifiable cloud computing platform security evaluation model

XU Jian, JIN Li
Beijing Fibrlink Corporation Company, Beijing 100029, China

Abstracts: A quantifiable security assessment model for accessing different clouds based on a consistent API was proposed. The evaluation system includes a security scan engine module, a security recovery engine module, a security quantitative evaluation module, and a visual display module. The progress of safety assessment and remediation was proposed, and simulation verification was carried out based on the G-Cloud platform. The results show that the proposed model can display the dynamic security scan scores of one or more clouds through visual graphics, which can guide electricity users to modify configurations, improve operations, repair vulnerabilities, and improve the security of cloud electricity resources.

Key words: cloud computing, visualization, quantifiable evaluation, security visualization

1　引言

随着云计算技术的不断发展，云服务日益普及，越来越多的组织开始使用云服务，亚马逊 AWS、微软 AZURE、阿里云等发展非常迅速，都拥有超大规模的数据中心。公共云、私有云、社区云、混合云都拥有大量用户。虽然云服务已经被广泛接受，但是仍然需要多方面考虑涉及云服务的安全和隐私问题，比如可信身份验证、适当的授权、数据安全和隐私。云用户无法知道其云服务是否安全以及数据是否可以安全地放置在不同的云中、不能全面把握安全形势、不能有效地

收稿日期：2019−12−20；修回日期：2020−06−27

修复安全问题。参考文献[1]提出了一种基于信任机制的方法来控制隐私暴露，通过使用信任机制提供的对个人信息公开的细粒度进行控制。参考文献[2]基于信任度量的信任决策，提出了一种适用于普适计算环境的全局信任管理方案，用于控制数据传输，加强数据的安全性和隐私。参考文献[3]通过在多用户网络上分割用户数据和操作实现更高程度的隐私保护。

目前，同一云中的主机、虚拟机、存储设备、网络设备等都有独立的安全扫描和修复方法。对于同一个云，其云用户、管理员和访问者很难掌握可访问和管理资源的整体安全情况，如果采用不同的服务，安全状况会更加复杂。因此，充分安全的云环境是紧急所需。但是面对不同的云服务提供商（cloud service provider，CSP）及其自身的私有云，CSP 也无法建立一个通用的安全管理机制来解决不同云之间的安全手段[4]。云用户需要一个 GSV（全局安全视图）或一个 USV（用户安全视图）处理所有可能由多个云组成的信息基础设施，所以通过创建 LSV、USV 和 GSV 改善安全状态是至关重要的。

综上所述，本文设计了一个可量化的云计算平台安全评估模型，包括安全扫描引擎模块、安全恢复引擎模块、安全量化评估模块、可视化显示模块等。安全评估模块由一组评估指标组成，这些指标分别对应计算、存储、网络、维护和应用安全等不同领域。每个指标包含漏洞、评分和修复方法 3 个方面。该系统采用一票否决的机制，对一个字段进行计分，并将汇总结果相加记为总分。云用户可以通过该安全可视化评估系统获得添加到用电信息资源库中的整个信息的安全情况，并通过评分来判断安全级别，该系统还可以指导用电用户修复其云的不足。

2 安全评价体系

安全可量化评估模块从计算安全集、存储安全集、网络安全集、运维安全集、应用安全集等方面定义了安全项目集合和可量化评估方法。评估系统模型可以根据监控资源的规模部署在单个服务器上，也可以部署在多个服务器上（作为一个集群）。

在实际应用中，评估系统的安全扫描引擎对用电用户的安全集合（计算安全、存储安全、网络安全、维护安全、应用安全等）进行扫描，得到不同安全项目的得分。扫描可采用串行或并行方式执行，并根据评价模型的定义对每个资源给出一个评分。对于一个云，总体安全性的可量化评估结果为 0 到最大值（最大值为 1、10 或 100）。当用电用户选择修复安全漏洞时，将调用修复引擎来检查漏洞并根据定义的规则[6]修复漏洞。

3 可量化的安全评估模型

3.1 安全类型集合及其指标

一个安全评估模型是由 $P=\{P_1, P_2, P_3, P_4, \cdots, P_N\}$ 等安全字段组成的集合。P_i 代表计算安全集合、存储安全集合、网络安全集合、维护安全集合、应用程序安全集合之一。

一个 P_i 包含不同的安全检查指标 P_{ij}，如式（1）所示，如物理服务器 OS、VM OS、容器系统和其他漏洞项，具体见表 1。

$$P_i=\left\{P_{i1}, P_{i2}, P_{i3}, P_{ij}, \cdots, P_{iM}\right\} \tag{1}$$

对于每个 P_{ij}，安全扫描引擎将检查一个用电用户的云资产集合 A 中对象当前的安全状态，如式（2）所示：

$$A=\left\{A_1, A_2, A_3, A_4, \cdots, A_N\right\} \tag{2}$$

$$A_i=\left\{A_{i1}, A_{i2}, A_{i3}, A_{i4}, \cdots, A_{iM}\right\} \tag{3}$$

对应于用户的物理机器、虚拟机等，如式（3）所示，A_{ij} 是检查其安全状态所需的对象之一。当处于安全检查状态时，扫描引擎将给出 $S=[S_{ij}, L_{ij}, O_{ij}]$。$S_{ij}$ 为最高分，L_{ij} 为安全漏洞级别，O_{ij} 为固

表 1　可量化安全评估模型的安全集合和指标

指标	集合名称	主要要素	子指标
P_1	计算安全集合	物理机操作系统（主机）	P_{11}
		虚拟机操作系统	P_{12}
		容器系统	P_{13}
		其他设备（GPU、FPGA 等）	P_{14}
P_2	存储安全集合	物理机器存储	P_{21}
		虚拟机存储	P_{22}
		对象存储	P_{23}
		块存储	P_{24}
		文件存储	P_{25}
P_3	网络安全集合	网络配置	P_{31}
		网络日志	P_{32}
		网络设备	P_{33}
P_4	维护安全集合	维护计划	P_{41}
		管理体系结构	P_{42}
		运行安全检查	P_{43}
P_5	应用程序安全集合	应用系统日志	P_{51}
		行为审计	P_{52}
		访问控制策略	P_{53}

定方式的一环。L_{ij} 的级别非常复杂，本文使用简化的方法，0 表示顶级弱点，1 表示没有安全风险。

一个 P_i 对应于一个 S_i，S_i 的总和为 MAX（1 或 100），如式（4）、式（5）所示：

$$S_i=\sum_{i=1}^{M}S_{ij} \tag{4}$$

$$\mathrm{MAX}=\sum_{i=1}^{N}S_i \tag{5}$$

其中，S_i 是根据计算安全、存储安全或网络安全的权重给出的一个固定分值，然后根据重要性和权重对每个安全检查项目给予一个 S_{ij} 评分。S_{ij} 也可以是一个动态评分，并随其包含的检查项的权重而变化。

3.2　安全评估过程

定义用电用户作为 UP 访问的资源集合。UP_i 对应于 P_i，如式（6）所示，P_i 定义了扫描 UP_i 所需的检查项。

$$\mathrm{UP}=\left\{\mathrm{UP}_1,\mathrm{UP}_2,\mathrm{UP}_3,\mathrm{UP}_4,\cdots,\mathrm{UP}_N\right\} \tag{6}$$

每个用户的资源视图都是全局资源视图的一个子集，拥有最高权限的管理员的资源视图是全局资源视图，如图 1 所示。

安全扫描引擎根据安全评估模型对用户资源视图进行扫描，可以通过串行或并行方式扫描检查项 P_{ij}，并给出一个实际的 US_{ij} 得分。

$$\mathrm{US}_i=\sum_{i=1}^{M}\mathrm{US}_{ij} \tag{7}$$

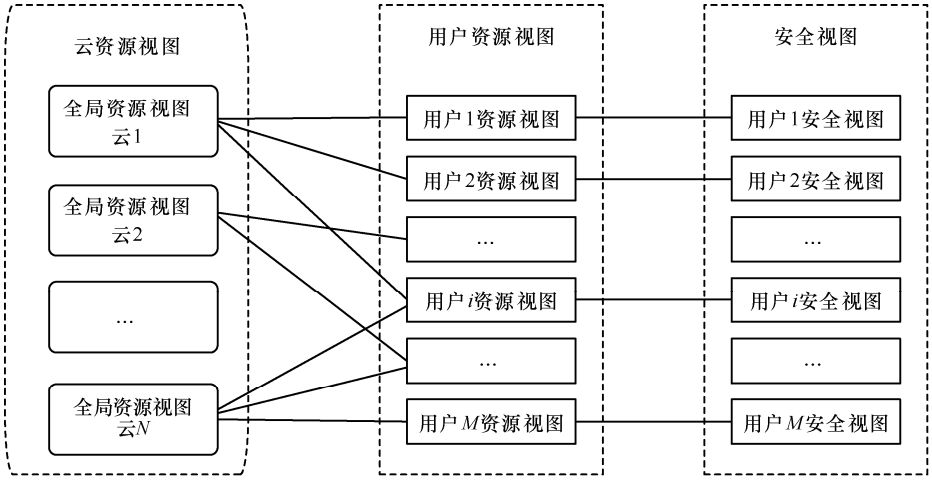

图 1　云资源、用户资源与用户安全视图的映射关系

云安全视图是用电用户云资源视图各种检查项的实际安全得分。管理员可以获取与总云对应的全局安全视图。为了提高一个用户对其云安全的关注程度，采用“一票否决”的策略来降低一个云存在严重漏洞时的得分。

“一票否决”策略与用户的安全视图相对应，总分之和是全局可量化的分数。通过利用直接总结、平均或“一票否决”策略计算总得分，在否决策略中，如果一个关键检查项的得分低于阈值，即 L_{ij} 为 0，则 US_i 为 0。

3.3 修复安全漏洞

当用电用户选择修复扫描的漏洞时，安全修复引擎将调用与 P_{ij} 对应的 O_{ij}。O_{ij} 是针对不同安全漏洞的修复规则对应的一个环节。维修引擎将对安全漏洞进行串行或并行修复。

对于一个管理员或普通用电用户，安全系统调用修复引擎修复安全漏洞，如下载补丁、更改配置、关闭服务或端口等。该安全修复引擎可以对漏洞进行静默修复，也可以通过用户界面与用户交互。修复后的发动机工作结束后，安全评估模型根据固定的结果[8]给出一个新的评分。安全评估系统的修复过程如图 2 所示。

4 仿真实验

量化安全评估系统的实施基于 G-Cloud 平台[15]。实验平台包含两个独立的云。其中一个云是基于 G-Cloud 操作系统建立的，另一个是基于 OpenStack 建立的，可以监视两个云并与相同的安全 API 进行交互。

通过实验来测试所提出的评估系统在单、双云平台上的工作情况，实验采用 3 000 个核心计算资源池、200 TB 存储资源池和 10 GB/s 网络资源池。实验平台包含两个独立的云：一个云基于 G-Cloud 操作系统，另一个基于 OpenStack。云 1 拥有 16 台物理机器（共计 512 个核心）作为计算资源，200 TB 存储资源；云 2 拥有 10 台物理机器（共 320 核）作为计算资源，150 TB 存储资源，这两个云共享 40 Gbit/s 的网络带宽，可以使用相同的安全 API 监视这两个云。

在云 1 中模拟一个私有云，运行状态、资源规模、安全评分、安全趋势。对于一个云平台，可以循环执行全局安全扫描。由于扫描模块可以访问具有相同 API 和拥有特权的 2 个云，所以可以在一个用户界面内扫描并显示两个云的安全情况。

可量化的评估手段也可以用来评估一个用户的安全状况。扫描模块只检查允许访问的用户资源的安全状态，然后给出安全视图来显示其状态。可量化的方法可以为管理员或用户提供一个直观的用户界面来了解其安全状态，并指导他们发现安全漏洞。这样可以取代一些非自动化的安全工具，提高安全维护效率。

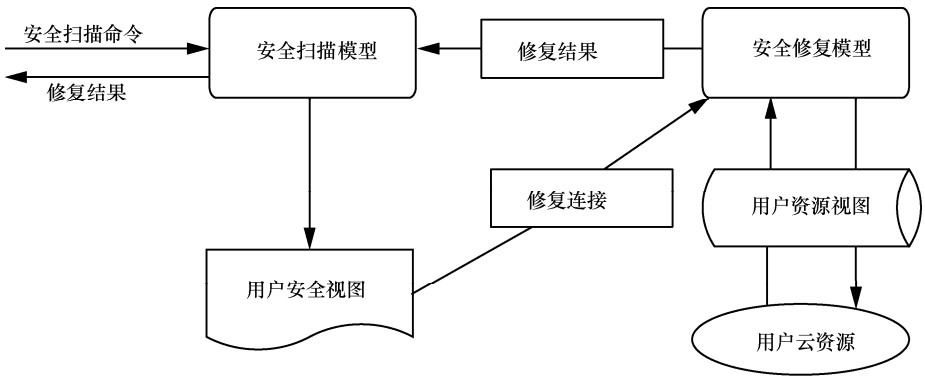

图 2 安全评估系统的修复过程

采用串行或并行方式进行安全性评估见表 2。如果采用串行扫描模式，则将安全扫描模块部署在一台服务器上，对每一个计算资源（作为物理服务器或虚拟服务器）、存储资源和网络资源进行逐一扫描。有时资源规模非常大、全局扫描时间非常长。因此可以采用并行模式部署安全扫描模块在不同的服务器上，一个云划分为不同的资源组织和扫描任务分配给不同的服务器，加快扫描速度和缩短时间，满足用户需求。对一个云或两个云中的一个用电用户的云资源的安全扫描也可以采用串行或并行方式。一般一个用电用户的安全视图可以在 30 s 内获取，在一个真实的云平台内，时间可以被用户接受。

表 2　用串行或并行模式进行安全扫描的时间成本（单位：s）

ID	扫描模型	串行扫描时间	并行扫描时间
1	单云全局扫描	3 607	806
2	云 2 全局扫描	5 700	1 211
3	单云用户扫描	121	30
4	云 2 用户扫描	260	50

5　结束语

针对单云和多云环境，提出了一种可量化的安全评估方法。可量化的评估模型为不同的云用户实现用电信息安全评估。通过可视化图形显示某云的动态安全扫描评分，引导用户修改配置、改进操作、修复漏洞，从而提高整个云平台的安全性。目前，可量化的安全评估系统可以在单云或多云环境下实现具有一致性的 API 和云操作系统的访问权限。以后的研究希望将评估系统扩展到其他基于相同安全评估系统的平台上，让需求侧资源监控和安全监控在统一的安全管理模式和用户界面下进行。

参考文献：

[1] 李鸿. 云计算环境下计算机信息安全与保密技术[J]. 信息与电脑(理论版), 2018(17): 163-164.
LI H. Computer information security and confidential technology in cloud computing environment [J]. Information and Computer (Theoretical Edition), 2018(17): 163-164.

[2] 刘恩军. 大数据云计算环境下的数据安全分析[J]. 网络安全技术与应用, 2019(5): 56-58.
LIU E J. Data security analysis under big data cloud computing environment [J]. Network Security Technology and Application, 2019(5): 56-58.

[3] NISHII K, TANIGAWA Y, TODE H. A search method of large-scale resources for providing efficient computing on a participating fine-granular cloud computing platform[C]// Proceedings of 2018 IEEE 7th International Conference on Cloud Networking (CloudNet). Piscataway: IEEE Press, 2018.

[4] 刘邵星, 杨尚跃, 杨树国. 基于云计算层次架构的安全框架研究[J]. 软件导刊, 2014(5): 162-164.
LIU S X, YANG S Y, YANG S G. Research on security framework based on cloud computing hierarchy [J]. Software Guide, 2014(5): 162-164.

[5] IKRAM M A, ALSHEHRI M D, HUSSAIN F K. Architecture of an IoT-based system for football supervision (IoT Football) [C]// Proceedings of 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). Piscataway: IEEE Press, 2015.

[6] 葛思江, 王利明, 李兆璨, 等. 云计算网络中基于隔离边界的安全审计体系研究[J]. 智能计算机与应用, 2019, 9(3): 16-22.
GE S J, WANG L M, LI Z C, et al. Research on security audit system based on isolation boundary in cloud computing network [J]. Intelligent Computer and Application, 2019, 9(3): 16-22.

[7] SINGH M, SINGH A, KIM S. Blockchain: a game changer for securing IoT data[C]// Proceedings of 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). Piscataway: IEEE Press, 2018.

[8] 吴宝江.云计算安全威胁及防护思路分析[J]. 通信技术, 2018, 51(8): 1961-1964.
WU B J. Analysis of cloud computing security threats and protection ideas [J]. Communication Technology, 2018, 51(8): 1961-1964.

[作者简介]

许剑（1983– ），男，北京中电飞华通信有限公司分公司总经理、高级工程师，主要研究方向为系统信息化安全、电力需求侧管理等。

靳莉（1981– ），女，现就职于北京中电飞华通信有限公司，主要研究方向为智能用电、智慧小区等。