# 基于改进 CP-ABE 算法的 ABAC 机制研究*

邹佳顺[1,2]，张永胜[1,2†]，高 艳[1,2]

(1. 山东师范大学 信息科学与工程学院，济南 250014；2. 山东省分布式计算机软件新技术重点实验室，济南 250014)

**摘 要**：为解决基于属性的访问控制(ABAC)机制下的数据安全问题，从访问体系结构和形式化定义两方面对 ABAC 机制进行研究，并进行了仿真和性能分析。通过与传统 CP-ABE 算法进行比较，提出一种适用于 ABAC 环境的改进 CP-ABE 算法，给出了改进算法的形式化定义。与传统 CP-ABE 算法相比，该算法在 ABAC 环境下具有更低的存储消耗和更高的效率。

**关键词**：数据安全；访问控制；属性；CP-ABE 算法；ABAC 机制

**中图分类号**：TP309.2 **文献标志码**：A **文章编号**：1001-3695(2014)06-1860-03

doi:10.3969/j.issn.1001-3695.2014.06.061

# Research of ABAC mechanism based on improved CP-ABE algorithm

ZOU Jia-shun[1,2], ZHANG Yong-sheng[1,2†], GAO Yan[1,2]

(1. *School of Information Science & Engineering, Shandong Normal University, Jinan* 250014, *China*; 2. *Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan* 250014, *China*)

**Abstract**: To solve the data security problem based on the attribute based access control(ABAC) mechanism, the research was done from two aspects of access system structure and formal definition to study the ABAC. This paper also finished the simulation and performance analysis. It proposed an improved CP-ABE algorithm which was applicable to ABAC environment through the comparison with traditional CP-ABE algorithm. Then it gave the formal definition of improved algorithm. The algorithm has less storage consumption and higher efficiency under ABAC environment compared with traditional CP-ABE algorithm.

**Key words**: data security; access control; attribute; CP-ABE algorithm; ABAC mechanism

基于属性的访问控制(attribute based access control, ABAC)机制是近几年研究的热点，它解决了复杂信息系统中的细粒度访问控制和大规模用户动态扩展问题，为开放网络环境提供了较理想的访问控制方案[1]。访问控制流程中离不开数据的加/解密，CP-ABE(ciphertext-policy ABE)作为一种细粒度的加密方式目前也被广泛应用。CP-ABE 是 Bethencourt 等人[2]基于属性加密机制(attribute-based encryption, ABE)提出的。CP-ABE 使用一个属性集合表示一个用户身份，解密依赖用户身份属性是否与访问控制结构相匹配。目前对于 CP-ABE 有许多相关研究，如文献[3]提出了一种在直接模式下支持完全细粒度属性撤销的 CP-ABE 模型，在合数阶双线性群上解决了以往的属性撤销粒度过粗的问题。文献[4]对 CP-ABE 中存在的问题也作了深入探讨。文献[5]将 CP-ABE 机制应用于云存储，防止云存储系统特权用户的内部攻击。而本文提出的是一种优化的 CP-ABE 机制，可以更好地适用于 ABAC 环境，通过共用属性集合从而进行细粒度的加密与访问控制。

## 1 ABAC 策略模型

目前并没有像 DAC、MAC、RBAC 模型一样被广泛接受的 ABAC 模型定义，因此本文将尝试给出 ABAC 的形式化定义。ABAC 策略包括主体、客体、环境、操作、权限五大元素，系统根据主体、客体及环境的属性来决定是否许可相应的权限。

### 1.1 策略模型相关概念

**定义 1** 实体属性是描述实体固有特征的变量，可以抽象化为二元组 $A$(name, Ran)。其中 name 和 Ran 分别表示属性的名称和取值范围。本文用 SA、OA、EA 分别表示主体属性、客体属性和环境属性。

**定义 2** ABAC 可以抽象化为一个四元组 $U$(SA, OA, EA, $P$)。其中 $P$ 表示权限集合；集合{SA, OA, EA}代表 ABAC 模型中所有属性的集合。

**定义 3** 属性谓词 ap 定义为三元组(name, $\propto$, Ran)，其中，$\propto \in \{=, \neq, <, \leqslant, >, \geqslant, 》, 《\}$，《|》为操作符，用以限定属性的取值范围，即 name $\propto$ Ran。其中“》”表示优先于、继承等偏序关系，“《”含义与“》”相反。本文用 sap、oap、eap 分别表示主体、客体和环境属性谓词。

在 ABAC 中，主体、客体、环境分别可由相关属性谓词加以约束，分别记为 SAP、OAP、EAP，其中，$SAP = sap_1 \wedge sap_2 \wedge \cdots \wedge sap_I$，$OAP = oap_1 \wedge oap_2 \wedge \cdots \wedge oap_P$，$EAP = eap_1 \wedge eap_2 \wedge$

**收稿日期**：2013-07-19；**修回日期**：2013-08-20 **基金项目**：山东省自然科学基金资助项目(ZR2011FM019)；山东省研究生教育创新计划资助项目(SDYY11117)

**作者简介**：邹佳顺(1990-)，男，山东青岛人，硕士研究生，主要研究方向为云环境下的访问控制、云计算安全；张永胜(1962-)，男(通信作者)，山东潍坊人，教授，主要研究方向为软件工程环境、Internet/Intranet 工程、网络信息安全(1010336028@qq.com)；高艳(1990-)，女，山东临沂人，硕士研究生，主要研究方向为云计算安全.

$\cdots \wedge eap_K$。

**定义 4**　ABAC 策略 $p$ 定义为 sign ←(SAP,OAP,EAP,ACT),SAP、OAP、EAP 定义见定义 3,ACT = $\{act_1, act_2, \cdots, act_m\}$ 表示操作的集合。sign 取值为 permit 或 deny,分别表示正向、负向授权。

### 1.2　策略评估相关概念

**定义 5**　属性名值对 nvp 表示属性的具体取值,抽象为二元组(name,val),其中 name 和 val 分别对应属性的名称和值。本文用 snvp、onvp、envp 分别表示主体、客体和环境名值对。

对于属性谓词评估,本文借鉴文献[6]的定义:ap 对 nvp 的评估结果 $\| ap \|_{NVP}$ 为真当且仅当两者的属性名相同且 nvp 的取值属于 ap 限定的范围。形式化定义如下:

$$\| ap \|_{nvp} = (nvp.name = ap.name) \wedge (nvp.val \propto ap.Ran)$$

给定属性名值对集合 NVP = $\{nvp_1, nvp_2, \cdots, nvp_m\}$,属性谓词 ap 对 NVP 的评估结果 $\| ap \|_{NVP}$ 为真当且仅当对于任意 ap ∈ NVP 使得 $\| ap \|_{NVP}$ 为真,否则为假。形式化定义如下:

$$\| ap \|_{NVP} = \| ap \|_{nvp1} \vee \| ap \|_{nvp2} \vee \cdots \vee \| ap \|_{nvpm}$$

对于组合 AP = $ap_1 \wedge ap_2 \wedge \cdots \wedge ap_n$,AP 对 NVP 的评估结果 $\| AP \|_{NVP}$ 为真当且仅当对于任意的 ap ∈ AP 有 $\| ap \|_{NVP}$ 为真。形式化定义如下:

$$\| AP \|_{NVP} = \| ap_1 \|_{NVP} \wedge \| ap_2 \|_{NVP} \wedge \cdots \wedge \| ap_n \|_{NVP}$$

**定义 6**　用户请求可以抽象为四元组 Req(snvp,onvp,envp,act)。其中 snvp、onvp、envp 定义见定义 5,act 则表示用户的请求操作。

当用户发出请求时,对于访问策略 $p$ = sign ←( SAP,OAP,EAP,ACT),访问控制策略评估当 $\| SAP \|_{snvp}$、$\| OAP \|_{onvp}$、$\| EAP \|_{envp}$ 均为真时,授权标志 sign 为允许,否则 $\| p \|_{Req}$ 为 not-applicable。对于策略集 $\{p_1, p_2, \cdots, p_n\}$ 的请求返回结果与 1.3 节的策略算法有关。

### 1.3　基于 XACML 的访问控制策略

XACML 策略语言是一种分布式策略语言,对于同一资源可能由不同的策略管理点(PAP)为其制定不同的策略。在 XACML 中定义了四种组合算法来解决冲突,并且避免不必要的运算。分别是以下几种:

a)拒绝优先算法。该算法的思想是一旦有一条规则或策略应用得到一条拒绝的结果,则返回结果为拒绝。

b)许可优先算法。该算法的思想是只要有一条规则或策略的应用结果为许可,则返回结果是许可。

c)首先应用算法。该算法的思想是在应用一组规则或策略过程中,如果有一条规则或策略是可以应用,则算法立即停止,并返回这一条规则或策略的应用结果。如果没有一条规则或策略是可以应用,则返回结果为 not-applicable,如果在处理规则或策略过程中出错,则返回结果是不确定的(indeterminate)。

d)唯一应用算法。该算法的思想是如果策略中只有一条策略可以应用,则返回这条策略的应用结果;如果没有一条策略可以应用,则返回结果是不可应用;如果多于一条策略可以应用则返回结果是不确定的;如果在处理过程中出现错误,或者发现策略无效,则返回结果也是不确定的[7]。

### 1.4　基于 XACML 的决策模型

ABAC 策略的管理基本上遵循 IETF 提出的框架,该框架讨论了基本组件及其相互关系。XACML 在 IETF 策略框架的基础上提出了面向策略实施的数据流模型。XACML 决策机制主要由策略执行点(policy enforcement point, PEP)、策略信息点(policy information point, PIP)、策略管理点(policy administration point, PAP)、策略决策点(policy decision point, PDP)、上下文处理器(context handler)等模块组成。模型如图 1 所示。

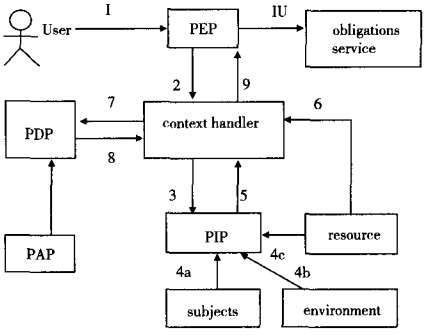


图1　XACML决策模型图

该模型的工作过程为:当客户端用户向服务器提出访问请求时,策略执行点(PEP)将接收到的访问请求转发给上下文处理器。上下文处理器将信息转换为能够接收的语言传达给策略信息点(PIP)。策略信息点(PIP)从主体、客体、环境功能模块获取相关属性返回给上下文处理器。在将这些信息进行一定的处理后向策略决策点(PDP)提出相应的请求。策略决策点(PDP)依据相关策略进行判决,并将判决结果返回给策略执行点(PEP),由策略执行点来实施决策结果,向任务服务器提交任务请求或拒绝用户请求[8]。

## 2　改进 CP-ABE 算法

### 2.1　传统 CP-ABE 算法

传统 CP-ABE 算法主要包括三个组成部分:

a)属性。设 $P = \{P_1, P_2, \cdots, P_n\}$ 为所有属性的集合,则每个用户的属性 $C$ 是 $P$ 的一个非空子集,$C \subset \{P_1, P_2, \cdots, P_n\}$,那么 $N$ 个属性可用于鉴别 $2^N$ 个用户。

b)访问结构。访问结构 $T$ 是全集 $\{P_1, P_2, \cdots, P_n\}$ 的一个非空子集,$T \subset 2^{(P1,P2,\cdots,Pn)}/\varnothing$。$T$ 代表一个属性判断条件,即在 $T$ 中的属性集合称为授权集,不在 $T$ 中的授权集合称为非授权集。

c)访问树。它用于描述一个访问结构,树的每个叶节点代表一个属性项,每个内部节点代表一个关系函数,关系函数可以是 AND($n$ of $n$)、OR(1 of $n$)以及 $n$ of $m$($m > n$)门限等。在实现过程中,访问树的每个节点都可以定义一个多项式,节点的遍历方式为先序遍历[9]。

CP-ABE 算法主要包括四个步骤:

a)Setup。生成主密钥 $MK$ 和公开参数 $PK$。

b)$CT$ = Encrypt($PK, M, T$)。使用 $PK$、访问结构 $T$ 和数据明文 $M$,加密后的数据密文为 $CT$。

c)$SK$ = KeyGen($MK, C$)。使用 $MK$ 和用户属性 $C$ 生成用户的私钥 $SK$。

d)$M$ = Decrypt($CT, SK$)。使用私钥 $SK$ 解密密文 $CT$ 得到明文 $M$。

### 2.2　CP-ABE 算法在访问控制方面的研究

对于将 CP-ABE 算法应用于访问控制机制,已经有学者作过相应的研究,如文献[10]提出一种基于 CP-ABE 算法的密文

访问控制机制，通过将 CP-ABE 算法引入到访问控制机制中来提高访问控制的安全性。但是，其仅仅是笼统地将 CP-ABE 算法的思想应用于访问控制机制，也并未将该算法与具体的访问控制模型相结合，进一步比较各访问控制模型的效率问题。文献[11]研究了基于密文策略属性基加密(CP-ABE)算法的云存储安全机制，实现了类似基于角色的数据访问控制机制。而本文则提出了改进的 CP-ABE 算法，在 ABAC 环境下对 CP-ABE 算法重新进行了形式化定义，并与在其他几种典型的访问控制环境下的 CP-ABE 机制进行比较。

### 2.3 改进 CP-ABE 算法

CP-ABE 算法和 ABAC 策略的共同点是两者都是基于属性的并且操作过程中都需要对主体进行属性收集。本文将尝试给出适合 ABAC 环境下的 CP-ABE 算法的形式化定义。

**定义 7** CP-ABE 属性用主体属性 SA(见定义 1)表示，每个用户的属性 $C$ 不再是单独的属性集合，$C \subset H\{sap_1, sap_2, sap_3, \cdots, sap_n\}$。其中，$H$ 是主体属性谓词的集合，也就是说，用户的属性不再是过去静态的属性而变成了属性谓词。但为防止算法效率的降低，在此可将每个属性谓词 sap 抽象化为新的属性名称。

**定义 8** 访问结构 $T$ 是集合 $H$ 的一个子集，$T \subset H$，代表着授权集合。$T \subset 2^{(sap1, sap2, sap3, \cdots, sapn)}/\varnothing$。

**定义 9** 访问树可形式化为：$sap_1$ ¤ $sap_2$ ¤ $sap_3$ ¤ … ¤ $sap_n$，其中，运算符 ¤ ∈ {∨，∧}，用以对 sap 进行约束。

经过上述定义，CP-ABE 算法可以通过 ABAC 原有属性进行描述，而不必重新建立相关属性，从而节省了存储空间。其算法步骤与传统算法基本相同，只是使用的访问结构 $T$ 和用户属性 $C$ 名称被替换为主体属性谓词名称。改进算法的解密示意图如图 2 所示。

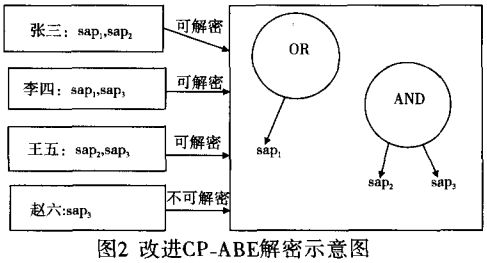


图2 改进CP-ABE解密示意图

## 3 仿真与性能分析

本文的实验环境为 Inter Core 1.73 GHz 的 CPU，2 GB 内存，操作系统为 Windows Server 2003，在 VMware Workstation 6.5.2 上安装了 Ubuntu 10.10，分配了 2 GB 内存。为测试改进与传统算法在 ABAC 环境下的效率问题进行了传统 CP-ABE 算法与改进 CP-ABE 算法在相同 ABAC 环境下的效率测试实验。

如图 3 所示，改进算法由于采用 ABAC 已存在的相关定义，XACML 框架对 CP-ABE 也同样有效。策略信息点(PIP)收集的属性信息节省了 CP-ABE 算法的属性处理时间，提高了算法的效率。

图 4 为采用本文改进的 CP-ABE 算法与传统算法在 ABAC 环境下用户数目为 500 以内、属性数目为 10 时算法的效率比较。图 5 为在属性数目为 10、用户数目为 500 以内时两种算法需要的存储空间比较。

实验结果表明，由于不需要额外的属性存储，并且策略信息点(PIP)的辅助减少了 CP-ABE 的信息收集时间，因此改进后的算法在 ABAC 环境下具有更低的存储消耗以及更高的效率。

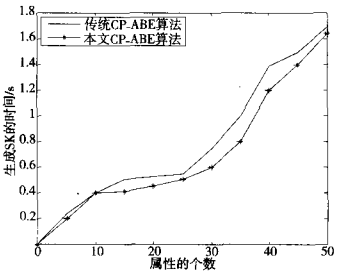


图3 算法私钥产生时间

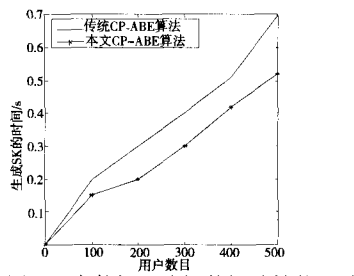


图4 用户数据对访问数据的性能影响

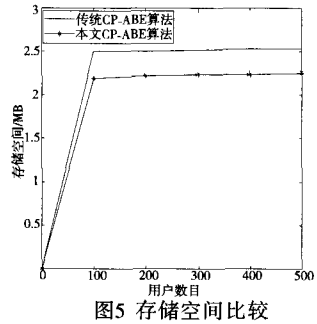


图5 存储空间比较

## 4 结束语

ABAC 访问控制模型与 RBAC 模型相比，ABAC 具有可扩展性强、细粒度访问控制等优点，具有更强的生命力，本文提出的改进 CP-ABE 算法可以很好地与 ABAC 访问控制模型相结合。从上述实验结果可以得出结论：改进的 CP-ABE 算法较原算法在 ABAC 环境中加/解密的速度更快，需要的存储空间更小，是一种更加适用于 ABAC 环境下的加密机制。

**参考文献：**


[1] 王小明，付红，张立臣. 基于属性的访问控制研究进展[J]. 电子学报，2010，38(7)：1660-1668.

[2] BETHENCOURT J，SAHAI A，WATERS B. Ciphertext-policy attribute-based encryption[EB/OL]. (2007-05-23)[2012-02-11]. http://ieeexplore.ieee.org/xpls/abs_all.jsp? arnumber=4223236.

[3] 王鹏翩，冯登国，张立武. 一种支持完全细粒度属性撤销的 CP-ABE 方案[J]. 软件学报，2012，23(10)：2805-2816.

[4] 苏金树，曹丹，王小峰，等. 属性基加密机制[J]. 软件学报，2011，22(6)：1299-1315.

[5] 刘帆，杨明. 一种基于云存储的密文策略属性基加密方案[J]. 计算机应用研究，2012，29(4)：1452-1457.

[6] 程相然，陈性元，张斌，等. 基于属性的访问控制策略模型[J]. 计算机工程，2010，36(15)：131-134.

[7] 陈伟鹏，王娜娜. 基于 XACML 的策略评估优化技术的研究[J]. 计算机应用研究，2013，30(3)：900-906.

[8] 高扬，张家钰，吴敏. 基于 XACML 和 RBAC 的访问控制系统[J]. 计算机应用软件，2006，23(8)：65-67.

[9] 张浩军，范学辉. 一种基于可信第三方的 CP-ABE 云存储访问控制[J]. 武汉大学学报，2013，59(2)：153-158.

[10] 孙国梓，董宇，李云. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报，2011，32(7)：146-153.

[11] 宋开波，罗军，孙金涛. 基于 CP-ABE 算法的云存储数据保护机制[J]. 华中科技大学学报，2012，40(S1)：266-270.