基于属性安全值的强制访问控制模型

陈杰伟[1] 关 宇[2] 刘 军[3]
(解放军理工大学通信工程学院研究生 1 队 南京 210007)[1]
(解放军理工大学通信工程学院 南京 210007)[2] (解放军理工大学指挥信息系统学院 南京 210007)[3]

摘 要 通过对 ABAC 定义的细粒度属性进行量化映射,结合 BLP 和 Biba 强制访问模型的基本特点,试图定义一个与属性相关的安全值量化概念,然后以安全值为基础,构建一个可以计算的封闭环境。其次计算得到一个基于属性映射的安全值集合,从而符合 BLP 和 Biba 强制访问控制模型的基本条件。再对 BLP 和 Biba 模型进行进一步优化,使其契合属性安全值的特点,形成一个灵活的基于属性安全值的强制访问控制模型。

关键词 BLP,Biba,ABAC,属性,访问控制,模型
中图法分类号 TP393.0 **文献标识码** A

Mandatory Access Control Model Based on Safety Value of Attributes

CHEN Jie-wei[1] GUAN Yu[2] LIU Jun[3]
(Postgraduate Team 1 CCE,PLA University of Science and Technology,Nanjing 210007,China)[1]
(College of Communications Engineering,PLA University of Science and Technology,Nanjing 210007,China)[2]
(College of Command Information Systems,PLA University of Science and Technology,Nanjing 210007,China)[3]

Abstract By quantitatively mapping the fine-grained attributes defined by ABAC and by combining the basic features of BLP and Biba mandatory access models,an attempt is made to define a quantitative concept of security values related to attributes,and then a closed environment that can be calculated based on security values is built. Then a set of security values based on attribute mapping is calculated to meet the basic conditions of BLP and Biba mandatory access control model. Then BLP and Biba models are further optimized to fit the attribute security value and form a flexible mandatory access control model based on attribute security value.

Keywords BLP,Biba,ABAC,Attribute,Access control,Model

传统的访问控制模型一般较为注重实体的保密性或完整性,如 BLP[10] 和 Biba[11],基于传统的访问控制模型的研究一般是模型在实际应用中的研究,或者对模型的访问灵活性、保密性或者完整性进行改进性的研究:文献[1]对 BLP 模型引入多级安全标签以及安全迁移规则,使其满足实际系统开发的需要,并证明了其迁移规则对模型的有效性;文献[4]通过对 BLP 和 Biba 进行综合改进,使其能够适用于云计算数据环境;文献[2]通过将基于条件随机场的机器学习方法引入 BLP 模型中,然后再进行适当改进,使其在访问控制灵活性方面有所提高;文献[3]对 BLP 和 Biba 模型进行综合,构建了一个兼顾保密性和完整性的强制访问控制模型。但传统模型在实际应用中仍有不少问题,如安全等级的变化的问题,显然,一个主体或一个客体的等级不会是一成不变的,它是随时间和条件环境等不断变化的。为了适应主客体的动态变化,本文引入了基于属性的访问控制模型 ABAC[12],ABAC 策略是一个基于属性的细粒度的访问控制模型,其从属性方面对主体、客体、环境等都给出了细粒度的定义,基于 ABAC 的研究也大多从细粒度方面进行优化,或将 ABAC 模型优化应用到各类环境中。文献[6,8]对 ABAC 在云环境下的应用及其访问控制的灵活性问题进行了改进。文献[7]针对 ABAC 在大规模分布式网络中容易出现的问题,通过量化分析和一致性检测等方法进行有效控制,但是细粒度的访问控制并不关注主客体的保密性和完整性要求。文献[9]尝试通过对实体自身所拥有的属性的特征的辨识,将之归并到相应的域中,从而实现 BLP 规则下的强制访问控制。本文尝试建立一种兼顾属性和安全等级概念的元素-安全值,在此基础上,构建一个完整的封闭的可用来计算和比对的强制访问控制模型,实现信息系统的强制访问控制。

1 安全值的环境搭建

新的强制访问控制模型是在综合了 ABAC 基于属性细粒度的特点和 BLP、Biba 基于等级的特点的基础上,建立的一套强制访问控制策略模型,该模型的核心和基础是安全值的设置,其在安全值的基础上套用了 BLP 和 Biba 的访问控制策略,从而实现了基于属性的强制访问控制。具体策略定义如下。

定义 1 实体属性 $A(name,value,level)$ 是用来描述实体基本特征的变量,其中,$name$ 为实体属性的名称,$value$ 为实体属性的取值范围,$level=(lev(f),lev(i))$ 为权重,反映属性 A 的安全等级的高低,$lev(f)$ 为保密等级权重,$lev(i)$ 为完整性等级权重。

定义 2 新模型可抽象化为 $\{SA,OA,EA,AU\}$。SA,

陈杰伟(1987—),男,硕士生,主要研究方向为保密技术与管理,E-mail:378080658@qq.com。

OA，EA 分别为主体属性集、客体属性集和环境属性集，AU 为权限集合。

定义 3　全局属性集中，任一属性 A 的取值 a 可以归约为对应数值 α，则属性 A 的取值范围 $value=\{a_0,a_1,\cdots,a_{k-1}\}$，令其映射为数值集合 $\Phi=\{\alpha_0,\alpha_1,\cdots,\alpha_{n-1}\}$，$value=\Phi$，$\Phi\subseteq\Psi$，$\Psi=\{\beta_0,\beta_1,\cdots,\beta_{m-1}\}$ 是全局属性的取值范围，Ψ 为有限集。

例如：集合 $\Phi=\{\alpha_0,\alpha_1,\cdots,\alpha_{n-1}\}$，令 $\alpha\in(0,10]$，则 α 的取值范围为 0 到 10。α 越趋近于 0，对应属性值 a 的安全等级越低；α 越趋近于 10，对应属性值 a 的安全等级越高。

在实际信息系统中，我们可以根据实际情况，将属性值 a 映射为 $\alpha\in(0,1]$ 或 $\alpha\in(0,100]$，或者其他可计算的集合。

规则 1　约定全局属性 A 的权重 $level$ 的取值范围为一个可计算数值，且约定所有属性的权重的和为一个固定数值。

如：约定 $level\in(0,1]$，则 $0<level\leqslant1$，假定全局所有属性数量为 n，则 $\sum_{0}^{n-1}level_i=1$。

定义 4　安全值 $R=(F,I)$，F 为保密值，I 为完整性值。因此，SR 和 OR 分别为主体安全值和客体安全值。

规则 2　约定某一主体 S 的某一属性 A 的安全值 r 的计算公式为 $r=level\otimes\alpha$，则该属性保密性值为 $r(f)=lev(f)\otimes\alpha$，该属性完整性值为 $r(i)=lev(i)\otimes\alpha$，其中，$\otimes$ 代表一种运算，在实际系统中一般为乘法运算。

规则 3　存在某一主体 s，约定其安全值 $r(f,i)$ 的计算公式为：

$$r_s(f,i)=\begin{cases}f(s)=r_0(f)\oplus r_1(f)\oplus\cdots\oplus r_{k-1}(f)\\ i(s)=r_0(i)\oplus r_1(i)\oplus\cdots\oplus r_{k-1}(i)\end{cases}$$

其中，$\oplus$ 代表一种运算，实际系统中可用加法代替，以求出保密值和完整值。

约定主体与客体全局属性集一一相互对应，即主客体属性集为满同态映射，根据 ABAC 规则[6]，当主体创建客体时，客体继承主体属性集，因此借鉴 ABAC 规则可得如下规则。

规则 4　约定当某一主体建立某一客体时，客体的属性继承主体属性集的映射集。

规则 5　约定客体属性的安全值计算方法与主体的属性安全值计算方法相同且相互对应，即客体的属性的取值应与对应的主体的属性的取值相同，其所对应的保密等级权重和完整性等级权重也应与主体该属性的保密等级权重和完整性等级权重相同。因此，当某一主体属性与某一客体属性一一对应时，它们的安全值应当相同。

2　基于安全值的访问控制规则

2.1　相关概念

定义 5　S 为主体集合，O 为客体集合。$P=\{x\mid r,a,w,c,g,d\}$ 为操作方式集合，r 表示对客体只读不写，a 表示对客体只写不读，w 表示对客体既读又写，c 表示对服务客体做检查包括读操作，g 表示产生一个客体，d 表示删除一个服务客体。

定义 6　请求 $req:(s,o,x)\rightarrow G=\{y,n,er\}$，表示主体 s 请求通过 x 方式调用客体 o，y 表示授予 s 以 x 方式调用客体 o 的权限，n 表示拒绝 s 以 x 方式调用客体 o，er 表示出现授权错误。

定义 7　$b\in\{B\mid B=(S\times O\times P)\}$ 表示某个主体 s 有权以某种方式 x 调用某个客体 o；$b(s:x_1,\cdots,x_n)$ 是调用客体服务 o 的所有方式的集合。即：

$$b(s:x_1,\cdots,x_n)=\{o\mid o\in O\wedge[(s,o,x_1)\in b\vee\cdots\vee(s,o,x_n)\in b]\}$$

2.2　基于 BLP 和 Biba 的访问控制规则

BLP 访问控制规则：

根据 BLP 模型简单安全的特性和 $*$-特性，可以得出如下结论[3]。

$(1)b(s:a)\neq\varnothing\Rightarrow[\forall o\in b(s:a)[f_o(o)\geqslant f_c(s)]]$；

$(2)b(s:w)\neq\varnothing\Rightarrow[\forall o\in b(s:w)[f_o(o)=f_c(s)]]$；

$(3)b(s:r)\neq\varnothing\Rightarrow[\forall o\in b(s:r)[f_o(o)\leqslant f_c(s)]]$。

Biba 访问控制规则：

由于 Biba 访问模型是借鉴 BLP 访问模型而来，因此，根据 Biba 的访问规则，可得如下结论[3]。

$(1)b(s:a)\neq\varnothing\Rightarrow[\forall o\in b(s:a)[i_o(o)\leqslant i_c(s)]]$；

$(2)b(s:w)\neq\varnothing\Rightarrow[\forall o\in b(s:w)[i_o(o)=i_c(s)]]$；

$(3)b(s:r)\neq\varnothing\Rightarrow[\forall o\in b(s:r)[i_o(o)\geqslant i_c(s)]]$。

根据 BLP 和 Biba 强制访问控制规则特性，当主体等级与客体等级完全相同时，主体才能对客体进行既读又写的操作[10-11]。但是在新的模型中，主客体的安全特性是以安全值的概念体现的，安全值是一个相对精确的值，是主客体安全特性的精细化表达，如果直接套用原 BLP 和 Biba 的访问控制规则，那么只有当主体安全值与客体安全值相同时，主体对客体才能进行读写访问，这样就使得某一特定主体所能同时读写的客体的范围相对较少，甚至几乎为零，因为除了主体自身所创建的客体外，别的客体的属性值都不一定与其相同。为了解决这一问题，本文尝试建立一个安全限的概念，以增强本模型在访问控制时的灵活特性。

定义 8（安全限）

$$F:=\{(f_{s+},f_{s-},f_o,i_{s+},i_{s-},i_o)\mid f_{s+},f_{s-}\in C^S,f_o\in C^O,i_{s+},i_{s-}\in K^S,i_o\in K^O\}$$

其中，f_{s+} 为访问主体的保密值上限，f_{s-} 为访问主体的保密值下限，f_o 为访问客体的当前保密值，i_{s+} 为访问主体的完整值上限，i_{s-} 为访问主体的完整值下限，i_o 为访问客体的当前完整值。

结合安全属性值，对 BLP 访问规则进行如下优化：

BLP 的简单安全特性为当主体保密等级不小于客体保密等级时，主体可以对客体进行读访问；$*$-特性为当主体保密等级不大于客体保密等级时，主体可以对客体进行写访问。然而在新模型中没有保密等级的概念，仅有保密值的概念，为了保证安全访问的灵活性，定义新模型简单安全特性如下。

定义 9　当主体的保密值上限大于客体的保密值时，主体可以对客体进行读访问。同理，新模型 $*$-特性的定义如下：当主体的保密值下限小于客体的保密值时，主体可以对客体进行写访问。

推理 1　根据新模型保密值访问规则，可得如下推论：

$(1)b(s:a)\neq\varnothing\Rightarrow[\forall o\in b(s:a)[f_o(o)\geqslant f_{s-}(s)]]$；

$(2)b(s:w)\neq\varnothing\Rightarrow[\forall o\in b(s:w)[f_{s-}(s)\leqslant f_o(o)\leqslant f_{s+}(s)]]$；

$(3)b(s:r)\neq\varnothing\Rightarrow[\forall o\in b(s:r)[f_o(o)\leqslant f_{s+}(s)]]$。

结合安全属性值，对 Biba 访问规则进行如下优化。

定义 10　当主体完整值上限不小于客体完整值时，主体可对客体进行写访问；当主体完整值下限不大于客体完整值时，主体可对客体进行读访问。

推理 2 根据新模型完整值访问规则，可得如下推论：

(1) $b(s:a)\neq\varnothing\Rightarrow[\forall o\in b(s:a)[i_o(o)\leqslant i_{s+}(s)]]$；

(2) $b(s:w)\neq\varnothing\Rightarrow[\forall o\in b(s:w)[i_{s-}(s)\leqslant i_o(o)\leqslant i_{s+}(s)]]$；

(3) $b(s:r)\neq\varnothing\Rightarrow[\forall o\in b(s:r)[i_o(o)\geqslant i_{s-}(s)]]$。

推理 3 综合新模型保密值和完整值访问控制规则，可得如下推论：

(1) $b(s:a)\neq\varnothing\Rightarrow[\forall o\in b(s:a)[f_o(o)\geqslant f_{s-}(s),i_o(o)\leqslant i_{s+}(s)]]$；

(2) $b(s:w)\neq\varnothing\Rightarrow[\forall o\in b(s:w)[f_{s-}(s)\leqslant f_o(o)\leqslant f_{s+}(s),i_{s-}(s)\leqslant i_o(o)\leqslant i_{s+}(s)]]$；

(3) $b(s:r)\neq\varnothing\Rightarrow[\forall o\in b(s:r)[f_o(o)\leqslant f_{s+}(s),i_o(o)\geqslant i_{s-}(s)]]$。

2.3 相关规则补充

规则 6 约定安全限由主体的实际安全值计算而来，我们可以通过主体安全值取相应的倍数等来确定安全限，具体可根据系统实际情况来定。

例如：$f_{s+}=n_1\times f_s$，$f_{s-}=n_2\times f_s$，且 $n_1\geqslant n_2$。其中，f_s 为主体实际安全值，f_{s+} 为主体安全值上限，f_{s-} 为主体安全值下限，本例取 n_1，n_2 为它的安全值上下限系数，约定 n_1 大于或等于 n_2，从而求得主体属性安全值的上下限值。同理 $i_{s+}=k_1\times i_s$，$i_{s-}=k_2\times i_s$，且 $k_1\geqslant k_2$。

当主体 s 对客体 o 进行写操作 a 或读写操作 w 时，客体 o 的保密等级和完整性等级必然发生变化，因此有如下规则。

规则 7 约定当发生写操作时，若主体保密值高于客体保密值，则客体保密值应当相应增加；若主体保密值低于客体保密值，则客体保密值不变。若主体完整值高于客体完整值，则客体完整值保持不变；若主体完整值低于客体完整值，则客体完整值应当相应降低。

具体计算方法如下：

$$req:(s,o,a/w)\rightarrow G=y\Rightarrow\begin{cases}\text{if}:f_s>f_o\rightarrow f_o=k_1(f_s-f_o)+f_o\\ \text{if}:f_s<f_o\rightarrow f_o=f_o\\ \text{if}:i_o>i_s\rightarrow i_o=i_o-k_2(i_o-i_s)\\ \text{if}:i_o<i_s\rightarrow i_o=i_o\end{cases}$$

由规则 7 得，当主体保密值大于客体保密值时，客体保密值应当相应增加，增加量为主体保密值与客体保密值的差值再乘以相应的保密系数 k_1。同时。当主体完整值小于客体完整值时，客体完整值应相应减少，其减少量应为主体完整值与客体完整值的差值再乘以相应的完整系数 k_2。

关于系数的计算建议与主体的安全值相关，一般为正比和反比的关系，如当主体的保密值越高，则客体所应增加的量就越多；当主体的完整值越低，客体所应减少的量也应越大。

建议主客体安全值系数的计算如下：

$$k_1=\frac{f_s}{f_m},k_2=1-\frac{i_s}{i_m}$$

假定 f_m 和 i_m 为规则所允许的最高保密值和最高完整值，那么当主体 s 的保密值 f_s 越高，保密系数 k_1 越趋近于 1，则客体 o 的保密值增加的辐度就越大；当主体 s 的安全值 i_s 越低，完整系数 k_2 越趋近于 1，则客体 o 完整值降低的辐度就越大。当主体保密值低于客体保密值，或者主体完整值大于客体完整值时，客体的保密值和完整值不变，因此不于考虑。

3 访问控制架构设计

进一步优化新模型访问控制架构基于 ABAC 的访问控制架构，如图 1 所示。

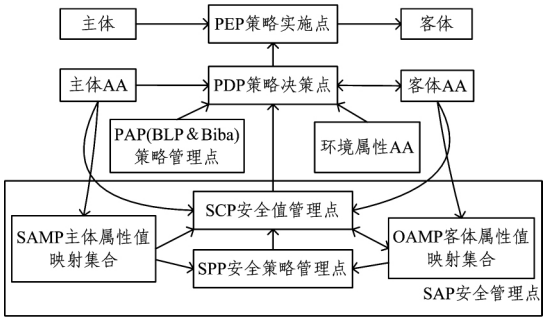

图 1 模型示意图

图 1 中，属性权威(Attributes Authority，AA)负责创建和管理主体、客体或环境的属性及安全值。策略实施点(Policy Enforcement Point，PEP)负责请求授权决策并实施决策。策略决策点(Policy Decision Point，PDP)负责评估适用的策略，并作出授权决策(允许/拒绝)。(BLP&Biba)策略管理点(Policy Administration Point，PAP)负责创建和管理访问控制策略，为 PDP 提供策略查询服务[5]。

安全管理点(Security Administration Point，SAP)负责建立和存储主体属性的映射值，对主体和客体安全值进行计算和管理，并将结果返回给 PDP，具体如下：

主体属性值映射集合(Subject Attributes Map Point，SAMP)负责创建和管理主体属性映射值集合，在系统建立时，建立一个与全局主体属性值一一对应的满同态映射，并限制属性值取值范围。

客体属性值映射集合(Object Attributes Map Point，OAMP)负责创建和管理客体属性映射值集合，在系统建立时，建立一个与全局客体属性值一一对应的满同态映射，并限制属性值取值范围。

安全策略管理点(Security Policy Point，SPP)负责创建和管理基于安全值的相关安全策略；负责维护和管理安全值计算所要遵循的一系列规则策略，限制和监督 SAMP 和 OAMP，当发生非法映射值时，及时做出反应并进行更正。

安全值计算点(Security Compute Point，SCP)负责全局所有主体和客体的安全值计算和管理。SCP 的任务主要分为两个方面，一方面在系统初始化时，SCP 从 AA 获取主客体所有属性值，从 SAMP 和 OAMP 获取相应属性值映射集合 $\Phi=\{\alpha_0,\alpha_1,\cdots,\alpha_{n-1}\}$，再从 SPP 获取相关安全策略，计算相关主客体安全值并返馈给 PDP。另一方面，SCP 还负责对主客体安全值进行存储管理，在 PDP 需要时直接将相应主客体安全值反馈给 PDP，而不需要再次计算。

4 新模型安全性分析

(1)关于访问控制的灵活性方面。新访问控制模型通过对安全值的定义来替代原访问控制模型对安全等级的定义，使得主客体之间的相互访问不再通过等级来进行比较，打破了等级的限制。原访问模型通过安全等级的定义使得各等级之间的集合局限化，如 BLP 强制访问模型[10]一般将主客体分为有限的多个等级，主客体之间的访问控制只能在这有限

(下转第 376 页)

计算机工程,2012,38(22):107-110.
[14] 罗明星,杨义先,王励成,等.抗窃听的安全网络编码[J].中国科学:信息科学,2010,40(2):237-246.
[15] EL ROUAYHEB S Y,SOLJANIN E. On Wiretap Networks II [C]// IEEE International Symposium on Information Theory, 2007(ISIT 2007). 2007:551-555.
[16] SILVA D,KSCHISCHANG F R. Security for wiretap networks via rank-metric codes[C]// IEEE International Symposium on Information Theory,2008(ISIT 2008). 2008:176-180.
[17] KOETTER R,KSCHISCHANG F R. Coding for Errors and Erasures in Random Network Coding[J]. IEEE Transactions on Information Theory,2008,54(8):3579-3591.
[18] ZHANG P,JIANG Y,LIN C,et al. Padding for Orthogonality: Efficient Subspace Authentication for Network Coding[C]// Infocom 2011. 2011:1026-1034.
[19] FANG Z,KALKER T,MEDARD M,et al. Signatures for Content Distribution with Network Coding[C]// IEEE International Symposium on Information Theory, 2007 (ISIT 2007). 2007: 556-560.
[20] TRACEY H,MEDARD M,KOETTER R,et al. A Random Linear Network Coding Approach to Multicast [J]. IEEE Transactions on Information Theory,2006,52(10):4413-4430.
[21] VAN LINT J H,WILSON R M. A Course in Combinatorics (2nd ed)[M]. Cambridge,U. K. :Cambridge Univ. Press,2001.

(上接第 350 页)

的几个等级的集合中进行比对,而新模型通过计算安全值,将主客体安全特性通过更加精细的方法表达出来,然后再通过安全限进行规范和约束,打破了集合的约束,将主体所能访问的客体范围与自身安全值相关,每个主体都拥有自己单独的可访问空间,而不再是有限的几个集合之间进行比较,增加访问控制的灵活度,使得主客体间的访问控制进一步规范化。

(2)关于安全限在访问控制中的安全方面。本文尝试将主体安全值放大到一个特定的范围,从而增加其可同时读写的客体的范围,增加访问控制的灵活性,但是,这同样存在部分隐患,当主体的保密值扩展为保密值限时,主体就可以在适当范围内同时读写部分比自身安全值高的或比自身安全值低的客体,这样势必会影响客体的安全特性,而本文采取的方法并不能详尽规避其中所有缺点,如隐蔽通道的问题(若主体通过特定方法将自身安全限系数无限放大,那么主体就可以读写全局所有客体)。另外,由于本文对客体安全特性的调整方法只允许保密值上行和完整值下行,全局的客体整体保密值趋势和完整值趋势固定,那么随着时间推移,势必会造成极端现象,从而导致只有极高保密值和极低完整值的主体才能读写客体,使得访问控制灵活性下降,因此这部分还需进行进一步研究与发展。

(3)关于访问控制模型计算量方面。本文借鉴 ABAC 细粒度访问控制的优点,尝试将属性值集合映射为可计算的特定值的集合,并对其计算方法进行约束定义,结合属性权重的特点,从细粒度方向对实体安全特性进行评估计算,从而得出一个可以用来相互比对的精确的数值,在这一过程中,需要大量的计算来保证读取的安全性,因此访问速度势必有所影响,但通过对安全值的计算,结合 BLP 和 Biba 的访问特点,既保证了基于属性的访问控制的细粒度特性,也保证了访问控制模型的灵活性,如果主体或客体属性发生变化,那么其对应的安全值同样也会发生变化,其可访问或可被访问的集合同样发生变化。

(4)关于强制访问控制规则方面。本文通过对 BLP 和 Biba 综合模型的改进,使其适应安全值环境需求,成功建立了一个基于保密值和完整值的强制访问控制模型,由于安全值是可以用来比对的,因此实体间的访问控制可以通过策略进行强制化,而安全值是系统通过属性值来对主客体进行安全评估的值,故主客体之间的访问控制可以完全通过 BLP 和 Biba 的访问控制规则来规范约束,具有很高的保密性和完整性。

结束语 本文通过对安全值计算环境的搭建,综合 BLP 和 Biba 的特点,建立了一个基于属性的兼顾保密性、完整性为一体的综合强制访问模型,通过对安全值上下限的定义,对信息上下行约束条件和规则的重新制定,不仅保证了访问模型的灵活性,同时又继承了 BLP 和 Biba 访问模型的优点,具有很高的实用性和安全性。但在属性权重和安全值的计算方面,还需要做进一步的考虑和完善;同时在环境属性的归约方面,本文也没有进行深入研究。下一步,在完善属性权重的设置和安全值计算的同时,要融入环境属性的变化和迁移特性以进一步提升综合强制模型的可用性和安全性。

参 考 文 献

[1] 徐亮,谭煌. BLP 改进模型的形式化描述及自动化验证[J]. 计算机工程,2013,39(12):130-135.
[2] 马萌,唐卓,李仁发,等. 基于条件随机场的改进 BLP 访问控制模型[J]. 计算机科学,2015,42(8):138-144.
[3] ZHANG J,YUN L J,ZHOU Z. Research of BLP and Biba dynamic union model based on check domain[C]// Preceedings of the seventh International Conference on Machine Learning and Cybernetics. Kunming,2008:12-15.
[4] 周向军. 基于 BLP/Biba 的混合云计算数据中心安全访问控制模型[J]. 信息安全与技术,2016,7(1):63-65.
[5] 于芳芳,马建红. 基于多优化技术的 ABAC 模型[J]. 计算机应用与软件,2015,32(11):312-316.
[6] 邹佳顺,张永胜,高艳. 云环境下基于使用控制的 ABAC 模型研究[J]. 计算机应用研究,2014,31(12):3692-3694.
[7] 倪川,黄志球,王珊珊,等. 基于属性的支持策略本体推理的访问控制方法研究[J]. 计算机科学,2015,42(3):96-101.
[8] 毋涛,张帆. 云计算下基于属性的访问控制方法[J]. 计算机系统应用,2016,25(2):231-234.
[9] BALAMURUGAN B,SHIVITHA G N,MONISHA V,et al. A Honey Bee Behaviour inspired novel Attribute-Based Access Control using Enhanced Bell-Lapadula Model in Cloud Computing[C]// International Conference on Innovation Information in Computing Technologies(ICIICT). IEEE,2015:1-6.
[10] BELL D,LAPADULA L. Secure Computer Systems:Mathematical Foundations and Model:echnical Report M74-244[R]. MITRE Corp. ,Bedford,MA 1973.
[11] BIBA K J. Integrity Considerations for Secure Computer Systems: EST TR-76-372[R]. ESD/AFSC, Hanscom AFB, Bedford, MA 1977.
[12] HU V C,FERRAIOLO D,KUHN R,et al. Guide to attribute based access control (ABAC) definition and considerations (draft)[J]. NIST Special Publication,2013,800(162).