DOI:10.16515/j.cnki.32-1722/n.2019.04.004

信任度和属性混合授权的访问控制模型研究

王洪欣,苗丽娟,徐尚瑜,严 冬

(金陵科技学院南京软件研究院,江苏 南京 211169)

摘 要:传统访问控制中角色设置单一,使得系统适应性差、细粒度访问控制不足等。针对此问提出了一种基于信任度与属性的权限访问控制模型。模型改进了传统的用户-角色-权限分配策略,引入信任约束条件来控制用户-角色分配,针对用户的恶意攻击和访问进行控制和过滤;引入属性对角色的有效权限分配实行进一步的约束。实例分析表明,基于信任度和属性的RBAC混合扩展访问控制模型不仅保留了RBAC授权访问的优势,还支持灵活、动态、细粒度的访问控制,可有效减少管理复杂度,为访问控制提供了一种新的解决方案。

关键词:信任度;属性;权限分配;动态授权;授权规则

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1672-755X(2019)04-0015-05

Hybrid Authorized Access Control Model Based on Trust Degree and Attribute

WANG Hong-xin, MIAO Li-juan, XU Shang-yu, YAN Dong

(Jinling Institute of Technology, Nanjing 211169, China)

Abstract: Aiming at the problems of poor adaptability and insufficient fine-grained access control caused by single role setting in traditional role-based access control, an improved Role-Based Access Control (RBAC) model based on trust-degree and attribute is proposed. The model improves the traditional user-role-permission allocation strategy, trust constraints are applied to user-role assignment to control and the attacks and accesses of malicious users are filtered. Further constraints are imposed on the effective permission allocation of roles by introducing attributes. The analysis implies that the hybrid extended access control model based on trust and attributes for RBAC retains the advantages of RBAC authorized access, and supports flexible, dynamic and fine-grained access control, which can effectively reduce the complexity of management and provide a new solution for access control.

Key words: trust-degree; attribute; permission assignment; dynamic authorization; authorization strategy

作为一种基于互联网的新兴网络计算模式,云计算受到越来越多企业和个人的青睐。而信息安全作为云计算发展中面临的关键性问题,已逐渐成为云计算安全的重要研究内容[1]。传统的安全访问控制是通过基于角色的访问控制(RBAC,Role-Based Access Control)模型及其扩展模型实现的[2-3],这类模型大多是静态的、粗粒度的,未考虑与安全相关的用户特性、资源、操作和上下文等属性信息,当系统规模发生变动或者业务逻辑发生变化时,需要设置大量角色来维护用户-角色关系和角色-权限关系,极易引起角色爆炸问题[4]。

收稿日期:2019-11-18

基金项目:江苏省农业科技自主创新资金项目(CX17-2015);南京市科技计划项目(201505055)

作者简介:王洪欣(1990—),女,山东临沂人,讲师,硕士,主要从事信息安全技术、计算机工程应用等研究。

国内外众多学者针对权限访问控制的问题开展了一系列研究，主要是对传统的基于角色的访问控制模型进行改进和扩展[5-6]。考虑到基于角色的访问控制存在的局限性，近年来，基于属性的访问控制(ABAC，Attribute-Based Access Control)成为国内外复杂计算系统安全领域研究的热点[7-9]。Coyne等[10]将基于属性的访问控制与基于角色的访问控制进行了对比分析，总结出了RBAC的成熟性和在管理、安全方面的优势，ABAC在环境适应性上的优势。综合考虑两者的优势，一些学者将RBAC与ABAC进行整合，既保证了安全性，又可以很好地支持权限访问控制[11-12]。

自Marsh将信任管理的概念引入到计算机领域后，信任模型被逐渐应用于访问控制系统中以解决网络安全问题[13]。邹佳顺等[14]将信任相似度的概念应用于RBAC模型，通过计算用户信任特征向量与标准特征向量之间的相似度来估算用户的可信程度。针对开放式网络下基于信任访问控制问题中的授权需求，提出了基于知识发现的风险最小化授权模型[15]。

针对细粒度授权和动态授权的问题，本文结合RBAC和ABAC的优势，同时引入授权信任约束条件和属性配置，构造一种基于用户信任度和属性的角色访问控制模型，实现了更加动态灵活的授权机制，增强了权限分配的安全合理性和灵活性。

1 混合扩展访问控制模型

为了实现访问控制的动态授权和细粒度授权，本模型引入了信任度约束和属性规则等模型元素，通过信任度与属性相结合的混合授权管理思想，提出了基于信任度和属性的混合授权访问控制模型，模型的整体架构如图1所示。

该模型取消用户-角色的直接分配方式，将信任约束引入用户和角色分配中，通过用户属性和环境属性计算用户的信任度，然后通过动态激活信任度约束条件来实现用户-信任度-角色的动态分配。通过操作属性和资源属性对角色-权限分配过程进行约束和限制，增加角色权限分配的细粒度和动态性，使模型更加灵活。通过建立用户角色分配规则和角色权限分配规则，使模型可以更好地实现动态授权管理。

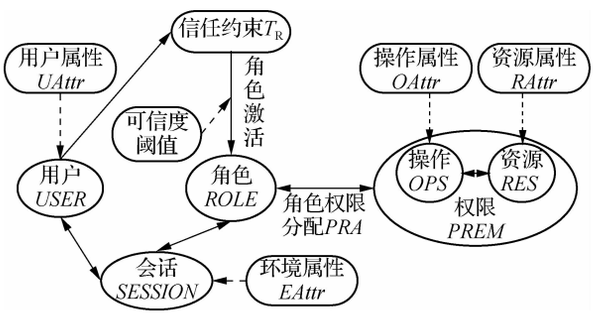

图1 混合授权访问控制模型

1.1 模型概念

模型中的元素、关系及函数定义如下：1)*USER*、*ROLE*、*OPS*、*RES*、*PREM*、*SESSION*与传统RBAC模型中元素的定义相同，分别表示用户、角色、操作、资源、权限和会话的集合。权限是由操作和资源共同构成的二元组，即$PREM=(OPS,RES)$。2)信任度T_R：模型中用户和角色没有直接指派关系，而是以信任度为中间约束条件，通过信任度计算模型对访问请求计算信任度值。信任度值为0～1。0表示完全不信任，1表示完全信任。3)信任度阈值T_{RD}表示激活角色时事先设定好的信任度的最小值，只有当信任度超过信任度阈值时，才能激活角色状态。4)属性值*Attr*表示某一对象所具有的特征信息及其描述。包括用户属性、环境属性、资源属性和操作属性。5)角色权限分配*PRA*(*Role-Permission Assignment*)：$PRA\subseteq P\times R$，权限P和角色R是多对多的指派关系。6)用户会话映射为$S\rightarrow U$，表示会话到用户的映射函数；角色会话映射为$S\rightarrow R$，表示会话到角色的映射函数，由用户创建会话，并选择是否激活用户角色。

1.2 属性认证

1)属性。模型在RBAC模型的基础上，引入用户属性*UAttr*、环境属性*EAttr*、操作属性*OAttr*、资源属性*RAttr*。*UAttr*是对操作系统用户的特征描述，包括用户名称、用户*ID*、用户基本信息等；*EAttr*表示执行操作时的会话环境的状态，包括时间、地点、网络环境等；*OAttr*表示用户能进行的操作，例如数据库的增删改查等；*RAttr*表示用户操作对象的特征描述，包括资源类型、资源提供者、存储状态等。

2)属性集合。每个属性均表示为属性的集合，表示为$Attr=\{attr_1,attr_2,\cdots,attr_i\}$，$attr_i$表示一个属

性变量，$attr_i \in Attr$。

3）属性表达式。多个属性之间通过属性表达式可以实现对属性的描述和约束。多个属性表达式之间通过逻辑运算得到复合属性表达式。

4）逻辑运算。非（～）运算，表示没有该属性，或不满足该属性表达式。并（∨）运算，类比编程语言中“‖”的含义，表示两个属性的并集，即满足属性 a 或属性 b，或表示满足两个属性表达式中的一个或所有，也就是两个属性表达式的并集。交（∧）运算，类比编程语言中“&&”的含义，表示两个属性的交集，需要同时满足属性 a 和属性 b，或表示同时满足两个属性表达式。

5）属性约束。用户要激活角色获取访问权限时，需要满足属性约束条件。

1.3　信任度计算

1.3.1　*直接信任度*　在用户访问系统资源时，需要向系统提供用户信息和环境信息，这些因素会影响用户访问资源的信任度。将用户访问系统资源的评估属性分解为基本属性和环境属性两部分，每个评估属性都分解为更细致的评估因子，对这些评估因子与系统安全的相关度进行处理为 Sr_i，并为它们分配权重 w_i，调整评估属性的权重可以设置用户属性和环境属性的重要程度，针对不同平台和不同使用场景实现灵活调整。

计算当前的直接信任度为：

$$T_{DCurrent}(u) = \alpha \sum_{i=1}^{n} Sr_i w_i + \beta \sum_{j=1}^{m} Sr_j w_j \tag{1}$$

其中 $\sum_{i=1}^{n} Sr_i w_i$ 表示用户属性信任度，$\sum_{j=1}^{m} Sr_j w_j$ 表示环境属性信任度，α、β 分别表示基本属性和环境属性信任度的影响权重。$\alpha + \beta = 1$，$0 \leqslant \alpha, \beta \leqslant 1$，用户属性含 m 个评估因子，环境属性含 n 个评估因子。

当访问控制请求者与资源进行多次交互时，需要考虑历史直接信任度的影响。考虑实体之间的信任度受上下文环境和时间衰减的影响，当前直接信任度与上一次的直接信任度之间的关系如下：

$$T_{Dt}(u) = (1-\gamma) T_{DCurrent}(u) + \gamma T_{D(t-1)}(u) \tag{2}$$

其中，γ 是上一次直接信任度的影响率，$\gamma \in [0,1]$，γ 越大表示历史信任度在计算信任度时占的比重越大。$T_{D(t-1)}(u)$ 是上一次的直接信任度。当用户首次获取权限时，用户的信任度为 $T_{Dt}(u) = T_{DCurrent}(u)$。

1.3.2　*间接信任度*　完全依赖直接信任度控制资源的访问并不全面，可能会面临恶意访问的问题，因此增加第三方信任度，来监控用户的行为，即基于他人对用户的评价信息进行信任度评估。

利用信任度的传递性来计算没有交互过的两个实体之间的信任度。资源所有者需要评定对资源请求者的间接信任度，通过征询其他与资源请求者有过交互的推荐者的建议，对资源请求者进行信任评价。资源所有者对各个推荐者的反馈信任度进行加权合成后，得到资源请求者的间接信任度。那么资源所有者对资源请求者的信任度可以通过 $T_{Dt}(p,x)$ 和 $T_{Dt}(x,q)$ 的乘积来获得。

间接信任度计算公式如下：

$$T_{It}(u) = T_{It}(p,q) = \frac{\sum_{m \in I(k)} T_{Dt}(p,x) \times T_{Dt}(x,q)}{\sum_{m \in I(k)} T_{Dt}(p,x)} \tag{3}$$

其中，$I(k)$ 为资源所有者的总数，$T_{Dt}(p,x)$ 表示资源所有者 p 对推荐者 x 的直接信任度，$T_{Dt}(x,q)$ 表示推荐者 x 对资源请求者 q 的直接信任度。为了防止推荐过程中的夸大或诋毁行为，采用 $T_{Dt}(p,x)$ 作为推荐信任系数。

1.3.3　*总体信任度*　总体信任度表示为，在特定环境下系统对用户及其所在平台信息进行认证评估后的数量度值。使用直接信任值和间接信任值之间的线性组合计算总体信任度，公式如下：

$$T_{Rt}(u) = \omega T_{Dt}(u) + (1-\omega) T_{It}(u) \tag{4}$$

其中 ω 是直接信任度的影响率，$\omega \in [0,1]$，ω 越大表示直接信任度对总体信任度的影响越大。

总体信任度具有动态性，会随着用户每次访问权限的变化而变化，当前总体信任度与上一次的总体信

任度之间的关系如下：

$$T_{Rt}(u)=(1-\theta)T_{Rt}(u)+\theta T_{R(t-1)}(u) \tag{5}$$

其中，θ 是上一次总体信任度的影响率，$\theta\in[0,1]$；$T_{R(t-1)}(u)$ 是上一次访问时的总体信任度。

2 模型授权规则

1)用户-角色激活规则。用户访问资源时，需要激活用户角色，当用户的信任度大于激活角色的信任度阈值时，即 $T_R(u)>T_{RD}(u)$，角色激活成功。如果用户具有属性，且满足属性约束条件和信任约束条件，则用户角色 r 被激活。表示为：

$$(attr_i(u)\neq\varnothing)\wedge(Cons(attr_i(u)))\wedge(Cons(T_R(u)>T_{RD}(u)))\Rightarrow user\_active(u,r) \tag{6}$$

2)角色-资源/操作权限激活规则。资源或者操作具有属性且满足属性约束条件，则将权限 p 分配给角色 r。

$$[(attr_i(res)\neq\varnothing)\wedge Cons(attr_i(res))]\vee[(attr_i(ops)\neq\varnothing)\wedge Cons(attr_i(ops))]\Rightarrow premission\_active(p,r) \tag{7}$$

3 实例分析

以某云存储平台为例说明该模型的合理性和有效性。

1)根据用户的 VIP 级别控制其享受不同类型的资源的访问，如表 1 所示。

表 1 点数资源分级

点数	角色	信任度阈值	资源类型
$count\geqslant 50\ 000$	$diamond\_member$	0.5	$video,music,picture,file,rar,other$
$10\ 000\leqslant count<50\ 000$	$gold\_member$	0.6	$picture,file,rar,other$
$5\ 000\leqslant count<10\ 000$	$silver\_member$	0.7	$file,rar,other$
$count<5\ 000$	$copper\_member$	0.8	$rar,other$

2)根据用户的上传文件量控制其享受对各类资源的操作，如表 2 所示。

表 2 点数操作分级

点数	角色	操作类型
$quantity<5$	$junior\_member$	$upload,modify,get$
$5<quantity\leqslant 20$	mid_member	$upload,modify,get,collect$
$quantity>20$	$senior\_member$	$upload,modify,get,collect,download$

基于以上策略，定义用户-信任度-角色规则和角色-权限分配规则为：

规则 1：$(count(u)>5\ 000)\wedge(Cons(T_R(u)\geqslant 0.5))\Rightarrow user\_active(u,diamond\_member)$

规则 2：$(10\ 000\leqslant count(u)<50\ 000)\wedge(Cons(T_R(u)\geqslant 0.6))\Rightarrow user\_active(u,gold\_member)$

规则 3：$(5\ 000\leqslant count(u)<10\ 000)\wedge(Cons(T_R(u)\geqslant 0.7))\Rightarrow user\_active(u,silver\_member)$

规则 4：$(count(u)<5\ 000)\wedge(Cons(T_R(u)\geqslant 0.8))\Rightarrow user\_active(u,copper\_member)$

规则 5：$(quality(u)<5)\Rightarrow user\_active(u,junior\_member)$

规则 6：$(5\leqslant quality(u)<20)\Rightarrow user\_active(u,mid\_member)$

规则 7：$(quality(u)>20)\Rightarrow user\_active(u,senior\_member)$

角色-资源/操作权限分配规则为：

规则 1：$Cons(category(res[movie\vee music\vee picture\vee file\vee rar\vee other]))\Rightarrow premission\_active(p,diamond\_member)$

规则 2：$Cons(category(res[picture\vee file\vee rar\vee other]))\Rightarrow premission\_active(p,gold\_member)$

规则 3：$Cons(category(res[file\vee rar\vee other]))\Rightarrow premission\_active(p,silver\_member)$

规则 4：$Cons(category(res[file\vee rar]))\Rightarrow premission\_active(p,copper\_member)$

规则 5：$Cons(option(ops[upload \vee modify \vee get \vee collect \vee download])) \Rightarrow premission\_active(p, senior\_member)$

规则 6：$Cons(option(ops[upload \vee modify \vee get \vee collect])) \Rightarrow premission\_active(p, mid\_member)$

规则 7：$Cons(option(ops[upload \vee modify \vee get])) \Rightarrow premission\_active(p, junior\_member)$

当用户访问系统时，根据用户的属性获取到用户的信任度，根据用户-属性-信任度约束规则获取用户的角色，然后根据角色-资源/操作权限分配规则获取对系统的访问权限。例如，*count* 为 12 000 点的用户的首次访问、默认信任度为 0.82、初始文件上传量为 0 时，获得用户角色为 *gold_member*、*junior_member*，获取到用户可访问的资源为 $res[picture \vee file \vee rar \vee other]$，可进行的操作为 $ops[upload \vee modify \vee get]$，因此该用户可以针对图片、文档、压缩文件、其他文档进行上传、修改、获取操作。

4　结　语

本文针对传统的 RBAC 不支持动态约束与细粒度约束的问题，给出了一种基于信任度和属性的混合授权访问控制模型，将信任管理、属性约束与 RBAC 相结合，充分发挥了各个部分的优势。以 RBAC 模型为基础，通过引入信任管理的概念，将信任约束条件应用于用户-角色分配中，实现用户-信任度-角色的动态分配；通过引入属性对角色的有效权限分配实行进一步的约束，并且制定了用户-角色和角色-权限的模型授权规则，实现了模型授权的动态性。通过应用实例对模型进行了验证，结果表明模型可以很好地支持动态授权和细粒度授权。

参考文献：

[1] Choi C，Choi J，Kim P. Ontology-based access control model for security policy reasoning in cloud computing[J]. The Journal of Supercomputing，2014，67(3)：711－722

[2] 熊光辉，白尚旺，党伟超. 一种基于角色等级树的 SaaS 多租户多域访问控制模型[J]. 计算机应用与软件，2018，35(6)：319－324

[3] Cheng Y，Wang F，Shang L，et al. Improved access control strategy based on RBAC model and its application[C]//ICCSAE. 2015 5th international conference on computer sciences and automation engineering. Atlantis：Atlantis Press，2016

[4] Fadhel A B，Bianculli D，Briand L. A comprehensive modeling framework for role-based access control policies[J]. Journal of Systems and Software，2015，107：110－126

[5] 蔡婷，聂清彬，欧阳凯，等. 基于角色扩展的 RBAC 模型[J]. 计算机应用研究，2016，33(3)：882－885

[6] 刘庆云，沙泓州，李世明，等. 一种基于量化用户和服务的大规模网络访问控制方法[J]. 计算机学报，2014，37(5)：1195－1204

[7] 周超，任志宇. 结合属性与角色的访问控制模型综述[J]. 小型微型计算机系统，2018，39(4)：782－786

[8] Fatima A，Ghazi Y，Shibli M A，et al. Towards attribute-centric access control：an ABAC versus RBAC argument[J]. Security and Communication Networks，2016，9(16)：3152－3166

[9] Khaled R. Behavior based access control for securing cloud infrastructure as a service[D]. Beijing：University of Science and Technology，2017

[10] Coyne E J，Weil T R. ABAC and RBAC：scalable，flexible，and auditable access management[J]. IT Professional，2013，15(3)：14－16

[11] Zhu Y，Huang D，Hu C J，et al. From RBAC to ABAC：constructing flexible data access control for cloud storage services[J]. IEEE Transactions on Services Computing，2015，8(4)：601－616

[12] Niu S Z，Tu S S，Huang Y F. An effective and secure access control system scheme in cloud[J]. Chinese Journal of Electronics，2015，24(3)：524－528

[13] Feng Y，Ying W. A reputation-based dynamic trust model for large scale distributed environment[J]. Journal of Computational Information Systems，2013，9(3)：1209－1215

[14] 邹佳顺，张永胜，高艳. 基于信任相似度的 RBAC 机制[J]. 计算机工程与设计，2015，36(8)：2069－2073

[15] 张佳乐，张桂玲，张秀芳. 基于实时行为可信度量的网络访问控制模型[J]. 计算机应用与软件，2017，34(7)：32－38

（责任编辑：湛　江）