# 云计算下基于属性的访问控制方法①

毋 涛, 张 帆

(西安工程大学 计算机科学学院, 西安 710048)

**摘 要**: 云计算作为一种新型的服务模式, 近年来受到各个企业的青睐. 虽有云有三种部署模式, 企业可以自己选择部署方式, 但是云中数据存储和传输安全还是企业最为担心的. 因此, 运用了一种基于属性的控制策略方法(Attribute Based Access Control, ABAC)来保证只有授权用户才有权限来操作云中的数据. 另外运用粗糙集属性约简的方法来减除冗余属性保留权威属性减少策略冲突问题的出现, 加快访问时间.

**关键词**: 云计算; ABAC; 权限; 属性约简

## Model of Attribute-Based Access Control in Cloud Computing

WU Tao, ZHANG Fan

(School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China)

**Abstract**: As a new mode of service, cloud computing receives the favour of various enterprises in recent years. Though there are three kinds of deployment models to be chosen, enterprises also worry about the storage and transmission security of data. A method of Attribute Based Access Control (ABAC) was used to ensure that only authorized users had access to the data in the cloud. In addition, the method of rough set attribute reduction method was used to reduce the redundant attributes, retain authority conflicts and speed up the access time.

**Key words**: cloud computing; ABAC; authorized users; attribute reduction

## 1 绪论

云计算是一种按使用量付费的模式, 这种模式提供可用的、便捷的、按需的网络访问, 进入可配置的计算资源共享池(资源包括网络, 服务器, 存储, 应用软件, 服务), 这些资源能够被快速提供, 只需投入很少的管理工作, 或与服务供应商进行很少的交互[1]. 云计算的基础设施即 IaaS(Infrastructure as a Service)、平台即服务 PaaS( Platform as a Service)和软件即服务 SaaS(Software as a Service)三种服务模式将传统所用的基础设施、功能通过互联网以服务的形式传递给云使用者[2]. 云计算有三种部署方式: 公有云, 私有云和混合云.

公有云是指企业将数据完全交给云服务提供商进行控制. 私有云是企业单独租用云服务提供商的服务或者企业自己搭架云服务平台, 采用私有云对企业来说可能提高了数据的安全性, 但是却提高了企业使用基础设施的成本降低了企业间数据的共享性能. 混合云是指企业对企业至关重要的数据放在私有云上, 其他数据放在公有云上的一种部署方式, 对云服务提供商来说需要具备把公有云和私有云对接起来的能力.

数据作为系统的核心组成部分, 不管采用何种部署方式, 数据拥有者将企业或者个人数据交给云服务商进行管理, 将数据存储在服务器中形成一个巨大的虚拟化云资源池, 用户失去了对数据的完全控制能力. 因此需要采取措施来保证云中数据在存储和传输过程中的安全. 访问控制是云计算中必不可少的保证云数据安全的一个措施, 首先访问控制技术可以防止非法用户对云中受保护数据的非法访问, 其次可以阻止已授权用户对云中资源进行非授权的访问操作. 本文主要对基于属性的访问控制方法进行了介绍, 与粗糙集属性约简方法相结合简化实体属性加快访问时间.

① 收稿时间:2015-05-16;收到修改稿时间:2015-07-02

## 2　基于属性的访问控制方法

访问控制模型是用来描述系统保护状态，以及描述安全状态的一种方法，访问控制技术是确保系统安全的核心技术之一[3].

基于属性的访问方法(Attribute Based Access Control,ABAC)是在基于身份的访问策略(Role Based Access Control,RBAC)基础上发展起来的[4]. RBAC 的主要思想是用户不直接获得访问权限而是通过对不同的角色进行授权来获得访问权限. 而 ABAC 的主要思想是不直接在用户和客体之间进行授权，而是利用主体与客体之间的属性关系作为授权决策的基础. 与 RBAC 控制策略相比 ABAC 更能适应云计算环境下的动态行和扩展性等特点.

基于属性的访问策略 ABAC 中实体属性主要包括四个方面[5]: 主体属性，客体属性，环境属性和权限属性(分别用字母 S、O、E、R 表示). 主体属性主要包括用户的身份，性别，职位，IP 等; 客体属性主要包括使用客体的大小，位置等; 环境属性是指主体对客体操作时的上下文环境因素，包括时间，区域等; 权限属性是指主体对客体的操作范围. 在基于属性的访问策略中主体、客体、化境和权限均用一组属性名及其对应的属性值进行表示，主体对数据的访问请求需要得到权限属性访问值的允许，而权限属性又是基于客体、环境、主体之上的. ABAC 根据数据访问的属性来进行授权操作的而不管数据请求者是谁. 如下图 1 所示，实体与属性之间的访问关系模型图:

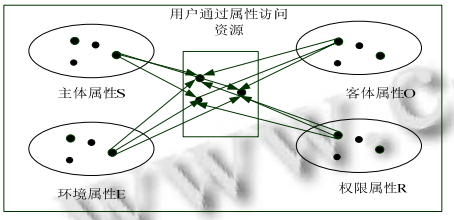


图 1　实体与属性之间的访问关系模型

定义 1. ABAC 可以用四元组{S、O、E、R}来表示. 主体集合记为: $\{s_1,s_3,\cdots,s_m\}$; 客体集合记为 $\{o_1,o_2\cdots,o_n\}$; 环境集合记为 $\{e_1,e_2\cdots,e_k\}$; 权限集合记为 $\{r_1,r_2\cdots,r_j\}$. 属性集合{S、O、E、R}记为 $\{a_1,a_2\cdots,a_m\}$，其中 m、n、k、j≥1.

定义 2. ABAC 所授权的一个四元组 $\{<s_1,s_3,\cdots,s_m>,<o_1,o_2\cdots,o_n>,<e_1,e_2\cdots,e_k>,<r_1,r_2\cdots,r_j>\}$,其中 m、n、j≥1, k≥0. 具体描述为主体属性 $\{s_1,s_3,\cdots,s_m\}$ 在环境属性为$\{e_1,e_2\cdots,e_k\}$的环境下对属性值为 $\{o_1,o_2\cdots,o_n\}$ 的客体进行 $\{r_1,r_2\cdots,r_j\}$ 的权限操作.

定义 3. ABAC 访问策略集表示为: R(p)=$G_1,\cdots G_n,\varphi$，其中≥1, $G_i$ 表示属性的授权谓语词, $\Psi$ 表示所受环境属性约束的授权值. 对于 $\Psi$, $G_i$ 中的任意变量 var, 有 var∈A, 称为属性变量. $G_1,\cdots G_n,\varphi$ 表示策略体，R(p)表示策略头， R∈{ permit,deny}其中 p 是一个常量，用于标示当前策略.

定义 4. ABAC 的访问控制策略集为 P=$\{p_1,p_2\cdots,p_m\}$其中 m≥1，如果满足当前策略，则结果为 permit 即允许访问; 反之则为 deny 阻止其对数据的访问操作.

如下图 2 所示授权用户访问资源实例图，可以简单对上述定义用访问结构树[6]进行描述，此授权结构树对人事部 classID=1 和人事部 classID=2 的用户进行了访问授权操作，只有满足上述条件的用才可以对云中的资源进行访问.

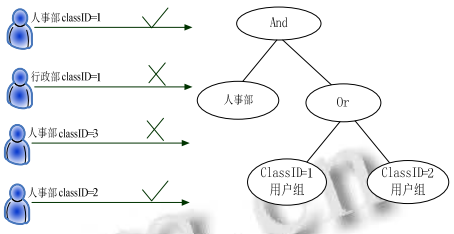


图 2　授权用户访问资源实例

## 3　云计算下基于属性的访问控制方法

### 3.1　粗糙集属性约简方法

属性约简是粗糙集理论知识获取的核心问题之一[7]. 在当今社会因为大数据的出现，系统中存在这不同程度的噪声或者不完整数据，在很大程度影响数据的分析或者决策的判定等，粗糙集就是为了解决数据出现上述问题而提出的.

粗糙集可以看作是一个信息系统，用知识库进行表示[8]. 设 U 代表整个信息系统，它用一个四元组表示为 U={D, A, V, f}. 其中, D 称为论域是一个非空集合，用数据集合可以表示为 D={$x_1,x_2,\cdots,x_n$}，在属性控制策略中代表各个属性的第 i(1≤i≤n)个实例，n 为该类实例的总个数; A 代表的是属性集合，属性包括条件属性 P 和决策属性 d，在决策表中必须包括这两个

属性即 $A=P\cup d$；$V=\bigcup_{p\in P} V_{pj}$ 代表所有属性的值域，其中 $V_{pj}$ 代表论域域 U 中关于属性 p 的值域；f 是一个信息函数 $f: D\times A\to V$ 即 $f(x_i,p_i)=p_{ij}(1\le i\le n;1\le j\le n)$·粗糙集理论的数据处理方法可以按以下几个步骤进行，如图 3 所示.

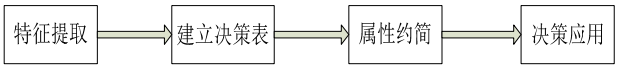


图 3 粗糙集理论属性约简过程图

其中，特征提取和建立决策表是进行属性约简的基础工作.｛S、O、E、R｝代表的是决策判定中的条件属性，用集合表示为 $P=\{p_1,p_2,\cdots,p_n\}$，属性约简的思想是通过采用近似算法使 $P'=\{P'_1,P'_2,\cdots,P'_k\mid 1\le k\le n\}$，最后得到的属性结果是 $P'\subseteq P$.

对于上面的信息系统，如果 $\forall R\subseteq A,x,y\in D$，$X\subseteq U$ 则称 x 和 y 关于 R 是不可分辨的关系(等价关系). X 关于 R 的下近似和上近似可分别表示为:

$$\underline{R}(X)=\{x\mid(\forall x\in U)\wedge([x]_R\subseteq X)\}$$ 和

$$\overline{R}(X)=\{x\mid(\forall x\in U)\wedge([x]_R\cap X\neq\varnothing)\}$$

利用上述原理首先计算出 ABAC 属性组中属性的下近似值，得出决策属性与条件属性的依赖关系，然后解决条件属性 $p_i$ 对决策属性 d 的重要程度:

$$SGF(p,P,d)=\gamma(P,d)-\gamma(P-\{p\},d)$$

式中 $\gamma(P-\{p\},d)$ 表示缺少属性 p 后，条件属性与决策属性之间的依赖关系. $SGF(p,P,d)\in[0,1]$，当 $SGF(p,P,d)$ =0 表述属性 p 是可以约简的，当 $SGF(p,P,d)\neq 0$ 0 时，表示属性 p 是不可约简的.

通过运用上述属性约简方法后得到一组新的 ABAC 授权组｛$<s_1,s_2\cdots,s_{m1}>$，$<o_1,o_2\cdots,o_{n1}>$，$<e_1,e_2\cdots,e_{k1}>$，$<r_1,r_2\cdots,r_{j1}>$｝其中 $m1\le m,n1\le n,k1\le k,j1\le j$. 利用属性约简方法简化主体、客体、环境、权限属性，从中选出权威属性，防止出现决策冲突的情况. 主体属性、环境属性、资源属性是该决策表的条件属性，其中 1 代表考虑该因素的影响，0 反之. 数据安全是该决策表的决策属性，1 代表数据安全，0 反之. 如表 1 所示基于属性的访问控制方法实体属性访问决策表.

表 1 基于属性的访问控制方法实体与访问决策表

| 序号 | 主体属性(S) | | | | 环境属性(E) | | | 资源属性(O) | | 数据安全 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 用户 ID | IP | 性别 | 部门 | 访问时间 | 访问地点 | 所用设备 | **数据**大小 | 存储位置 | |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 2 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 3 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 4 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 5 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 6 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 7 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 8 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 9 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| 10 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |

将上面决策表中的数据进行数据补齐和离散化后，确定条件属性和决策属性的一栏关系，进行属性约简删除其中的不确定因素和冗余属性，得到了入校决策决，如表 2 所示属性约简后的决策表.

通过仿真实验来记录属性个数对访问时间的影响，每次实验只删除一个冗余属性然后记录所需的访问时间，得出实体属性取值数量对访问时间的影响，去除冗余属性得到最简属性集合后，用户访问资源的速度越快，如图 4 所示属性数量与访问时间关系图.

表 2 属性约简后的决策表

| 序号 | 主体属性(S) | | | 环境属性(E) | 资源属性(O) | 数据安全 |
|---|---|---|---|---|---|---|
| | 用户 ID | IP | 部门 | 访问时间 | 存储位置 | |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 2 | 1 | 1 | 0 | 0 | 0 | 1 |
| 3 | 1 | 0 | 0 | 1 | 1 | 0 |
| 4 | 1 | 0 | 1 | 1 | 0 | 0 |
| 5 | 1 | 1 | 0 | 1 | 1 | 0 |
| 6 | 1 | 1 | 0 | 0 | 1 | 0 |
| 7 | 1 | 1 | 1 | 1 | 1 | 1 |
| 8 | 1 | 1 | 0 | 1 | 1 | 0 |
| 9 | 1 | 0 | 1 | 1 | 1 | 1 |
| 10 | 1 | 1 | 1 | 1 | 0 | 0 |

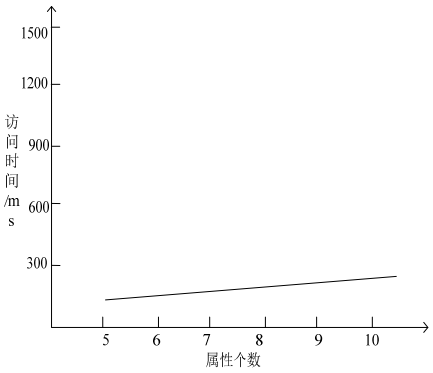


图 4 属性数量与访问时间关系图

在对 ABAC 策略的四元组进行属性约简后，接着进行云计算下属性访问方案的设计.

### 3.2 云计算下基于属性的访问方案

云用户将数据存储在云服务器中，对云服务器的数据共享及其数据保密性的要求也会越来越高. 首先，第三方授权机构对用户进行属性分配，并对其进行管理. 接着数据管理者对用户进行授权操作，授权的用户只能访问操作自己权限之内的数据. 为了避免授权的用户操作非授权的数据，数据拥有者对数据进行加密，将密钥交给第三方授权机构进行数据管理，第三方授权机构将加密处理后数据得到的密钥分配给授权的每一位数据访问者以及数据拥有者，这样密钥就掌握在用户自己手中，数据拥有者将加密后的数据交给云服务提供商进行管理，授权的数据者可以访问下载云中的数据并对其进行操作.

本文采用对数据加密的方法是基于属性的加密方法(Attribute Based Encryption,ABE)中的基于密文的加密策略(CP-ABE),这是一种可以实现可扩展的细粒度

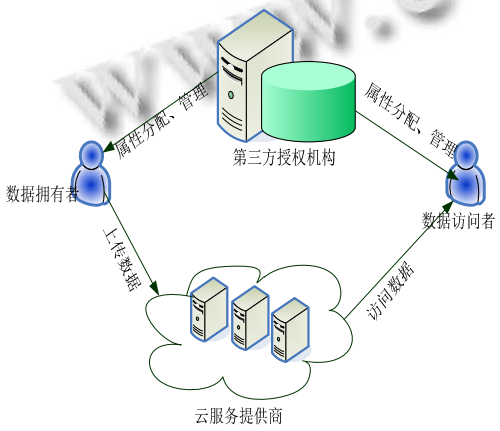


图 5 云计算下数据共享的系统架构

数据共享方法. 基于密文的加密策略与定义的访问结构树(如图 2 提到的访问资源实例图)相关联，使数据拥有者可以制定一种访问策略并在这一策略上进行加密，只有用户在用户属性与密文的访问结构相匹配时，用户才能解密数据进行数据访问.

如图 5 所示云计算下数据共享的系统架构.

## 4 结论

在云计算中实行数据共享，基于属性的访问控制方法是保证云计算中数据安全的一个重要举措. 基于属性的访问方法利用实体的属性进行授权操作，满足云计算分布式应用及其细粒度的特点，当用户对某种客体发出访问请求时，就需要向系统提供自己的属性信息，只有当属性信息访问结构完全匹配的时候用户才有对资源进行访问的权限. 属性信息数量影响用户访问的时间，本文采用属性约简方法对实体属性进行约简，剔除对决策应用无关的属性，从而提高用户访问的速度，本文通过仿真实验验证了通过属性约简与基于属性的访问控制方法(ABAC)相结合结的有效性.

## 参考文献

1 方晓平,陈年生,郭宇等.云计算资源分配策略研究.湖北师范学院学报(自然科学版),2013,(4):56–62.
2 Hirzalla M. Realizing business agility requirements through SOA and cloud computing. Proc. of the 2010 18th IEEE International Requirements Engineering Conference. 2010.
3 Sandu R, Samarati P. Access control: Principles and practice. IEEE Communications Magazine, 1994, 32(9): 40– 48.
4 刘君,曹宝香.基于本体的面向服务的属性访问控制模型.山东科学,2010,23(6):78–81.
5 王立,万世昌，等.基于互信属性调配机制的访问控制模型.计算机技术与发展,2009,(12):127–130.
6 孙国梓,董宇,李云.基于 CP-ABE 算法的云存储数据访问控制.通信学报,2011,32(7):146–152.
7 Jelonek J, Krawiec K, Slowinski R. Rough set reduction of attributes and their domains for neural networks. International Journal of Computational Intelligence, 1995, 11(2): 339–347.
8 李鸿.一种基于粗糙熵的知识约简算法.计算机工程与应用,2005,(14):78–80,148.