

基于云物元分析法的军事云计算安全评估研究

郭保平, 程 建

(空军工程大学 信息与导航学院, 陕西 西安, 710077)

摘 要: 安全性是军事云计算得以深入应用和发展的关键因素. 首先分析了军事云计算安全评估的流程, 构建了安全评估的指标体系, 提出了一种结合云模型和物元分析对军事云计算的安全度进行综合评估的方法. 最后使用这种方法对实际的军事云计算平台进行了安全评估, 结果表明该方法可以较好地应用于信息安全评估领域.

关键词: 军事云计算; 云模型; 物元分析; 安全评估

中图分类号: TP393. 08

文献标识码: A

文章编号: 1000-7180(2016)07-0049-05

Safety Assessment of Military Cloud Computing Based on Cloud Model and Matter Element Analysis

GUO Bao-ping, CHENG Jian

(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract: Safety is the key factor of the application and development of military cloud computing. Firstly the process of safety assessment of military cloud was analyzed. And then the index system of safety assessment was structured. On this foundation, a comprehensive assessment method of the safety of military cloud using cloud model and matter element analysis was proposed. At last the safety assessment of an example of military cloud was implemented using this method, and the effectiveness of this method was shown by the results.

Key words: military cloud computing; cloud model; matter element analysis; safety assessment

1 引言

云计算因其强大的计算能力、良好的服务性和经济性等优势, 在信息技术领域得到了广泛的应用. 军事云计算已成为未来的发展方向. 但军事信息系统对于安全性的要求更高, 因而安全问题也成为军事云计算能否深入发展及应用的关键问题. 对于军事云计算进行安全评估, 应该符合军事信息系统安全评估和等级保护的相关法规标准, 采用定性和定量相结合的方式, 并且综合评估结果要能用于安全等级划分和安全策略的制定^[1].

目前, 针对传统的信息系统安全风险的研究已经较为深入, 但针对云计算安全风险的研究还刚处于起步阶段. 在云计算安全评估指标体系

的构建方面, 现有, 指标体系主要针对商业云计算领域, 对于军事云计算安全评估来说, 指标项过于复杂, 且有一定的冗余. 在安全评估的方法方面, 包括层次分析法^[2]、模糊综合评估方法^[3]、基于人工智能的评估方法^[4]等, 这些方法各自都有不同的特点及适用性.

本文在传统的军事信息系统安全评估理论的基础上, 研究军事云计算安全评估的问题, 利用云评估模型的随机性和模糊性, 结合物元分析方法对于矛盾指标的处理能力, 构建了一种云物元分析方法进行综合安全评估. 这种方法不仅可以应用于军事云计算的安全评估, 也可用于传统的信息系统安全评估.

2 军事云计算安全评估的流程

信息安全风险评估,即风险评估或安全评估,是信息安全风险管理的核心环节.其运用定性和定量等方法,分析信息和信息系统等资产面临的威胁和存在的脆弱性,提出相应的安全措施,并得出综合评价结果,为信息系统进行等级保护提供依据.军事云计算本质上还是一种军事信息系统,其安全评估也应该遵循国家及军队信息系统安全评估的法规及标准.依据国家标准《GB/T31167-2014 信息安全技术云计算服务安全指南》^[5]、《GB/T31168-2014 信息安全技术云计算服务安全能力要求》^[6]和军队信息安全风险评估的相关要求,构建出军事云计算安全评估的流程图,如图 1 所示.军事云计算安全评估的评估对象包括军事云数据中心、军事云客户端及通信网络链路.评估样本数据的获取,主要通过传感器从评估对象内部收集大量的关键安全数据,并对数据进行格式标准化、聚类合并及关联处理.对于一些难以量化的指标,通过专家打分的方式得到其评估样本数据.对于经过融合处理后的评估样本数据,综合利用漏洞库和知识库,运用综合评估方法,即可得到综合安全评估结果,并进行安全等级划分.若最终评估结果满足相应军事信息系统的安全要求,则评估结束.若不能满足要求,则提出相应的安全措施,进行安全整治,然后重新进行评估,直到军事云计算的安全度满足要求为止.

3 军事云计算安全评估指标体系的建立

3.1 安全评估指标体系的构建

军事云计算安全评估指标体系的构建,是在参

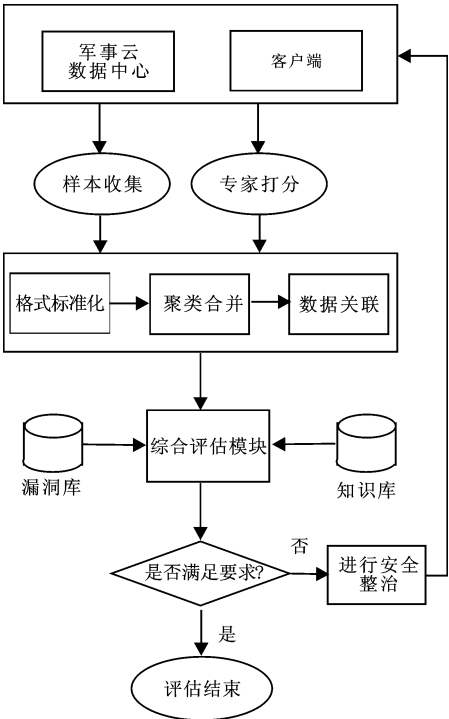


图 1 军事云计算安全评估流程图

考美国的 FedRAMP、云安全联盟的云计算关键领域安全指南 v3.0 及欧盟的云计算信息安全保障框架 IAF 的基础上,主要使用资产、威胁、脆弱性及已有安全措施的顶层模型,对军事云计算的安全指数进行综合评估.依据层次分析法的思想,按照科学性、完整性、层次性等评价指标选择的基本原则,将顶层的指标进行细分,如表 1 所示.表中,对于军事云面临的威胁,脆弱性和安全措施两个准则,其包含的因素可以作为子指标进行评估.脆弱性和安全措施下面的子指标还可以进一步细分.

表 1 军事云计算安全评估指标体系

准则层	指标层	描述及包含的因素
军事云计算资产 A ₁	机密性 A ₁₁	不泄露给未授权的访问者、实体和进程,或被其利用的特性
	完整性 A ₁₂	保持未经授权不能改变的特性
	可用性 A ₁₃	可被授权者访问并按需求使用的特性
军事云面临的威胁 A ₂	外部威胁 A ₂₁	网络攻击、物理攻击、社会工程学攻击
	内部威胁 A ₂₂	内部攻击、供应链攻击
	自身缺陷 A ₂₃	数据丢失或泄露、恶意使用云资源、多租户隔离
	环境因素 A ₂₄	旁路攻击、服务可用性
脆弱性和安全措施 A ₃	技术安全 A ₃₁	物理环境安全、通信网络安全、主机系统安全、应用数据安全
	管理安全 A ₃₂	设施安全管理、安全技术管理、人事安全管理、法规标准管理
	运行安全 A ₃₃	安全预警、监控和取证、应急响应、灾难恢复、安全服务

3.2 指标权重的确定

在综合评价中,指标权重确定的方法主要有主观赋权法和客观赋权法两种.因为在评价样本矩阵获取的过程中,有些指标属于定性评价,具有一定的主观性.故此处为了消除部分人为因素的影响,采取以下公式确定指标权重^[7]:

$$w_i = \begin{cases} 1 & i = 1 \\ \frac{1}{2} + \frac{\sqrt{-2\ln(\frac{2(i-1)}{n})}}{6} & 1 < i \leq \frac{n+1}{2} \\ \frac{1}{2} - \frac{\sqrt{-2\ln(2 - \frac{2(i-1)}{n})}}{6} & \frac{n+1}{2} < i \leq n \end{cases} \quad (1)$$

式中, n 为指标数; i 为排队等级, $i = 1, 2, \dots, m (m \leq n)$.排队等级是按指标重要程度所作的排列,通常由专家意见确定,指标越重要, i 取值越小.不同的指标若是重要程度相同,可以取相同的排队等级.将计算出的值进行归一化处理,即可得最终指标权重 w_i^* .

4 基于云物元分析的综合评估方法

4.1 云模型简介

云模型是在概率理论和模糊集合理论交叉渗透的基础上,将用人类自然语言描述的定性概念转换为定量描述的模型.云模型可以同时描述某个概念的模糊性和随机性.云模型可分为正态云、三角云、梯形云等不同的类型,其中正态云最接近社会和自然科学领域大量的模糊概念,应用范围最广.正态云有三个数字特征值,期望 E_x ,熵 E_n 和超熵 H_e . E_x 是云的重心位置,代表了模糊概念的信息中心值,是定性概念最重要的值; E_n 反映定性概念的模糊性,熵值越大,概念所分布的范围也越大,说明定性概念越模糊; H_e 是熵的熵,主要表征概念的随机性,反映了云的厚度.在军事云计算安全评估中,指标数据获取的数据源类型多样、环境复杂,具有很大的随机性和模糊性,使用云模型可以较好地反映待评估指标及评估标准的这种特征.

4.2 物元理论

物元理论是由我国学者蔡文创立的,是系统科学、思维科学与数学的交叉学科.物元分析中,把事物 N 、特征 c 及其量值 v 组成一个有序三元组 $R = (N, c, v)$ 作为描述事物的基本元,称为物元.其基本原理是将评价对象作为一个物元,根据各个特征的

理想值生成标准物元.通过比较待评价物元与标准物元,计算待评价物元对标准物元的隶属度,对各个方案进行排序^[8].物元分析方法,适用于存在或可以通过指标设定出理想或标准方案的评估对象,并且通过物元变换可将矛盾问题转换为相容问题进行综合评估.之所以在军事云计算安全评估中使用物元分析的方法,一是因为对于最终的军事云计算安全度综合评价结果,大量的待评价指标难免出现矛盾问题,二是需要运用评估标准对最终的评估结果进行安全等级划分.

4.3 用于军事云计算安全评估的云物元分析方法

云物元模型,是将物元模型中的 v 值用正态云模型 (E_x, E_n, H_e) 来代替,即

$$R = \begin{bmatrix} R_1 \\ \vdots \\ R_n \end{bmatrix} = \begin{bmatrix} N, c_1, (E_{x1}, E_{n1}, H_{e1}) \\ \vdots \\ c_n, (E_{xn}, E_{nn}, H_{en}) \end{bmatrix}.$$

用于军事云计算安全评估的云物元分析方法步骤如下所示.

(1)评价指标的获取与量化.

对于从实际军事云计算平台获取到的指标样本数据,因其量纲和数量级不同,需要首先按照物元分析法的思想,按照效益型、成本性和适中性三种类型对原始数据进行区间值化处理.对于不能直接获取到原始数据的指标,利用专家打分的方法,得到评价指标的量化值.

(2)安全等级标准的划分.

根据军事信息系统安全等级划分的要求,将安全等级划分为 5 级,分别为高、较高、一般、较低和低,安全等级和风险等级对应的区间划分如表 2 所示.其中风险度分值 = 1 - 安全度分值.

表 2 军事云计算安全度/风险度等级与分值

安全度等级	高安全	较高安全	一般安全	较低安全	低安全
分值	0.8~1	0.6~0.8	0.4~0.6	0.2~0.4	0~0.2
风险度等级	低风险	较低风险	一般风险	较高风险	高风险
分值	0~0.2	0.2~0.4	0.4~0.6	0.6~0.8	0.8~1

(3)构建待评价云物元.

根据军事云计算安全评估指标体系,将待评价的军事云计算总的安全度作为目标层云物元.目标层云物元下面,有三个准则层云物元,分别是军事云计算资产云物元、军事云面临的威胁云物元以及脆

弱性和安全措施云物元. 在准则层云物元之下, 还可以构建指标层云物元. 其中目标层云物元为

$$R = \begin{bmatrix} A_1 \\ A_2 \\ A_3 \end{bmatrix},$$

三个准则层云物元分别是

$$R_1 = \begin{bmatrix} A_1 & A_{11} \\ & A_{12} \\ & A_{13} \end{bmatrix}, R_2 = \begin{bmatrix} A_2 & A_{21} \\ & A_{22} \\ & A_{23} \\ & A_{24} \end{bmatrix},$$
$$R_3 = \begin{bmatrix} A_3 & A_{31} \\ & A_{32} \\ & A_{33} \end{bmatrix}.$$

(4) 确定云物元模型的经典域与节域.

根据传统的物元分析模型以及表 2 中安全度等级与分值的划分, 物元分析模型的安全度经典域分别是 $[0, 0.2)$ 、 $[0.2, 0.4)$ 、 $[0.4, 0.6)$ 、 $[0.6, 0.8)$ 、 $[0.8, 1.0]$, 节域为 $[0, 1]$. 这种划分方法中, 某个安全评价只属于一个非此即彼的安全等级, 忽略了安全等级边界处的模糊性以及各指标对各安全等级隶属度的随机性. 将云模型加入物元分析方法经典域划分的过程中, 各风险等级允许一定范围的重叠, 相同的属性值可能属于不同的安全等级, 不同的属性值对同一个安全等级的隶属度存在差异. 按照区间型数据 $[c_{\min}, c_{\max}]$ 转换为云模型的方法, 期望值 E_x 用区间的中值表示, 即

$$E_x = (c_{\min} + c_{\max})/2 \tag{2}$$

在转换过程中, 对于区间分界点处的数据, 既可以属于上一个安全等级, 也可以属于下一个安全等级, 故使用隶属度为 0.5 作为云物元模型经典域的分界处. 从而熵

$$E_n = (c_{\max} - c_{\min})/2.3548 \tag{3}$$

对于超熵 H_e , 可根据实际经验和专家意见, 选择合理的取值, 表示安全等级划分的随机性. 根据式 (2) 和式 (3) 计算出的 E_x 、 E_n 的值及 H_e 可以确定云的三个数字特征, 从而利用正向云发生器得到云物元模型的经典域和节域.

(5) 计算待评价云物元与安全等级之间的隶属度.

云物元的隶属函数主要用来对云物元指标和云物元安全等级的关系进行量化. 对于获取到的原始

指标数据, 由于其已经经过了量化和归一化处理, 此处使用确定数值与等级云之间隶属度计算的方法^[9]. 假设待评价指标的数值为 x , 将 x 作为云滴, 产生一个均值为 E_n 、标准差为 H_e 的正态随机数 E_n . 则指标值 x 属于该等级云的隶属度 $\mu(x)$ 计算方法为:

$$\mu(x) = \exp\left[-\frac{(x - E_x)^2}{2E_n^2}\right] \tag{4}$$

利用式 (4) 计算出指标层云物元对于等级云的隶属度, 结合式 (1) 计算出的指标权重, 对指标层云物元的隶属度进行加权, 可得到准则层云物元对各安全等级的隶属度:

$$\mu_j(R_i) = \sum_{p=1}^n w_{ip} \mu_j(I_{ip}) \tag{5}$$

式中, $\mu_j(R_i)$ 为第 i 个待评价的准则层云物元对第 j 个安全等级的隶属度, 此处 $i = 1, 2, 3; j = 1, 2, 3, 4, 5$. $\mu_j(I_{ip})$ 为第 i 个待评价的准则层云物元对应的第 ip 个指标层云物元对风险等级 j 的隶属度, w_{ip} 为其相应的指标权重. 更进一步, 可以利用计算出的准则层云物元的隶属度, 计算出军事云计算安全度总的云物元, 即目标层云物元对各安全等级的隶属度:

$$\mu_j(R) = \sum_{i=1}^3 w_i \mu_j(R_i) \tag{6}$$

(6) 确定基于云物元分析法的军事云计算安全等级.

根据隶属度最大原则, 由式 (6) 计算出的目标层云物元的隶属度最大的 $\mu_j(R)$ 对应的 j 即为军事云计算安全评估所得的安全等级.

5 实例分析

利用云物元模型对军事云计算安全度进行评估. 假设对于某军事云计算平台, 组织相关专家对其指标层安全度进行打分, 首先可得到待评价物元为

$$R_1 = \begin{bmatrix} A_1 & A_{11} & 0.4 \\ & A_{12} & 0.6 \\ & A_{13} & 0.8 \end{bmatrix}, R_2 = \begin{bmatrix} A_2 & A_{21} & 0.7 \\ & A_{22} & 0.5 \\ & A_{23} & 0.8 \\ & A_{24} & 0.3 \end{bmatrix},$$
$$R_3 = \begin{bmatrix} A_3 & A_{31} & 0.7 \\ & A_{32} & 0.6 \\ & A_{33} & 0.4 \end{bmatrix}.$$

利用式 (4), 可计算出云物元指标对各安全等级的隶属度, 如表 3 所示.

表 3 各云物元指标对各安全等级的隶属度					
二级指标	低	较低	一般	较高	高
A ₁₁	0.002 1	0.500 3	0.503 7	0.002 0	0.000 0
A ₁₂	0.000 0	0.001 8	0.500 4	0.500 8	0.002 0
A ₁₃	0.000 0	0.000 0	0.001 9	0.501 0	0.501 2
A ₂₁	0.000 0	0.000 0	0.062 9	1.000 0	0.062 6
A ₂₂	0.000 0	0.062 4	1.000 0	0.061 4	0.000 0
A ₂₃	0.000 0	0.000 0	0.001 9	0.501 0	0.501 2
A ₂₄	0.062 7	1.000 0	0.062 0	0.000 0	0.000 0
A ₃₁	0.000 0	0.000 0	0.062 9	1.000 0	0.062 6
A ₃₂	0.000 0	0.001 8	0.500 4	0.500 8	0.002 0
A ₃₃	0.002 1	0.500 3	0.503 7	0.002 0	0.000 0

利用式(1),可计算各二级指标及一级指标的权重,如表 4 所示.

表 4 军事云计算安全评估指标权重		
目标层	准则层	指标层
军事云计算安全度	军事云计算资产	机密性 $A_{11}(0.325\ 0)$
	$A_1(0.434\ 8)$	完整性 $A_{12}(0.500\ 0)$
		可用性 $A_{13}(0.175\ 0)$
	军事云面临的威胁	外部威胁 $A_{21}(0.370\ 9)$
	$A_2(0.282\ 6)$	内部威胁 $A_{22}(0.185\ 4)$
		自身缺陷 $A_{23}(0.258\ 2)$
		环境因素 $A_{24}(0.185\ 4)$
	脆弱性和安全措施	技术安全 $A_{31}(0.245\ 3)$
	$A_3(0.282\ 6)$	管理安全 $A_{32}(0.377\ 3)$
		运行安全 $A_{33}(0.377\ 3)$

由表 3 中各二级指标的云物元隶属度和表 4 中的指标权重,结合式(5)及式(6),可得军事云计算总的安全度对各安全等级的隶属度为(0.003 8,0.180 3,0.353 9,0.414 8,0.086 3),取隶属度最大值所对应的安全等级,即为军事云计算安全评估所得的安全等级.可得出,此军事云计算平台的安全度为较高,但安全度为一般的隶属度也不低,说明其安全方面还有较大的改进空间.

6 结束语

云计算在军事信息系统中的深入应用,需要首先解决安全问题,而科学合理的军事云计算安全评

估则是重中之重.首先分析了军事云计算安全评估的系统流程,构建了完整的军事云计算安全评估指标体系,并提出使用云物元分析的方法进行安全综合评估,得到军事云计算的安全等级.最后使用实例验证了该方法的可行性.下一步的工作包括,对指标体系进行进一步地完善,并设计军事云计算安全评估的软件,以提高评估过程的自动化水平.

参考文献:

[1] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing V3. 0 [EB/OL]. [2014-11-28]. <http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>.

[2] 赵刚,刘换.基于多层次模糊综合评判及熵权理论的实用风险评估[J].清华大学学报(自然科学版),2012,52(10):1382-1387.

[3] 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.

[4] 付钰,吴晓平,王甲生.基于模糊一组合神经网络的信息系统安全风险评估[J].海军工程大学学报,2010,22(1):18-23.

[5] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. GB/T31167-2014. 信息安全技术云计算服务安全指南[S]. 北京:中国标准出版社,2014.

[6] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. GB/T31168-2014. 信息安全技术云计算服务安全能力要求[S]. 北京:中国标准出版社,2014.

[7] 覃德泽.云重心理论在网络安全风险评估中的应用[J].计算机仿真,2011,28(3):174-177.

[8] 蔡文.物元模型及其应用[M].北京:科学技术文献出版社,1994.

[9] 胡涛,王树宗,杨建军.基于云模型的物元综合评估方法[J].海军工程大学学报,2006,18(1):85-88.

作者简介:

郭保平 男,(1981-),博士研究生,工程师.研究方向为军事云计算及其安全问题. E-mail:gil007@qq.com.

程建 男,(1962-),博士,教授,博士生导师.研究方向为信息化作战与建设.