计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200400013

云计算下基于动态用户信任度的属性访问控制

潘瑞杰　王高才　黄珩逸
广西大学计算机与电子信息学院　南宁 530004
(3035596023@qq.com)

摘　要　为便于对云中资源的管理,云计算环境通常会被划分成逻辑上相互独立的安全管理域,但资源一旦失去了物理边界的保护会存在安全隐患。访问控制是解决这种安全问题的关键技术之一。针对云计算环境多域的特点,提出了一种基于动态用户信任度的访问控制模型(CT-ABAC),以减少安全域的恶意推荐的影响并降低恶意用户访问的数量。在CT-ABAC模型中,访问请求由主体属性、客体属性、权限属性、环境属性和用户信任度属性组成,模型采用动态细粒度授权机制,根据用户的访问请求属性集合来拒绝或允许本次访问。同时,该模型扩展了用户信任度属性,并考虑时间、安全域间评价相似度、惩罚机制对该属性的影响。仿真实验结果表明,CT-ABAC模型能够有效地降低用户的恶意访问,提高可信用户的成功访问率。

关键词:云计算;可信;属性;访问控制;多域
中图法分类号　TP393

Attribute Access Control Based on Dynamic User Trust in Cloud Computing

PAN Rui-jie,WANG Gao-cai and HUANG Heng-yi
School of Computer and Electronic Information,Guangxi University,Nanning 530004,China

Abstract　In order to facilitate the management of resources in the cloud,the cloud computing environment is usually divided into logically independent security management domains,but there is a hidden danger in the loss of resources' physical boundary protection. Access control is one of the key technologies to solve this security problem. Aiming at the characteristic of multiple domains of cloud computing environment,this paper proposes an access control model (CT-ABAC) based on dynamic user trust to reduce the impact of malicious recommendations in the security domain and reduce the number of malicious users' visits. In the CT-ABAC model,an access request consists of subject attributes,object attributes,permission attributes,environment attributes,and user trust attributes. A dynamic fine-grained authorization mechanism is used to deny or allow this access based on the user's access request attribute set. At the same time,this model extends the attribute of user trust,and considers the impact of time,similarity between security domains,and penalty mechanisms on this attribute. Simulation results show that the proposed model can effectively reduce the malicious access of users and improve the success rate of trusted users.

Keywords　Cloud computing,Trust,Attribute,Access control,Muti-domain

1　引言

云计算改变了传统IT的运行方式,过去由各个企业专属的计算资源转变成了共享的"公共"计算资源,即企业将资源转交给了云服务提供商,这给资源的保护带来了不安全的因素,安全问题一旦出现极可能给企业带来高额的失败成本,严重的情况可能会导致企业市场的一败涂地。研究机构Cybersecurity Insiders于2018年的云安全报告中指出,云安全面临的第二大云威胁是不当的访问控制。因此,云计算下访问控制的设计显得尤为重要。

访问控制是一种用于资源保护的机制,是指在身份认证的基础上,根据授权策略决定是否允许用户对资源进行某种操作[1]。目前,国内外的学者结合云计算环境的特点,提出了比较多的访问控制方案。在现有的访问控制方案中,比较常用的是基于角色的访问控制(Role-based Access Control,RBAC)和基于属性的访问控制(Attribute-based Access Control,ABAC)。

基于角色的访问控制是在用户和权限之间引入角色这一层次,形成以角色为中介,授予主体能完成本次访问的最小权限[2]。因此,基于角色的访问控制比传统的MAC[3](Mandatory Access Control)和DAC[4](Discretionary Access Control)更具灵活性,且更易于管理。但是,把基于角色的访问控

到稿日期:2020-04-07　返修日期:2020-07-15　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61562006);广西自然科学基金(2016GXNSFBA380181)
This work was supported by the National Natural Science Foundation of China(61562006) and Natural Science Foundation of Guangxi,China (2016GXNSFBA380181).
通信作者:王高才(wanggcgx@163.com)

制应用到云计算环境有诸多限制。一方面，随着越来越多的用户加入云环境中，这些用户购买不同的云服务，其分配的角色也可能不同，从而产生了大量的用户-角色、角色-权限关系，这些关系冗杂且难以管理，极大地增加了管理员的工作量。另一方面，基于角色的访问控制只是在身份验证的可靠性和合法性的基础上给用户分配角色，并未对用户的可信性进行评估，也未对用户的访问过程进行监控，因此存在一定的安全问题。

基于属性的访问控制[5]是根据访问者的属性组合是否符合访问控制规则来做出决策的，在授权的过程中不仅要考虑主体属性、客体属性和权限属性，还要考虑用户访问时的环境属性，因此它既可以满足细粒度的访问控制和授权需求，也能适应云计算动态变化的环境。基于属性的访问控制避免了基于角色的访问控制中角色激增带来的关系管理复杂的问题，但是，仅仅将用户的主体属性、客体属性、权限属性、环境属性作为评判能否成功访问的标准是不完善的，同时因为其无法对用户的可信性进行评估，所以同样存在安全问题。

本文针对基于属性的访问控制出现的问题，结合云计算环境多域的特点，提出了一种基于动态用户信任度的属性访问控制模型(ABAC based on dynamic user trust incloud computing，CT-ABAC)，该模型在基于属性的访问控制模型的基础上扩展了用户信任度属性，并提出针对用户信任度属性的评估方法，以提高云计算环境的安全性。

本文第 2 节对相关研究工作进行总结；第 3 节介绍 CT-ABAC 访问控制模型；第 4 节是信任度计算；第 5 节是实验分析；最后总结全文。

2 相关工作

为提高云计算环境的安全性，保障云资源不受非法访问，许多国内外的研究工作者开展了对访问控制的研究。文献[6-8]对基于角色访问控制模型的时间角色映射、角色挖掘进行了研究，在一定程度上提高了模型的灵活性和动态性。文献[9]提出了一种基于标签访问控制的 ABAC 模型，该模型通过枚举用户属性(uLabel)和对象属性(oLabel)来表达授权策略。文献[10]提出一种受限的访问控制模型 rHGABAC (Restricted ABAC with Group Attributes and Attribute Hierarchies)，该模型在 ABAC 模型上进行扩展，形成了包括用户、对象组以及组层次受限的 HGABAC 模型。该模型使用 NIST(National Institute of Standards and Technology)策略机(Policy Machine，PM)来实施 rHGABAC 授权体系的结构。文献[11]在用户和用户属性之间、客体和客体属性之间引入角色这一概念，以在 ABAC 模型中实现最小特权。文献[12-13]主要针对基于属性的访问控制策略冲突、策略迁移过程出现的问题提出解决方案。但以上的研究都没有考虑到访问过程中主体的可信性以及云计算下跨域访问的问题，存在一定的安全隐患。

为了提高访问控制的安全性，国内外学者已经做了大量的研究，但是就可信度评估的具体方法，至今未达成一致。文献[14]提出一种基于信任角色的访问控制模型(Trust Role Access Control Model，T-RBAC)，该模型通过在角色映射和权限授予之前判断用户信誉的方式来阻止一些低信誉用户的非法攻击，增强访问的安全性，但是该模型的信誉值是预先定义好的，因此缺少灵活性和动态适应性。文献[15]提出了基于用户行为信任的访问控制模型，并考虑了时间、权重和 QoS 等因素对模型的影响，通过分析用户的行为特征来完成用户信任度的计算，该模型能够有效地防止用户访问非法资源。文献[16]提出一种基于信任管理和角色的信任模型 TrustR-BAC，该模型利用两个域之间的安全策略来计算直接信任度和推荐信任度，提高了系统的效率和可靠性。文献[17]提出基于信任和信誉的 RBAC 模型，该模型实现了一种新的计算直接信任值的方法，并考虑到一些安全指标，能够很好地抵御基于信任的 RBAC 模型的安全威胁并且具有良好的可扩展性。文献[12-14,16]在基于角色的访问控制的基础上进行扩展，但仍难以摆脱 RBAC 本身的限制。为了摆脱 RBAC 的限制，同时阻止恶意用户的攻击，提高访问的安全性和灵活性，文献[18]把基于属性的访问控制和信任管理相结合，提出混合云和私有云访问的信任计算方法，该模型具有比较好的灵活性和扩展性，但是并未考虑到多域和惩罚机制。

本文针对以上研究存在的问题，结合云计算环境多域的特点，提出了一种基于动态用户信任度的属性访问控制模型，该模型在基于属性的访问控制的基础上扩展了信任属性概念，并提出了计算用户信任度的新方法，即通过考虑安全域与安全域之间的评价相似性、时间的有效性、惩罚机制对用户信任度属性值的影响，来减少恶意安全域的推荐行为和恶意用户的访问，以提高访问的安全性。

3 CT-ABAC 访问控制模型

3.1 模型相关定义

基于动态的用户信任度的属性访问控制模型在基于属性的访问控制的基础上扩展了用户信任度属性，以衡量用户的可信性，因此它同样采用实体属性进行授权，并根据主体、客体、环境、用户信任度属性的属性值来判断用户是否满足授权规则的属性组合，以决定是否授予其主体访问客体的权限。本文根据 NIST 于 2014 年发布的关于 ABAC 的标准[19]和文献[20]对融合可信模块的 CT-ABAC 模型做出以下定义。

定义 1 CT-ABAC 模型的形式定义由五元组(S,O,E,P,T)组成。S,O,E,P,T 分别表示主体(Subject，S)、客体(Object，O)、环境(Environment，E)、权限(Priviledge，P)、用户信任度属性(Trust，T)。

定义 2(属性(Attribute，Attr)) 用于区分一个实体与其他实体的标识，可以被抽象定义为三元组$\langle Attr,Val,R(val)\rangle$以表示属性、属性值、属性取值范围的关系。本文用 SA,OA,EA,PA,TA 分别表示主体属性、客体属性、权限属性、环境属性、用户信任度属性。

定义 1 中的主体、客体、环境、权限、用户信任度都具有属性。主体属性一般包括用户名称、年龄等；客体属性一般为资源所在的安全域的名称、资源的创建者等；环境属性指的是用户访问的时间、地点等；权限属性通常是读、写、执行、修改等；用户信任度属性是根据用户的历史访问情况计算的数值，其取值范围为[0,1]，该值越大，则该用户越可信。

定义 3 云计算环境下可用作安全互操作的管理域 $SD=\{sd_1,sd_2,sd_3,\cdots,sd_s\}$。$sd_1,sd_2,\cdots,sd_s$ 分别表示相互独立的安全域。

定义 4（基于属性的访问控制请求（Arribute-based Access Control Request，AAR）） 由五元组 $Req(SA,OA,EA,PA,TA)$ 构成，表示主体进行访问的属性信息，作为授权的依据。

定义 5（策略（Policy）） 定义了在允许的环境条件下主体可以对客体执行的操作，其表现形式如下：

$$(permit,deny)\leftarrow(Attr(SA),Attr(OA),Attr(EA),Attr(PA),Attr(TA))$$

其中，$Attr(SA),Attr(OA),Attr(EA),Attr(PA),Attr(TA)$ 分别表示主体、客体、环境、权限、用户信任值属性的取值范围。若访问请求的属性信息符合策略规定的属性范围，则允许访问；否则，拒绝访问。

3.2 模型的建立

3.2.1 CT-ABAC 模型

云计算环境中，由于主体所在范围的广泛性，用户进行跨域访问资源的需求越来越频繁。为增强访问控制的安全性，本文提出了如图 1 所示的访问控制模型 CT-ABAC，该模型主要将可信管理（Trust Management，TM）和与信任值计算有关的模块（Domain Management Center，DMC）融入到基于属性的访问控制模型中。

假设 sd_1 和 sd_2 安全域都采用基于属性的访问控制模型，当 sd_1 安全域的用户发出访问 sd_2 安全域的客体的请求时，可信管理就会从跨域管理中心获取该用户的历史访问记录信息（History Information，HI）和域集信息（Domain Informaiton，DI），并计算用户的综合信任值，以扩展访问控制请求，并将其作为主体是否可以访问客体的依据。如果该用户的主体属性、客体属性、权限属性、环境属性、用户信任度属性的属性值都符合访问控制策略，就允许访问资源；否则，拒绝访问该资源。

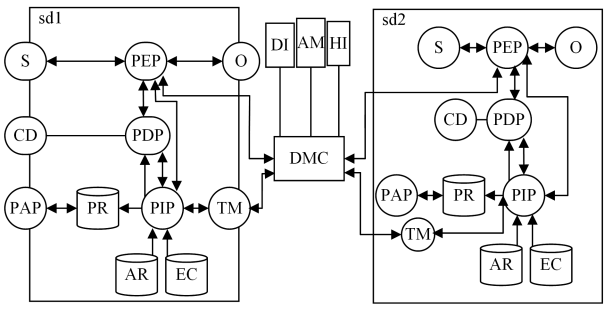


图 1 跨域访问控制

Fig. 1 Cross-domain access control

该模型各模块的功能如下。

（1）策略执行点（Policy Enforcement Point，PEP）

将主体发出的原始访问请求转变成基于属性的访问请求。同时，PEP 执行 PDP 的决策结果，即拒绝或允许本次访问请求。

（2）策略管理点（Policy Administrate Point，PAP）

对访问控制的规则进行管理，为 PDP 的策略决策提供规则支持。

（3）策略信息点（Policy Information Point，PIP）

对一些属性信息进行管理（如主体属性、客体属性、权限属性、环境属性等），并从可信管理获取用户的信任度属性。此外，PIP 也为 PEP 构建 AAR（Attribute-based access control request）提供属性支持。

（4）策略判定点（Policy Decision Point，PDP）

从域管理中心获得域集信息做出是否跨域（Cross Domain，CD）的决定，并根据访问控制规则做出授权决策。

（5）可信管理

通过跨域管理中心获取用户历史访问信息来计算该用户的综合信任度，并为 PEP 构建基于属性的访问控制请求提供用户信任度属性。

4 信任度模块的计算机制

本文假设：云计算环境下的访问控制均是采用基于属性的访问控制模型，安全域 sd_i 的主体 s_i 要访问安全域 sd_j 的客体 o_j，为区分主体 s_i 是否是恶意用户，我们引入信任的概念，信任度就是判定安全域 sd_j 对安全域 sd_i 的主体 s_i 的信任程度。以 s_i 和 sd_j 历史交互记录为凭据来计算直接可信度，s_i 访问 sd_j 之前访问的其他安全域对 sd_j 安全域都有推荐作用，本文引入评价相似度的概念，来评估参与推荐的安全域的可信度，以及此安全域是否存在恶意推荐的情况，同时考虑时间因素、惩罚机制对用户信任度属性值的影响。

4.1 信任度的计算

4.1.1 滑动窗口机制

云计算环境是一个不断变化、高度动态的环境，安全域对主体的信任程度会随着时间的推移而发生变化，因此在超过一定时间后，主体访问过安全域的历史记录对本次访问已经没有任何参考价值，为保证计算数据的时效性，本文引入时间窗口机制，数据的计算只采用窗口（win）内的数据，忽略窗口外的数据。每交互一次，时间窗口就向前移动一次，窗口内的数据都处在不断变化之中，其可信度也会随着窗口的移动权重的降低而降低，直至没有参考价值。滑动窗口模型如图 2 所示。

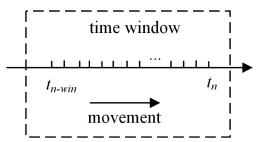


图 2 滑动窗口的机制

Fig. 2 Sliding window mechanism

式（1）用数学模型表示出访问控制中的滑动窗口机制。

$$\partial_{(t)}=\begin{cases}t, & t\leqslant N\\ (t-\left\lfloor\frac{t}{N}\right\rfloor*N)+(\left\lceil\frac{t}{N}\right\rceil*N-t), & t>N\end{cases}\tag{1}$$

该函数主要用于把窗口外的数据转换成窗口内的数据，其中，t 表示用户当前历史访问行为与用户第一次访问的间隔次数，N 表示窗口的长度。

4.1.2 信任衰减函数

信任是一个不断变化的过程，起初的高信任值也会因为时间过长而变得不太可信，云计算的访问控制中存在用户恶

意刷信任值的情况，当恶意用户获得足够高的信任值后，其再对资源进行恶意访问就会对安全域内的资源造成更大的危害。为避免这种情况，在 CT-ABAC 模型中引入时间衰减函数 $W_{(t)}$，以减少历史访问数据对当前访问的影响，具体公式如下：

$$W_{(t)}=\begin{cases}1-\zeta, & t=n\\ w_{(t-1)}+\dfrac{1}{n}, & t<n\end{cases} \tag{2}$$

其中，n 表示窗口内某一用户可能进行访问的总次数，t 表示用户当前历史访问行为与用户第一次访问的间隔次数，若 $n>win$，则通过式(1)把该数据转换成 win 内数据。ζ 为任意小的正数，用于调节信任度衰减的范围，用户历史信任度的权重会随着访问次数的增加而减小。

4.1.3 惩罚机制

信任级别越高的用户，其进行恶意访问对客体资源造成的危害越大，因此，本文设计了针对用户的信任级别进行惩罚的机制。信任级别的划分如表 1 所列，惩罚函数如式(3)所示。$p=A\sin(\dfrac{l_i}{2*L}*\pi)$ (3)

其中，A 为调节因子，用于控制惩罚的力度，惩罚力度越大，A 的值就越大；L 为所划分的信任等级的总数；l_i 为用户当前所处的信任等级，随着用户访问客体的进行，其值处于动态变化中，因此其信任级别也处于动态变化之中。

表 1 信任等级

Table 1 Trust level

Comprensive Trust Level	Rank
(0,0.3]	Lower
(0.3,0.5]	Low
(0.5,0.7]	Medium
(0.7,0.9]	High
(0.9,1]	Higher

4.1.4 安全域之间的相似度

定义 6 评价相似度用于刻画两个安全域 sd_i 和 sd_j 对共同的访问者信任程度的相似性，sd_i 和 sd_j 相似程度越高，sd_i 和 sd_j 对共同访问的用户的评价就越相似，sd_j 向 sd_i 的推荐越具有可信性。本文采用余弦相似度，即两个向量夹角的余弦来表示两个向量的相似度，即：

$$sim(i,j)=\frac{\sum_{k=1}^{N}SD_{ik}*SD_{jk}}{\sqrt{\sum_{k=1}^{N}|SD_{ik}|^2}*\sqrt{\sum_{k=1}^{N}|SD_{jk}|^2}} \tag{4}$$

其中，N 表示主体 s_k 在访问目标 sd_i 安全域之前访问过的其他安全域的总数，SD_{ik} 为 sd_i 安全域对用户 s_k 的评价，SD_{jk} 为 sd_j 安全域对用户 s_k 的评价。SD_{ik} 的具体公式如下：

$$SD_{ik}=\frac{S_{ik}}{F_{ik}+S_{ik}} \tag{5}$$

其中，S_{ik} 表示 s_k 用户成功访问 sd_i 安全域的次数，F_{ik} 表示用户 s_k 访问 sd_j 安全域失败的次数。

本文将主体 s_i 在访问安全域 sd_j 之前，与安全域 sd_j 评价相似度比较高的其他安全域对安全域 sd_j 的推荐作为评估安全性的一部分。若 $sim(i,j)$ 值较低，即推荐相似度较低，则舍弃该域的推荐；若 $sim(i,j)$ 值较高，即推荐相似度较高，则以该值作为推荐因子。该推荐可信度的值控制在[0,1]范围内，以避免恶意安全域推荐过高的信任值。则其间接可信度的计算式为：

$$IDT=\frac{\sum_{k=1}^{N}DT_{ik}*sim(j,k)*w(\partial(t))}{N} \tag{6}$$

其中，N 表示主体 s_i 访问过所有安全域的总数，DT_{ik} 表示主体 s_i 和安全域 sd_k 的直接信任度，$sim(j,k)$ 表示安全域 sd_k 和安全域 sd_j 的共同访问者的评价相似度。

4.2 综合信任度的计算

根据直接信任度的计算，主体 s_i 要访问安全域 sd_j 中的资源，s_i 处于 sd_i 安全域。假设主体 s_i 要访问安全域 sd_j 中的资源，s_i 处于 sd_i 安全域。当主体 s_i 第一次访问客体资源时，直接信任度初始化为 0.3，根据贝叶斯理论，可得出直接信任度的计算式如式(7)所示：

$$DT_{ij}=\begin{cases}0.3, & n=1\\ \dfrac{S_{ij}+1}{N_{ij}+2}, & n>1\end{cases} \tag{7}$$

其中，S_{ij} 表示成功交互的次数，N_{ij} 表示主体 s_i 和安全域 sd_j 交互的总次数。

主体的综合可信度的计算不仅要考虑直接访问产生的信任度，还要考虑其他安全域的推荐可信度，这样可以保证用户在所有安全域的访问行为都会影响到其他安全域的信任度，从而对恶意主体的访问起到更大范围的监管作用。主体的综合信任度可以通过对直接信任度和综合信任求加权平均来计算。因此，综合信任度的计算如式(8)所示，可以调整 θ 的大小在直接信任和推荐信任之间进行取舍。一般情况下，直接信任的权重要比间接信任的权重大一些，但是若直接信任度过高(如 0.9)，则不再考虑间接信任度。

$$T=\begin{cases}DT, & DT>0.9\\ \theta*DT+(1-\theta)*IDT, & DT\leqslant 0.9\end{cases} \tag{8}$$

计算用户综合信任值的伪代码如算法 1 所示。

算法 1 用户综合信任值的计算

```
输入:(User_A,Object_R,Access_Record,S_D)
输出:Com_Tr
  //计算直接信任度
1. User_Recc←cell2mat(User_Rec(U_Amount,4));
2. num_true←sum(cell2mat(User_Rec(:,4)));
3. D_Tr←(num_true+1)/(U_Amount+2);
  //计算间接信任度
4. for User_Reci in Rec_Set:
5. R_8c←cell2mat(User_Reci(:,6));
6.   if U_Amount<win_num+1
7. W←1/(2*U_Amount):
     /U_Amount:1/(2*U_Amount)
8. sim1←sum(R_8c(1:U_Amount,1).*R_8(1:U_Amount,1));
9. sim2←sqrt(sum(R_8c (1:U_Amount,1)*R_8c(1:U_Amount,
   1)))*sqrt(sum(R_8(1:U_Amount,1).*R_8(1:U_Amount,
   1)))
10. sim←sim1/sim2;
11.   if sim<0.3
12.   Continue
13.     else
14.       Ind_Tr←Ind_Tr+sum(cell2mat(User_Rec(:,5)).*sim.*
```

```
        w′)/U_Amount * 2;
15.   end if
16.   else
17.   w←1/2 * (win_num+1):1/(win_num+1):1-1/2 * (win_
      num+1);
18. sim1←sum(R_8c((U_Amount-win_num):U_Amount,1). * R_8
    ((U_Amount-win_num):U_Amount,1));
19.   sim2←sqrt(sum(R_8c((U_Amount-win_num):U_Amount,
      1))) * sqrt(sum(R_8((U_Amount-win_num):U_Amount,1). *
      R_8((U_Amount-win_num):U_Amount,1)));
20. sim←sim1/sim2;
21.   if sim<0.3
22.     Continue;
23.   else
24.     Ind_Tr←Ind_Tr+sum(cell2mat(User_Rec(((U_Amount-
        win_num):U_Amount),5)) * sim. * w′)/win_num * 2;
25.   end if
26. end if
  //计算综合信任度
27. Ind_Tr←Ind_Tr/size(Rec_Set);
28. Com_Tr←k * D_Tr+(1-k) * Ind_Tr
29. end for
```

5 仿真实验及分析

本文在 Win10 系统环境下通过 Matlab 工具实现基于动态的用户信任度的属性访问控制。仿真环境为：Intel(R) Xeon(R) E5-1603 @2.8 GHz 2.8GHz CPU，4 GB 内存，8.6.0.267246 (R2015b)版本的 Matlab。本文将所有用户的初始可信度设置为 0.3，其中，直接可信度所占比重为 0.6。

5.1 时间因素对用户综合信任值的影响

图 3 给出了测试用户跨域访问 30 次，在不设置滑动窗口和时间窗口设置为 10 这两种情况下，用户的综合可信度的变化趋势。由图 3 可知，当访问次数为 10 时，win-num＝10 和 no window 曲线由原来的重合发生分离，此后 win-num＝10 的综合信任值比 no window 的综合信任值要高。这是因为当用户第一次访问资源时，所有用户都获得一个初始综合信任值 0.3，因此当用户进行可信访问时，根据本文提出的计算综合信任值的方法，其值会越来越大，用户的可信度也会越来越高；当滑动窗口被设置为 10，用户进行第 11 次访问时，本文方法会忽略初始综合信任值 0.3 对本次访问的综合信任值的影响，当发生第 12 次访问时忽略第一、二次访问结果对本次访问的影响，以此类推，直至窗口外的数据对当前访问不产生影响。

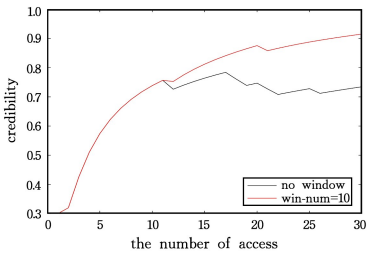


图 3 时间因素对可信度的影响

Fig. 3 Influence of time factor on credibility

图 4 给出了时间窗口 win-num 设置为 10 和未设置时间窗口对用户成功访问资源的影响。由图 4 可知，当用户进行相同的访问时，设置时间窗口能使用户获得比较大的成功访问率。通过对比图 3 和图 4 可知，设置时间窗口的用户的综合信任度要比不设置时间窗口的用户的综合信任度高，这表明该用户更加可信，因此其访问客体的请求更不容易被拒绝。

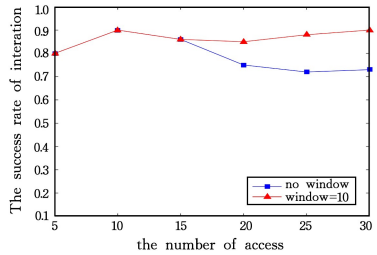


图 4 时间因素对访问成功率的影响

Fig. 4 Impact of time factor on visit success rate

5.2 余弦相似度评价的影响

图 5 给出了在滑动窗口、可信衰减、惩罚机制的基础上引入余弦相似度和未引入余弦相似度对用户综合信任值的影响。由图 5 可知，未引入余弦相似度和引入余弦相似度的用户综合信任度都会随着访问次数的增多而动态地发生变化。其中，未引入余弦相似度的信任值不考虑其他安全域对本次访问的推荐是否可信，只是对其推荐简单地求平均值，其综合信任值会大于或等于引入余弦相似度的综合信任值。未引入余弦相似度的综合信任度和引入余弦相似度的综合信任值由刚开始的重合逐渐分离，这是因为在前 3 次的访问中其他安全域的推荐完全相似，所以两者会出现短暂的重合，后来随着推荐信任的不同两者逐渐分离。由图 5 可知，引入余弦相似度的模型和未引入余弦相似度的模型相比，更能阻止恶意用户的访问。

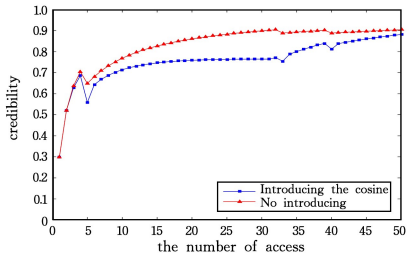


图 5 余弦相似度对可信度的影响

Fig. 5 Effect of cosine similarity on credibility

5.3 CT-ABAC 模型的交互成功率

为验证本文所提模型在阻止恶意用户访问和安全域的恶意推荐上更具有优势，我们选取 Wu 等提出的基于动态线性的访问控制模型[21](这里简称为 DLAC)和 Li 等提出的基于相似度的改进信任机制[22](这里简称为 BSAC)与本文所提模型进行对比。由图 6 可知，当恶意用户的比例分别为 10%，20%，30%，40%，50%，60%，70%时，本文提出的 CT-ABAC 模型、DLAC 模型、BSAC 模型的用户成功交互的比率都有不同程度的下降，其中，DLAC 模型下降的速度最快；当恶意用户的比例超过 60%时，DLAC 模型交互的成功交互率下降到 50%以下，而本文模型的成功交互率仍然维持在 85%以上。这是因为 DLAC 模型缺乏惩罚机制，所以当用户进行恶意访

问时，其不能有效降低信任值以阻止用户继续进行恶意访问。虽然 BSAC 模型和 CT-ABAC 模型都采取了余弦相似度推荐，但是 BSAC 是依据安全域之间的内容相似度，CT-ABAC 是依据历史访问信息的评价相似度，且忽略了相似度比较低的安全域的推荐。因此，相比 BSAC 和 DLAC 模型，本文提出的模型在计算用户信任度属性时能够识别出更多安全域的恶意推荐，即当用户发生恶意访问时，根据用户的信任级别进行惩罚来阻止恶意用户继续进行恶意访问。因此，可信用户的成功访问率也有所提高。

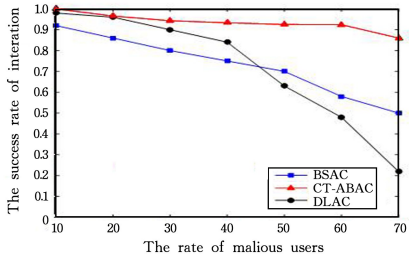


图 6 访问成功率随恶意用户占比的增多而发生的变化

Fig. 6 Changing in access success rate with increasing proportion of malicious user

为测试用户在不同的网络环境中的成功交互率，我们参照文献[23]提出的两个参数：服务请求频度(Service Request Frequency，SRF)和服务动态频度(Service Dynamic Frequency，SCF)。服务请求频度 ($0 \leqslant SRF \leqslant 1$)表示系统的繁忙程度，其值越接近 1 表示系统越繁忙。服务动态频度($0 \leqslant SCF \leqslant 1$)表示系统资源的不稳定性，其值越大表示资源越不稳定。我们通过调整 SCF 和 SRF 的值来测试用户在不同网络状况下的访问状况，如图 7 所示。由图 7 可知，在不同的系统繁忙程度和资源稳定程度下，用户的成功访问率都随着访问次数的增多而逐渐趋向于一个固定的值。其中，当系统比较繁忙、资源不稳定性高(如 $SCF=0.6$，$SRF=0.6$)时，用户的成功访问率仍然可以保持比较高的值(0.85 以上)，这说明该系统具有比较好的动态适应性。

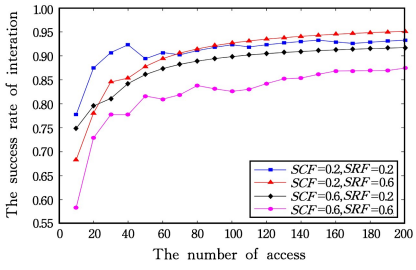


图 7 不同访问环境的成功交互率

Fig. 7 Successful access rate in different access environments

结束语 针对云计算多域环境出现的安全问题，本文提出了一种基于动态用户信任度的属性访问控制模型。该模型是在基于属性的访问控制的基础上融合可信的思想，通过使用户和安全域建立信任机制的方式来提高可信用户的成功访问率，降低恶意安全域的推荐。在 CT-ABAC 中，访问请求由主体属性、客体属性、权限属性、用户信任度属性组成，模型采用动态的授权机制，根据访问控制请求的属性组合做出决策，同时也考虑到时间因素、域间相似度、惩罚机制对用户信任度的影响。仿真实验结果表明，该模型能够有效地降低恶意用户的访问，并且提高可信用户访问的成功率。

云计算环境具有复杂的特点，本文提出的模型将用户的可信性作为进行访问控制的约束之一以提高安全性，但是用户进行跨域访问中仍存在着不同安全域之间的策略冲突的情况，因此后续工作将主要集中于如何有效地避免策略冲突。

参 考 文 献

[1] SIBAI R E, GEMAYEL N, ABDO J B, et al. A survey on access control mechanisms for cloud computing[J]. Transactions on Emerging Telecommunications Technologies, 2019, 31(2): 1-21.

[2] ZHANG P, SHI N F, JIANG H. A New Research of Delegation Agent Model Based On RBAC[C]// The 3rd International Conference on Wireless Communication and Sensor Networks. Paries: Atlantis Press, 2016: 15-18.

[3] RIVERA S Y K, DEMURJIAN S A, BAIHAN M S. A service-based RBAC & MAC approach incorporated into the FHIR standard[J]. Digital Communications and Networks, 2019, 5(4): 214-225.

[4] LACEY-BARNACLE M, ROBISON R, FOULDS C. Energy justice in the developing world: a review of theoretical frameworks, key research themes and policy implications[J]. Energy for Sustainable Devlelopment, 2020, 2020(55): 122-138.

[5] SERVOS D, OSBORN S L. Current Research and Open Problems in Attribute-Based Access Control[J]. ACM Computing Surveys, 2017, 2017(65): 1-45.

[6] JAMES B D. A generalized temporal role based access control model for developing secure systems [D]. Indiana: Purdue University, 2013.

[7] RANISE S, TRUONG A, VIGANÒ L. Automated Analysis of RBAC Policies withTemporal Constraints and Static Role Hierarchies[C]// The 30th Annual ACM Symposium. New York: ACM, 2015: 2177-2184.

[8] JIANG J G, YUAN X B, MAO R. Research on Role Mining Algorithms in RBAC[C]// The 2nd High Performance Computing and Cluster Technologies. New York: ACM, 2018: 1-5.

[9] BISWAS P, SANDHU R, KRISHNAN R. Label-Based Access Control: An ABAC Model with Enumerated Authorization Policy[C]// ACM International Workshop on Attribute Based Access Control, New York: ACM, 2016: 1-12.

[10] BHATT S, PATWA F, SANDHU R. ABAC with group attributes and attribute hierarchies utilizing the policy machine[C]// The 2nd ACM Workshop on Attribute-Based Access Control. New Yorck: ACM, 2017: 17-28.

[11] MUHAMMAD U A, QIN G Z. Role-Based ABAC Model for Implementing Least Privileges[C]// The 8th International Conference on Software and Computer Applications. New York: ACM, 2019: 467-471.

[12] DAS S, SURAL S, VAIDYA J, et al. Policy Adaptation in Hierarchical Attribute-Based Access Control Systems[J]. ACM transactions on Internet technology. 2019, 19(40): 1-24.

[13] XIE R N, LI H, SHI G Z. Lightweight and reconfigurable access control strategy based on attributes[J]. Journal of Communications, 2020, 41(2): 112-122.

[14] HUANG L Y,XIONG G W. A Trust-role Access Control Model Facing Cloud Computing[C]// The 35th Chinese Control Conference. New York:IEEE,2016:5239-5242.

[15] LI X. Access Control Strategy Based on Trust under Cloud Computing Platform[C]// International Conference on Virtual Reality and Intelligent Systems. New York: IEEE, 2018: 327-330.

[16] UIKEY C,BHILARE D S. TrustRBAC:Trust role based access control model in multi-domain cloud environments[C]// IEEE, International Conference on Information, Communication, Instrumentation and Control. New York:IEEE,2017:1-7.

[17] GHAFOORIAN M,ABBASINEZHAD-MOOD D,SHAKERI H. A Thorough Trust and Reputation Based RBACModel for Secure Data Storage in the Cloud[C]// IEEETransactions on Parallel and Distributed Systems. New York:IEEE,2018:1-12.

[18] ZHAO Z Y,SUN L. Attribute-based Access Control with Dynamic Trust in a Hybrid Cloud Computing Environment[C]// International Conference on Cryptography,Security and Privacy. New York:ACM,2017:112-118.

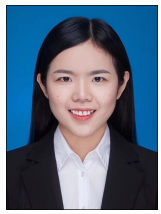
[19] HU V C,FERRAIOLO D,KUHN R,et al. Guide to Attribute Based Access Control(ABAC) Definition and Considerations: 800-162 [S]. U. S. Department of Commerce:National Institute of Standards and Technology,2014.

[20] DANIEL S,OSBORN S. Current Research and Open Problems in Attribute-Based Access Control[J]. ACM Computing Surveys,2017(65):1-45.

[21] WU C Q,HUANG R N. Research on Access Control Model Based on Dynamic Linear Correlation[J]. Computer Science, 2015,42(9):94-106.

[22] LI D Q,GUO R M. An Improved Trust Mechanism Based on the Similarity[C]// National Conference on Electrical. Paries: Atlantis Press,2015:722-728.

[23] LI X Y,GUI X L. Cognitive Model of Dynamic Trust Forecasting[J]. Journal of Software,2010,21(1):163-176.



PAN Rui-jie, born in 1993, postgraduate. Her main research interests include network security and so on.

WANG Gao-cai, born in 1976, Ph. D, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include computer network, system performance evaluation and random method.