Computer Science and Application 计算机科学与应用, 2019, 9(3), 517-526
Published Online March 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.93059

Hans汉斯

A Role and Attribute-Based Access Control Model with Trust Management

Yan Huang, Xiaoling Wu*, Jie Ling

School of Computer, Guangdong University of Technology, Guangzhou Guangdong
Email: *xl.wu@giat.ac.cn, 1370438664@qq.com

Received: Feb. 15th, 2019; accepted: Feb. 26th, 2019; published: Mar. 5th, 2019

Abstract

With the illegal access from illegal users to data which is stored in the cloud, cloud services suffer from a variety of security risks. Reasonable authorization through access control is one of the most urgent problems to be solved in current cloud security. To solve this problem, a Role and Attribute-Based Access Control model with Trust Management (TRABAC) is proposed. Firstly, the trusted users are screened out by calculating the trust value of the users. Secondly, the Role-Based Access Control (RBAC) model and the Attribute-Based Access Control (ABAC) model are combined to complete the user-role assignment and role-permission assignment. And the user-role mapping relationship and the role-permission mapping relationship are dynamically reduced according to the corresponding attribute filtering policy. Finally the minimum set of permissions that the user can have can be achieved. The security analysis results show that this model can achieve more dynamic security and fine-grained access control in the cloud computing environment.

Keywords

Access Control, Cloud Security, Trust Management, Role, Attribute

一种支持信任管理的基于角色和属性的访问控制模型

黄　艳，吴晓　*，凌　捷

广东工业大学计算机学院，广东　广州
Email: *xl.wu@giat.ac.cn, 1370438664@qq.com

收稿日期：2019年2月15日；录用日期：2019年2月26日；发布日期：2019年3月5日

*通讯作者。

文章引用: 黄艳, 吴晓鸽, 凌捷. 一种支持信任管理的基于角色和属性的访问控制模型[J]. 计算机科学与应用, 2019, 9(3): 517-526. DOI: 10.12677/csa.2019.93059

摘　要

由于存在非法用户对云中存储的数据的非法访问，云服务遭受各种各样的安全风险。通过访问控制进行合理授权是当前云安全问题中亟待解决的问题之一。针对此问题，本文提出了一种支持信任管理的基于角色和属性的访问控制模型(TRABAC)。首先，通过计算用户的信任值对其进行信任评估筛选出可信用户。其次，结合基于角色的访问控制模型(Role-Based Access Control, RBAC)与基于属性的访问控制模型(Attribute-Based Access Control, ABAC)来完成用户－角色分配和角色－权限分配，并根据相应的属性过滤策略动态地缩减用户－角色映射关系和角色－映射权限映射关系。最后，得到用户可以拥有的最小权限集合。安全性分析结果表明，该模型在云计算环境下能更好地实现动态安全和细粒度的访问控制。

关键词

访问控制，云安全，信任管理，角色，属性

1. 引言

云计算作为一种新型的计算模式，如何对开放性、共享性和弹性的云环境进行安全有效的管理是当前云计算信息安全领域的一个研究热点[1]。访问控制技术成为云计算中保护云服务访问和数据安全的有效措施。通过制定有效的访问控制策略能使合法用户获得相应的访问权限以防止非法获取、篡改和破坏数据。

访问控制技术是信息安全的核心技术之一。通过对关键资源实行访问限制，防止非法用户进入系统及合法用户对系统资源的非法使用，从而保护信息系统中存储和处理信息的安全[2]。访问控制技术由访问主体、访问客体与控制策略三个基本要素组成，传统的访问控制模型主要包括自主访问控制(Discretionary Access Control, DAC) [3]、强制访问控制(Mandatory Access Control, MAC) [4]和基于角色访问控制(Role-Based Access Control, RBAC) [5]，但这些模型都是基于预定义的规则进行授权，属于静态的访问控制。

传统的 RBAC 模型首先通过用户与角色之间的用户分配来实现关联，再通过角色与权限之间的权限分配实现相关性。最后，用户与角色之间、角色与权限之间的关联可以实现用户与权限之间的关联。但 RBAC 模型并不适合需要动态控制用户权限映射或实现动态粒度控制的环境，容易在授权过程中遇到一些安全隐患，从而威胁到云数据的分配和使用。

针对 RBAC 不支持细粒度授权和动态授权的问题，基于属性的访问控制(Attribute-Based Access Control, ABAC)将用户、资源和环境等参与者的属性作为授权与访问判定的依据，成为新一代的访问控制技术[6]。而随着网络规模与开放程度的不断加大，ABAC 模型在实际应用中存在着中心节点负担过大，决策过程中安全风险较高等问题[7]。因此需要设计安全的访问控制模型，并使其更好地适用于动态、复杂的云环境以保证云数据的完整性与安全性。

2. 相关工作

国内外已有大量的学者对云计算中的访问控制技术进行相关研究，提出了一系列用于云计算的访问控制模型。文献[8]提出了一种基于规则自动进行用户－角色分配的访问控制模型，但只考虑到了用户属

性，没有考虑到客体属性和环境属性，缺乏一定的灵活性；其次，这种方法有可能产生大量的角色，造成角色爆炸问题；更重要的是，角色根据优先级来构建，容易违背最小权限原则。

文献[9]提出了一种结合属性和角色的访问控制模型(ARBAC)，通过自动产生角色集合和权限集合，完成权限到角色、用户到角色的映射，从而降低授权管理的工作量。文献[10]提出了结合 RBAC 和 ABAC 的复合访问控制模型，该模型既有高效的管理机制又有细粒度的访问控制，但其用户角色分配速度和效率较低。文献[11]以客体权限角色以及用户的属性为基础，通过引入客体容器与行为等级将属性类型相同的客体进行分类并对该类客体可执行的操作划分等级，实现了权限的自动化构建，并将客体的属性转嫁到自动生成的权限中，然后使用属性表达式将权限自动分配给角色，角色就拥有了客体的属性，根据角色和用户的属性使用属性表达式就能将角色自动分配给用户，从而实现了 RBAC 模型的自动化构建。文献[12]提出了基于属性和 RBAC 的混合扩展访问控制模型(HARBAC)，通过基于属性的权限过滤策略对会话角色的有效权限进行进一步控制。文献[13]提出了一种基于角色和属性的云数据访问控制模型，为相关实体引入属性元素，用户能够通过自身和所在租户的属性集当前的状态分配角色，从而访问不同属性的数据。文献[14]提出了一种用户友好型且易于安全管理的 ABAC 机制。通过比较 RBAC 与 ABAC 之间的异同，将角色映射为多个属性的集合、角色间的层次关系映射为属性表达式间的偏序关系、用户－角色的分配映射为规则，从而实现了从 RBAC 到 ABAC 的迁移。

针对云计算环境中的访问控制模型，也有学者结合信任进行相关研究。文献[15]将信任评价模型与静态 RBAC 模型结合提出基于信任和角色的访问控制模型，该模型根据用户的身份证书和历史访问行为等信息为用户赋予一个信任级别，并由预先设定的信任级别－角色集列表和角色－权限集列表决定用户当前可被赋予的访问角色和权限。但用户的信任级别仅在每次获取角色时才重新评估，因此信任度量的动态性不强，访问控制粒度较粗。文献[16]对文献[15]提出改进，用户的信任度可在资源访问的整个过程中进行实时评估，同时引入角色基本权限集的思想，提高了授权的安全性和细粒度性。

文献[17]针对当前云计算访问控制中角色不能随时间动态改变的问题，提出了一种基于用户信任值确定其信任等级的方法，激活其所对应的角色及赋予该角色一定的访问权限，从而达到访问控制的目的。文献[18]将基于角色和信任的访问控制模型相结合，提出一种基于信任－角色的混合云计算访问控制模型。该模型在基于角色的访问控制基础上引入信任度的计算，即用户需进行信任值的验证，才能获得访问数据的权限。文献[19]提出基于信誉值的结构化数据访问控制模型。从系统中的所有主体入手，通过对主体进行信誉值的不断评估，得到一个较为符合的信誉体系，使系统可以通过信誉值的等级来控制访问系统不同程度的隐私数据。

现有的访问控制模型通常是将 RBAC 模型与 ABAC 模型结合或者将信任与 RBAC 模型结合起来，虽为解决云安全问题提供了一些策略，但仍存在一些不足之处。本文在文献[10]的基础上进行改进，提出了一种支持信任管理的基于角色和属性的访问控制模型(TRABAC)，将信任、RBAC 模型与 ABAC 模型三者结合起来，充分发挥各自的优势。通过对用户的信任评估筛选出可信用户并接受其请求资源访问，然后根据 RBAC 模型的最大隶属原则给可信用户分配角色以及角色分配权限并通过 ABAC 模型动态缩减用户－角色映射关系和角色－权限映射关系得到用户的最小权限集合。

3. TRABAC 模型

3.1. 相关知识

定义 1 RBAC 模型可用一个元组表示(U,R,P,UR,RP,RH)，提供了用户、角色、权限以及对象或资源之间的关系。

1) U、R、P 分别代表用户集 Users、角色集 Roles、权限集 Permissions。

2) 用户角色映射关系 UR：形式化描述为 $U \to R$，表示用户 U 被赋予角色 R，描述了用户与角色间多对多的映射关系。即 $UR \subseteq Users \times Roles$。

3) 角色权限映射关系 RP：形式化描述为 $R \to P$，表示角色 R 被赋予权限 P，描述了角色与权限间多对多的映射关系。即 $RP \subseteq Roles \times Permissions$。

定义 2 用户角色过滤策略 $policy1 = \{U', R, U_{ATT}, R_{ATT}, Env\}$ 可抽象表示为一个布尔表达式：$Users' \times Roles \times 2^{U_{ATT}} \times 2^{R_{ATT}} \times 2^{Env} \to \{T, F\}$。其中 $User'$ 表示筛选后的可信用户，U_{ATT} 表示用户属性，R_{ATT} 表示角色属性，Env 表示环境属性值。

定义 3 角色权限过滤策略 $policy2 = \{U', R', P, R_{ATT}', O_{ATT}, Env\}$ 可抽象表示为一个布尔表达式：$Users' \times Roles' \times Permissions \times 2^{RATT'} \times 2^{OATT} \times 2^{ENV} \to \{T, F\}$。其中 $Roles'$ 表示过滤后的角色集，R_{ATT}' 表示角色属性，O_{ATT} 表示对象属性，Env 表示环境属性值。

定义 4 Jaccard 相似系数(Jaccard similarity coefficient) [20]用于比较有限样本集之间的相似性与差异性。给定两个集合 A，B，若两者 Jaccard 系数值越大，则相似度越高。可由下式来计算：

$$J(A,B) = \frac{|A \cap B|}{|A \cup B|} \tag{1}$$

3.2. 基本思想

TRABAC 模型的基本思想主要包括信任管理和 RBAC 与 ABAC 的结合，即利用 RBAC 模型静态管理用户与权限之间的关系、ABAC 模型动态管理用户与权限之间的关系。如图 1 所示。

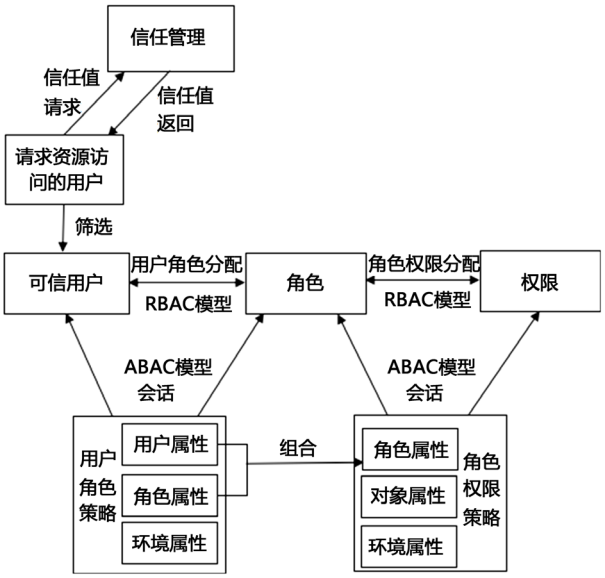

Figure 1. TRABAC model
图 1. TRABAC 模型

1) 信任管理

信任管理模块主要通过信任值的计算对用户进行信任评估来判断用户的可信度。用户的综合信任值是基于用户属性、用户行为反馈和用户信誉计算的，然后根据综合信任值与设置的阈值之间的关系来判断用户是否可信，决定是否接受其用户请求资源访问并为其分配角色。

用户属性主要包括用户的访问 IP 地址、访问时间、访问时长、访问状态。通过量化用户的属性因子并分配相应的权重计算用户属性信任值。计算公式如下：

$$T_{Atrust}=\varpi_1 T_{IP}+\varpi_2 T_{time}+\varpi_3 T_{length}+\varpi_4 T_{state} \tag{2}$$

$$T_{length}=\frac{t_{access}}{t_{total}} \tag{3}$$

$$T_{state}=\frac{a}{a+b} \tag{4}$$

其中 T_{Atrust} 指基于用户属性的信任值。T_{IP} 指用户的 IP 地址，不同的网段信任值不同。若用户的 IP 地址在安全网段内，则 T_{IP} 的取值为 $0.5 \le T_{IP} < 1$。若不在安全网段内，则 T_{IP} 的取值为 $0 \le T_{IP} < 0.5$。T_{time} 指用户请求资源服务的访问时间段，不同的访问时间段信任值不同。若用户访问时间在资源服务时间内，则 T_{time} 的取值为 $0.5 \le T_{tine} < 1$。若不在资源服务时间内，则 T_{time} 的取值为 $0 \le T_{tine} < 0.5$。T_{length} 为访问时长，t_{access} 为用户请求资源服务的时间，t_{total} 为总访问时间。T_{state} 为访问状态，a 为用户请求资源服务成功状态的次数，b 为用户请求资源服务失败状态的次数。$\varpi_i\ (i=1,2,3,4)$ 为每个属性因子的权重，且 $\sum_{i=1}^{4}\varpi_i=1$。

用户行为反馈是指用户之前请求访问过该资源，并根据用户请求资源访问的交互历史次数计算用户的行为反馈信任值。计算公式如下：

$$T_{Btrust}=\frac{\alpha+1}{\alpha+\beta+2} \tag{5}$$

其中 T_{Btrust} 指基于用户行为反馈的信任值。α 是指在用户请求访问资源总次数中良性访问的次数，β 指用户请求访问资源总次数中恶性访问的次数。

用户信誉是指其他用户对该目标用户请求资源访问时的一个信任值评价，通过 *Jaccard* 相似系数法计算用户间共同请求访问资源的个数占总请求服务个数的比重，得到用户请求资源访问的相似度表示其他用户对该目标用户的信誉值，能够对目标用户首次访问进行较好的处理。计算公式如下：

$$T_{Rtrust}=\frac{\left|S(u)\cap S(u')\right|}{\left|S(u)\cup S(u')\right|} \tag{6}$$

其中 T_{Rtrust} 指基于用户信誉的信任值。$S(u)$表示目标用户请求访问的资源集合，$S(u')$表示其他用户请求的资源集合。

综合上述三个方面的信任值计算用户的综合信任值：

$$T=\varpi_1 T_{Atrust}+\varpi_2 T_{Btrust}+\varpi_3 T_{Rtrust} \tag{7}$$

其中 ϖ_1、ϖ_2、ϖ_3 分别为用户属性信任值、用户行为反馈信任值、用户信誉信任值的权重，且 $\varpi_1+\varpi_2+\varpi_3=1$。式(7)中的 T_{Atrust}、T_{Btrust}、T_{Rtrust} 分别由式(2)、式(5)、式(6)得到。

根据用户历史访问的信任值进行历史平均信任值的计算并以此作为阈值 ε，假设当前用户前 n 次的信任值分别为 $T_n, T_{n-1}, \cdots, T_1$，由于信任值的时间相关性，其中 n 的取值越大表示距离本次信任值越近，对信任评估的影响也越大。因此引入一个时间参数 $a_i=\frac{1}{1+(m-k)/\rho}\left(0<\rho<1, 1\le k\le m, i=1,2,\cdots,k\right)$ 满足 $a_i > a_{i-1} > \cdots > a_1$，且 $\sum_{i=1}^{k} a_i=1$。其中 m 表示最近一次交互产生信任值的时刻，k 表示第 k 次交互产生信任值的时刻，ρ 表示时间衰减因子。

阈值计算公式如下：

$$\varepsilon = \frac{\sum_{i=1}^{n} a_i \cdot T_i}{n} (i = 1, 2, \cdots, n) \tag{8}$$

其中 a_i 为时间参数，T_i 为用户第 i 次历史访问的信任值。

通过将请求资源访问的用户综合信任值 T 与阈值 ε 进行比较判断用户的可信度，若 $T \geq \varepsilon$，则用户是可信的。反之，用户是不可信的。

2) RBAC 和 ABAC 的结合

通过信任管理进行用户可信度的判断后，在用户集 *Users* 中筛选出不可信用户实现第一次访问控制机制，得到可信用户集 U' 并接受其可信用户请求资源访问。在此基础上，再结合 RBAC 和 ABAC 模型进一步执行访问控制机制。流程图如图 2 所示。

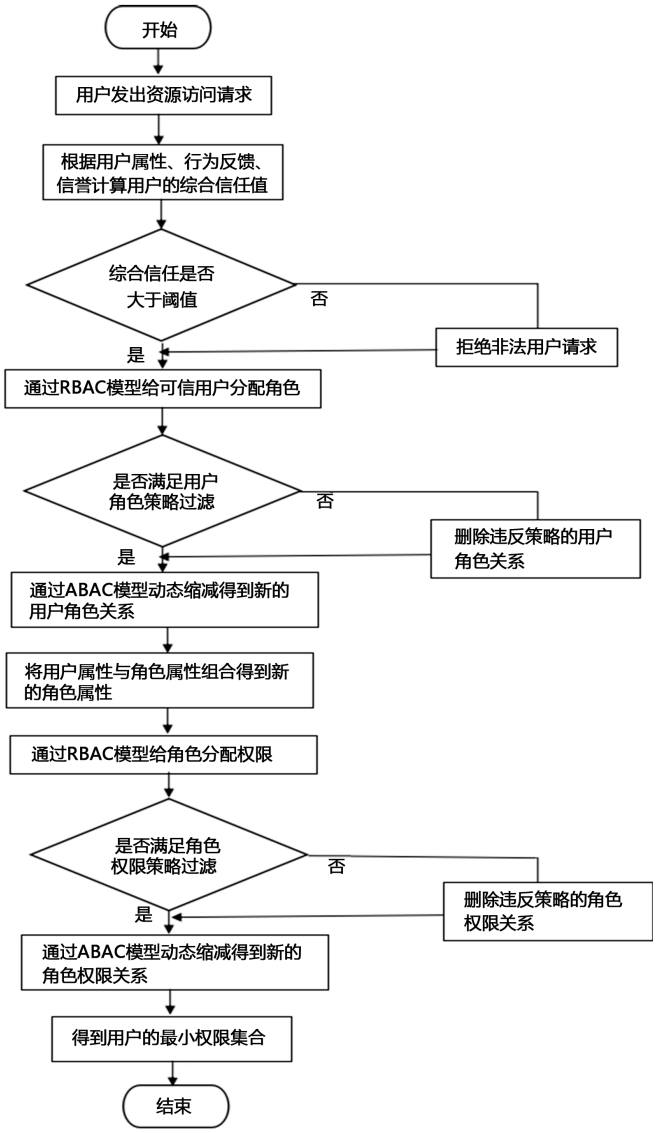

Figure 2. TRABAC model flow chart
图 2. TRABAC 模型流程图

1) 使用 RBAC 模型确定可信用户－角色映射关系，即 $U^{'} \to R$。

2) 使用 ABAC 模型根据用户－角色过滤策略 $policy1 = \{U^{'}, R, U_{ATT}, R_{ATT}, Env\}$ 实现动态角色的过滤，从 $U^{'} \to R$ 映射关系中删除违反上述用户角色策略的映射关系，形成新的用户－角色映射关系，即 $U^{'} \to R^{'}$，其中 $(U^{'} \to R^{'} \subseteq U^{'} \to R)$。图 3 给出了具体的伪代码实现。

输入：可信用户 $U^{'}$，$U^{'} \in Users$； 角色集 R，$R \in Roles$；
输出：新的角色集 $R^{'}$，$R^{'} \in Roles$。

```
1:  R'=R;
2:  policy1 = ({U', R, U_ATT, R_ATT, Env} → {T, F}); /*定义用户-角色过滤策略*/
3:  for r ∈ R do:    /*对可信用户-角色映射关系中的角色集进行循环判断
                       看是否满足过滤策略 policy1 来实现动态角色的过滤*/
4:      if ¬(policy1) then
5:          R' = R \ r;    /*若违反过滤策略，则从角色集 R 中删除，进一步得到
                             新的用户-角色映射关系*/
6:          break;
7:      end if
8:  end for
```

Figure 3. The algorithm of dynamically reducing the user-role mapping relationship
图 3. 动态缩减用户－角色映射关系算法

3) 使用 RBAC 模型确定角色－权限映射关系，即 $R^{'} \to P$。并将用户属性(U_{ATT})与角色属性(R_{ATT})结合形成新的角色属性 $(R_{ATT}^{'})$，其中 $R_{ATT}^{'} = U_{ATT} \cup R_{ATT}$。

4) 使用 ABAC 模型根据角色－权限过滤策略 $policy2 = \{U^{'}, R^{'}, P, R_{ATT}^{'}, O_{ATT}, Env\}$ 实现动态权限的过滤，从 $R^{'} \to P$ 映射关系中删除违反上述角色权限策略的角色权限关系，得到新的角色－权限映射关系，即 $R^{'} \to P^{'}$。其中 $(R^{'} \to P^{'} \subseteq R^{'} \to P)$。图 4 给出了具体的伪代码实现。

输入：可信用户 $U^{'}$，$U^{'} \in Users$；角色-权限映射关系 RP，$RP \subseteq Roles \times Permissions$；
输出：新的权限集 $P^{'}$，$P^{'} \in Permisssions$。

```
1.  RP = Φ; P' = Φ;
2.  for r ∈ R' do: /*执行该循环是为角色分配权限，并得到相应的角色-权限映射关系*/
3:      P = 2^Permissions;
4:          for p ∈ P do:
5:              RP = RP ∪ <r, p>
6:          end for
7:  end for
8:  policy2 = ({U', R', P, R_ATT', O_ATT, Env} → {T, F}); /*定义角色-权限过滤策略*/
9:  for p ∈ P do: /*对角色-权限映射关系中的权限集进行循环判断
                    看是否满足过滤策略 policy2 来实现动态权限的过滤*/
10:     if ¬(policy2) then
11:         P' = P \ p; /*若违反过滤策略，则从权限集 P 中删除，进一步得到新的
                          角色-权限映射关系*/
12:         break;
13:     end if
14: end for
```

Figure 4. The algorithm of dynamically reducing the role-permission mapping relationship
图 4. 动态缩减角色－权限映射关系算法

5)通过上述动态缩减用户－角色映射关系和角色－权限映射关系的步骤进一步达到缩减用户－权限关系的目的，得到用户确定的最小权限关系，即 $U^{'} \to P^{'}$，其中 $(U^{'} \to P^{'} \subseteq U \to P)$。

4. 安全性评价

4.1. 三重控制机制

1) 第一重控制：筛选可信用户，即基于用户信任的访问控制。当用户发出对某一资源的请求访问时，

首先通过对用户的综合信任值进行信任评估判断用户的可信度，对请求资源访问的用户集*Users*中的不可信用户进行筛选得到可信用户集并拒绝非法用户的资源访问请求。

2) 第二重控制：用户－角色映射关系过滤，即基于ABAC模型的第一次动态访问控制。使用RBAC模型对可信用户进行角色分配，然后根据会话中基于属性的用户角色策略动态缩减用户－角色关系得到最小角色集合。

3) 第三重控制：角色－权限映射关系过滤，即基于ABAC模型的第二次动态访问控制。将用户属性与角色属性结合形成新的角色属性并通过RBAC模型确定角色权限分配，再根据会话中基于属性的角色权限策略动态缩减角色－权限关系得到最小权限集合。

最终得到的用户－权限映射关系$U' \to P$，是RBAC模型定义的用户－权限映射关系的子集。由于$U' \to P$的安全性是由RBAC模型保证的，本文提出的访问控制模型通过ABAC模型从$U' \to P$过滤不符合策略的映射关系，最终确定的$U' \to P$不会违反RBAC模型的规则，因此可以保证安全性及动态和细粒度的访问控制。

通过三重控制机制有效地限制了非法用户对资源的访问，同时基于属性的权限过滤策略对会话中用户的角色分配以及角色的可用权限进行了约束和限制，动态控制了用户能够拥有的访问权限并满足用户完成其任务的最小权限原则，实现了细粒度的访问控制，提高了数据资源的完整性及资源访问的安全性，实现了访问控制过程的动态管理。

4.2. 相关模型比较分析

为了更直观地比较TARBAC模型与其它访问控制模型的性能及安全性，本文选取了11个访问控制模型从6个方面进行相关的比较。如表1所示，可以看出TARBAC模型相对于其它访问控制模型更适合动态复杂的云计算环境，能对云中的数据进行安全的访问控制。

Table 1. Comprehensive comparative analysis of access control models
表1. 访问控制模型综合比较分析

模型	主客体属性	云计算	动态性授权	多级安全控制	安全性	最小权限原则
RBAC [5]	不支持	不适用	不支持	不支持	低	不支持
ABAC [6]	支持	不适用	中	不支持	低	不支持
文献[8]	不支持	不适用	低	不支持	低	不支持
ARBAC [9]	支持	适用	中	不支持	中	不支持
文献[10]	支持	适用	高	支持	中	支持
HARBAC [12]	支持	适用	中	支持	中	不支持
文献[15]	不支持	不适用	低	不支持	低	不支持
TRBAC [16]	不支持	适用	低	支持	中	不支持
文献[17]	不支持	适用	低	支持	高	不支持
文献[18]	不支持	适用	低	支持	中	不支持
TRABAC (本方案)	支持	适用	高	支持	高	支持

5. 结论

本文提出了一种支持信任管理的基于角色和属性的访问控制模型(TRABAC)，将信任、RBAC、ABAC三者结合实现了动态性授权、细粒度访问控制及多级安全控制。与现有模型相比，此模型通过对用户信

任的判定、基于属性策略对会话用户分配的角色以及会话角色的有效权限进行缩减，达到防止非法用户访问、允许合法用户访问以及合法用户进行非授权访问的三重访问控制机制的目的。安全性评价表明该模型更加适用于动态和共享的云环境，保证了云计算中访问控制的安全性和动态性。

基金项目

本文得到广东省科技计划项目(2017B090906003)、广州市科技计划项目(201802010043、201807010058)和机器智能与先进计算教育部重点实验室开放课题基金(MSC-201604A)的资助。

参考文献

[1] Almulla, S.A. and Chan, Y.Y. (2010) Cloud Computing Security Management. *Second International Conference on Engineering Systems Management and ITS Applications*, Sharjah, 30 March-1 April 2010, 1-7.

[2] Majhi, S.K. and Dhal, S.K. (2016) A Study on Security Vulnerability on Cloud Platforms. *Procedia Computer Science*, **78**, 55-60. https://doi.org/10.1016/j.procs.2016.02.010

[3] Bertino, E., Samarati, P. and Jajodia, S. (1993) High Assurance Discretionary Access Control for Object Bases. *Proceedings of the* 1*st ACM Conference on Computer and Communications Security*, New York, 3-5 November 1993, 140-150. https://doi.org/10.1145/168588.168606

[4] Rayi, K. (2006) Towards a Location-Based Mandatory Access Control Model. *Elsevier Advanced Technology Publications*, **25**, 36-44. https://doi.org/10.1016/j.cose.2005.06.007

[5] Ferraiolo, D.F., Sandhur, G., *et al*. (2001) Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security*, **4**, 224-274. https://doi.org/10.1145/501978.501980

[6] Yuan, E. and Tong, J. (2005) Attributed-Based Access Control (ABAC) for Web Services. *IEEE International Conference on Web Services*, Orlando, 11-15 July 2005, 569.

[7] 马星晨, 朱建涛, 邵婧, 刘明达. 一种基于属性的去中心化访问控制模型[J]. 计算机技术与发展, 2018, 28(9): 118-122.

[8] Al-Kahtani, M.A. and Sandhu, R. (2002) A Model for Attribute-Based User-Role Assignment. 18*th Annual Computer Security Applications Conference*, Las Vegas, 9-13 December 2002, 353-362. https://doi.org/10.1109/CSAC.2002.1176307

[9] 洪帆, 饶双宜, 段素娟. 基于属性的权限-角色分配模型[J]. 计算机应用, 2004, 14(S2): 153-156.

[10] Qi, H., Luo, X., Di, X., *et al*. (2017) Access Control Model Based on Role and Attribute and Its Implementation. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Nanjing, 12-14 October 2017, 66-71.

[11] Aftab, M.U., Habib, M.A., Mehmood, N., *et al*. (2015) Attributed Role Based Access Control Model. 2015 *Conference on Information Assurance and Cyber Security* (*CIACS*), Rawalpindi, 18-18 December 2015, 83-89. https://doi.org/10.1109/CIACS.2015.7395571

[12] 熊厚仁, 陈性元, 费晓飞, 桂海仁. 基于属性和 RBAC 的混合扩展访问控制模型[J]. 计算机应用研究, 2016, 33(7): 2162-2169.

[13] 王于丁, 杨家海. 一种基于角色和属性的云计算数据访问控制模型[J]. 清华大学学报(自然科版), 2017, 57(11): 1150-1158.

[14] Zhu, Y., Huang, D., Hu, C.J., *et al*. (2015) From RBAC to ABAC: Constructing Flexible Data Access Control for Cloud Storage Services. *IEEE Transactions on Services Computing*, **8**, 601-616. https://doi.org/10.1109/TSC.2014.2363474

[15] Chakraborty, S. and Ray, I. (2006) Trust BAC: Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems. *Proceedings of the* 11*th ACM Symposium on Access Control Models and Technologies*, New York, 7-9 June 2006, 49-58.

[16] 刘武, 段海新, 张洪, 任萍, 吴建平. TRBAC: 基于信任的访问控制模型[J]. 计算机研究与发展, 2011, 48(8): 1414-1420.

[17] 张凯, 潘晓中. 云计算下基于用户行为信任的访问控制模型[J]. 计算机应用, 2014, 34(4): 1051-1054.

[18] 刘萍萍, 闫琳英. 云计算中基于信任-角色访问控制模型的研究[J]. 计算机与数字工程, 2016, 44(2): 286-290.

[19] 许浩海, 于炯, 卞琛, 鲁亮, 金亮. 基于信誉值的结构化数据访问控制模型[J]. 计算机工程与设计, 2018, 39(8):

2407-2411.

[20] Paul, J. (1912) The Distribution of the Flora in the Alpine Zone. *New Phytologist*, **11**, 37-50. https://doi.org/10.1111/j.1469-8137.1912.tb05611.x