doi:10.11959/j.issn.1000-436x.2016220

# 动态自适应访问控制模型

史国振[1,2]，王豪杰[3]，慈云飞[1]，叶思水[4]，郭云川[5]

（1. 北京电子科技学院信息安全系，北京 100070；2. 西安电子科技大学计算机学院，陕西 西安 710071；
3. 西安电子科技大学通信工程学院，陕西 西安 710071；4. 瑞庭网络技术（上海）有限公司房产技术部，上海 200127；
5.中国科学院信息工程研究所信息安全国家重点实验室，北京 100093）

**摘 要**：随着云计算技术、智慧城市及移动办公的发展和移动智能设备的出现，资源所处的网络环境越来越复杂，传统的访问控制模型已很难满足多样化的访问控制条件以及访问控制策略动态自适应调整的需求。以基于行为的访问控制模型为基础，结合资源生命周期管理，提出了一种动态自适应访问控制模型。该模型以资源生命周期为中心，充分考虑资源的生命周期阶段及其访问控制策略的关联性和动态性，使资源访问控制策略能够随着资源生命周期所处阶段的变化而自动变化，提高了访问控制的灵活性和复杂网络环境下的适用性；模型加入用户访问行为历史管理功能，考虑用户的历史访问行为，进一步约束主体的访问能力，提高模型适应开放的网络环境的能力。最后，在通用访问控制系统和云访问控制系统中对该模型进行了实现和验证。

**关键词**：访问控制；基于行为的访问控制模型；资源生命周期管理；动态自适应；用户历史访问行为

**中图分类号**：TP302 **文献标识码**：A

# Dynamic and adaptive access control model

SHI Guo-zhen[1,2], WANG Hao-jie [3], CI Yun-fei[1], YE Si-shui[4], GUO Yun-chuan[5]

(1. School of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China;
2. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;
3. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China;
4. Dept. of House Technology, Ruiting Networking Technology (Shanghai) Co, Ltd., Shanghai 200127, China;
5. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

**Abstract:** With the development of cloud computing technology, smart city and mobile office and emergence of mobile smart devices, the resources' environment is increasing complex. The traditional access control model has been difficult to meet the diverse access control requirements and the dynamic and adaptive access control policy. A dynamic and adaptive access control model combining the resource life cycle management based on ABAC was proposed. The model focused on resource life cycle management considering the relevance of the resource life cycle management and access control policy. In this model, the policy can be changed as the resource life cycle states' change, so the applicability has been improved. In addition, the user access behavior history management function was added in this model, which can adapt the environment better by considering history of user access behavior. At last, the model in general and cloud computing access control system was implemented and verified.

**Key words:** access control, action-based access control model, resource life cycle, dynamic adaptation, user access behavior history

**收稿日期**：2016-08-12；**修回日期**：2016-10-08

**通信作者**：郭云川，guoyunchuan@iie.ac.cn

**基金项目**：国家重点研发计划基金资助项目（No.2016YFB0800304）；北京市自然科学基金资助项目（No.4152048）；江苏省自然科学基金资助项目（No.BK20150787）

**Foundation Items:** The National Key Research Program of China (No.2016YFB0800304), The Natural Science Foundation of Beijing (No.4152048), The Natural Science Foundation of Jiangsu Province (No.BK20150787)

## 1 引言

作为计算机安全服务核心技术之一，访问控制一直是信息安全领域研究的热点问题。访问控制是一种通过授权策略显式地允许或限制访问能力及范围的方法。通过限制对关键资源的访问，防止非法用户的侵入或合法用户因不慎操作造成的破坏，保证资源受控合法的使用。早期的自主访问控制（DAC, discretionary access control）和强制访问控制（MAC, mandatory access control）已经难以满足越来越复杂的网络环境，基于角色的访问控制（RBAC, role-based access control）应运而生[1,2]。

虽然 RBAC 模型得到了广泛的应用，但是其应用环境相对固定，访问主体及资源动态性较弱。但随着互联网的快速发展以及电子文档资料的普及化，访问控制应用环境更为复杂。以某机构发布公文的流程为例，描述文件在不同的生命周期阶段需要不同的访问控制策略，如图 1 所示。该机构发布公文的完整流程从公文起草开始到发布结束，过程中每次访问行为都将触发文件生命周期阶段的变动，这时就需要不同的访问控制策略保证公文不被非法访问及篡改，保证了公文的安全性，并且极大地提高了发文效率。

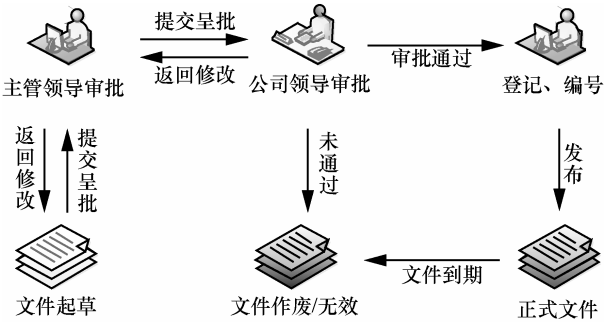



图 1 公司的发文流程

通过对上述发布公文流程的分析，公文所处的不同阶段构成了公文的生命周期，在不同的阶段对公文的访问控制策略要求也不同。因此，访问控制模型需要根据客体所处的环境进行动态自适应调整，必须满足以下需求。

1) 访问控制模型要考虑资源的生命周期，并将其作为访问控制决策时需要考虑的客体属性信息。

2) 访问控制模型能够记录主体历史访问行为。历史访问行为作为资源生命周期动态调整的因素，可以阻止部分主体对资源进行破坏性访问，使权限服务器超出负载而不能正常提供服务的恶意行为；历史访问行为还被作为主体访问的约束条件，即无恶意行为的主体可以正常访问资源，有恶意行为的主体则会被自动拒绝。

3) 访问控制模型进行策略调整时要尽量减少用户的主动操作，做到自适应调整。当主体访问行为触发资源生命周期改变时，模型自动调整资源生命周期所处的阶段，无须主体进行主动干预。

本文以基于行为的访问控制模型为基础，结合资源生命周期管理，提出了一种动态自适应访问控制模型，以资源生命周期为中心，充分考虑资源的生命周期阶段及其访问控制策略的关联性和动态性，使资源访问控制策略能够随着资源生命周期所处阶段的变化而自动变化，提高了访问控制的灵活性和复杂网络环境下的适用性。所提模型加入了用户访问行为历史管理功能，考虑用户的历史访问行为，进一步约束主体的访问能力，能够提高模型适应开放的网络环境的能力。

## 2 相关工作

RBAC 基本解决了 DAC 由于灵活性造成的安全问题和 MAC 不支持完整性保护所导致的局限性问题[3]。但是随着网络的快速普及和发展，对 RBAC 在实用性的基础上提出了更高的要求，即安全性、分布式特性和灵活性。因此，研究人员不断对此进行改进。安全问题是主要的研究内容，首先要保证管理员和系统管理行为安全可信。文献[4]提出了 ATRBAC 模型，通过预处理可达状态减少管理行为处理来自动分析控制策略安全性，将 ATRBAC 策略的安全性问题转化为 BSR 转换系统的可达性问题，实现了对管理员的严格授权。文献[5]通过一个 RBAC test model 和一个 model-implementation mapping 产生可执行的 RBAC test code 自动检测访问控制策略的所有原则。PARBAC 模型[6]极大增强了 RBAC 管理模型的可扩展性和实用性，但是由于不同管理者各自所做出的安全管理策略汇聚在一起使安全性问题更加突出，文献[6]定义了一个对于参数化的管理模型的符号化的可达性分析方法，使设计者和管理者真正明白各种策略的真实含义，有助于他们做出最终决策。分布式特性增加了资源管理的灵活性和可扩展性，但是降低了管理者对这些资源的控制。文献[7]提出了对 TRBAC[8]的管理模型，使用规则表分解和角色表分解 2 种分解方法将 TRBAC 分析问题分解成为更加简单的 RBAC 子问题，虽然

该模型实现了一些模型的管理功能，但是并没有正规地考虑完全的 TRBAC 管理模型，在一定程度上降低了 TRBAC 模型使用程度。文献[9]在 ARBAC97 管理模型的基础上提出了一个 TRBAC 的管理模型 AMTRAC，用于描述角色能够修改定期作用的周期性事件、维持角色触发器的修改及新增和移除角色使能库（role enabling base）成员。以 APP 为代表的网络应用广泛普及，造成网络环境越来越复杂，与之对应的是用户需求也水涨船高，对 RBAC 的灵活性提出了新的挑战。文献[10]针对用户角色、时空位置、客体和访问时间等时空限制条件提出了 STRBAC 模型，用来处理特定应用场景的访问控制制需求。文献[11]提出一种具有可信度特征的多级安全模型，通过在 BLP 模型中增加主客体的可信度标记和可信度评估函数，该模型可以准确地评估访问请求的可信度以及主客体可信度随访问行为变化的情况.以此可信度评估机制为基础，该模型建立了对可信主体的约束机制，使系统可以赋予更多主体有限程度的特权，增加了系统的灵活性和可用性。文献[12]提出了基于动态敏感性标签的用户访问策略，使用动态敏感性标签来标记用户的私有权限和对象的权限、安全级别，分析访问的约束，并帮助用户快速和灵活地访问对象。它采用机密性和完整性执行强制性访问控制，为大型企业系统中灵活，高效的访问控制策略提供理论依据。文献[13]引入了“行为(action)”的概念，将角色、时态约束以及环境约束组成用户行为提出 ABAC，但未把资源的生命周期[14]这一属性考虑进访问控制模型中。

现有的访问控制模型很难满足多样化的访问控制条件以及资源访问控制策略动态自适应调整的需求，本文在 ABAC 的基础上融入“生命周期”因素，提出了一种动态自适应访问控制模型。该模型充分考虑了资源生命周期阶段和访问控制策略的关联性及其动态性，提高了访问控制能力。

## 3　模型概述

为了使基于行为的访问控制模型能够达到自适应的目的，本文在“资源生命周期”和“访问行为历史”等概念的基础上，引入了“资源生命周期管理器”和“访问行为历史管理器”等概念。

**定义 1**　资源从创建到失效的全过程称为资源生命周期。

**定义 2**　资源生命周期包括若干不同的阶段，每个阶段称为资源的生命周期阶段（简称阶段）。资源生命周期管理器则是对不同阶段的资源进行管理控制。

**定义 3**　历史访问行为是指主体过去的访问行为。访问行为历史管理器通过分析主体历史访问行为检测该用户是否有恶意访问行为，使系统功能更安全，并保证系统资源能被更高效地访问。

本文提出的自适应访问控制模型的整体结构如图 2 所示，实线连接表示系统实体间存在数据交

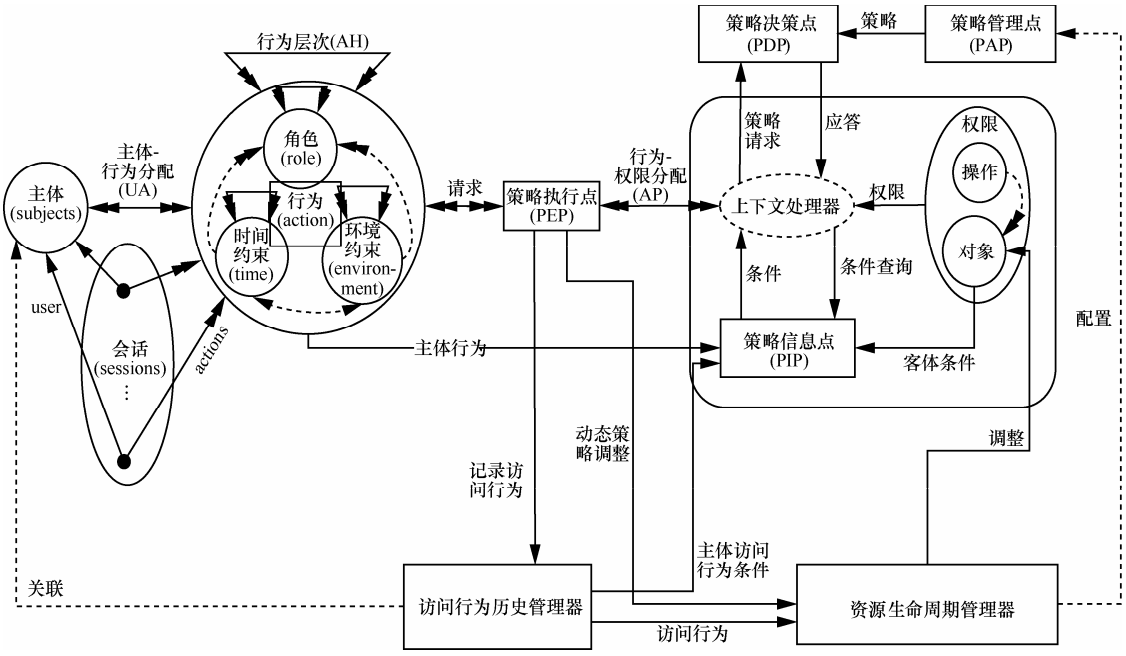



图 2　动态自适应访问控制模型

互，虚线连接表示实体间存在逻辑联系。策略决策点（PDP, policy decision point）综合条件与策略等信息对访问请求进行决策。策略执行点（PEP, policy execution point）负责接收访问请求，并执行访问控制结果。策略信息点（PIP, policy information point）包含请求信息的属性，并且访问控制需要的其他信息由它向其他外部服务器进行请求获取。策略管理点（PAP, policy administration point）定义策略或策略集（描述对特定目标的完整策略），使其对 PDP 可用。上下文处理器负责请求消息与响应消息的解析与转发。资源生命周期管理器依据资源创建时设定的资源生命周期变动触发条件，自适应地对资源所处生命周期阶段进行更改。访问行为历史管理器用于存储主体访问行为的记录，并对这些记录进行分析统计，为 PDP 对访问请求做决策提供依据。

## 4 模型形式化描述与分析

### 4.1 模型形式描述

该模型可分为策略初始化过程、主体访问过程和策略动态调整过程，涉及的符号说明如表 1 所示。

**表 1 动态自适应访问控制模型符号说明**

| 符号 | 说明 |
|---|---|
| $S_i$ | 主体 |
| $O_j$ | 客体 |
| *Ocycle* | 资源生命周期初始状态 |
| *op_* | 操作 |
| *req* | 访问请求 |
| *condition* | 访问条件 |
| *PQ_req* | 访问条件查询请求 |
| *action* | 主体行为 |
| *attr_O* | 客体属性 |
| *attr_H* | 主体访问历史 |
| *per_O* | 资源生命周期 |
| *policy* | 策略 |
| *rule* | 访问控制规则类型 |
| *track* | 用户—权限映射表 |
| *des* | 策略描述 |

1) 策略初始化过程

初始化流程完成访问控制系统的初始化工作。首先，系统管理员依据访问控制需求初始化权限，然后对用户—权限映射表初始化。用 Z 符号语言描述初始化过程如下。

*op*_PriorityInit

{

Input ?: $S_i$, $O_i$, *policy*, *rule*

Output !: *Ocycle*

*op*_init($S_i$, $O_i$, *policy*, *rule*)

Δ*track*

}

2) 主体权限分配过程

访问授权根据已初始化的权限及用户—权限映射表对用户提出的访问请求进行约束，给出允许访问或者拒绝访问的结果。首先，访问控制系统通过函数 Certificate_U 验证用户的身份，若用户身份合法且通过证书验证，返回 TRUE，否则返回 FALSE；函数 Get_UserInfo 获取用户的时空等环境因素；函数 Extract_Req 获取用户的访问请求，最后通过函数 Grant_Response 决定是否授权。用 Z 符号语言描述该过程如下。

*op*_PriorityAlter{

*op*_PriorityAlter{

Input ?: *action*, *attr_O*, *req*, *PQ_req*

Output !: TRUE, FALSE

Certificate_U(*action*)

Get_UserInfo(*attr_O*)

Extract_Req(*req*)

Grant_Response(*PQ_req*)

}

3) 策略动态调整过程

策略动态调整包含 2 部分：以资源生命周期为中心的策略调整和基于用户访问行为历史的调整。在以资源生命周期为中心的策略调整过程中，首先，资源生命周期更改函数 Cycle_Alter（）对生命周期进行更改，然后触发权限变动函数 Priority_Alter（）对权限进行更改。在基于用户访问行为历史的调整过程中，首先由用户访问行为统计分析函数 User Behave_Stat（）获得用户访问行为历史记录，再由用户访问行为历史变动函数 UserBehaveH_ Alter（）对用户访问行为历史进行更改。其 Z 符号语言描述如下。

Input ?: *per_O*, *Policy*, *attr_H*, *action*
Output !: Δ*policy*, Δ*per_O*
Cycle_Alter(*per_O*)
　　Δ*per_O*
Priority_Alter(*policy*)
　　Δ*policy*
UserBehave_Stat(*attr_H*)
　　Δ*attr_H*
UserBehaveH_Alter(*action*)
　　Δ*action*
}

### 4.2　模型分析

ABAC 模型已分析过其安全性和其功能[13]。本文的模型细化了对象的属性，加入资源生命周期和访问行为历史。ABAC 的管理模型可以控制权限分配的安全，而该模型可以保证其在安全性的前提下更具灵活性。

该模型既引入资源生命周期的概念，也加入了历史行为访问约束。主体历史访问行为可以作为条件供模型动态调整资源生命周期阶段，经过访问行为历史管理器的统计分析，用于判断主体是否有恶意访问行为。

该模型的动态自适应特点体现在 2 方面。主体的生命周期阶段可以根据预先设计的调整方式进行动动态调整，并对相应的访问控制策略进行动态更新；对用户行为进行动态监测，可以自适应地拒绝用户对资源的恶意访问行为。该模型与其他模型的特征比较如表 2 所示。

**表 2 ABAC 模型与现有几种访问控制模型的特性比较**

| 模型 | 角色 | 时态 | 环境 | 资源生命周期 | 访问行为历史 | 机密性 | 完整性 | 灵活性 |
|---|---|---|---|---|---|---|---|---|
| RBAC | Yes | No | No | No | No | No | Yes | 低 |
| ABAC | No | No | No | No | No | Yes | No | 中等 |
| L-RBAC | Yes | No | No | Yes | No | Yes | Yes | 中等 |
| 文献[12] | No | No | No | No | No | Yes | No | 中等 |
| 文献[13] | No | Yes | No | No | No | Yes | Part | 中等 |
| 本文模型 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | 中等 |

## 5　模型实现机制

下面主要介绍在主体访问过程和策略动态调整过程中的资源生命周期管理过程和访问行为历史管理过程。

### 5.1　资源生命周期管理过程

资源生命周期管理器接收 PEP 的资源生命周期调整操作，通过与 PAP 交互接口对访问控制策略进行动态调整。资源生命周期管理过程分为资源生命周期初始化和资源生命周期调整 2 个阶段。资源管理器的内部结构，如图 3 左侧所示。

资源生命周期初始化主要是主体将资源通过授权服务器提供给其他用户共享时，为资源设置生命周期的各个阶段，并为各个阶段设置对应访问控制策略。其算法描述如下。

**算法 1**　资源生命周期初始化

**输入**　资源生命周期阶段 $Ocycle_i$，对应的策略 $policy_i$ 及策略描述 $des_i$

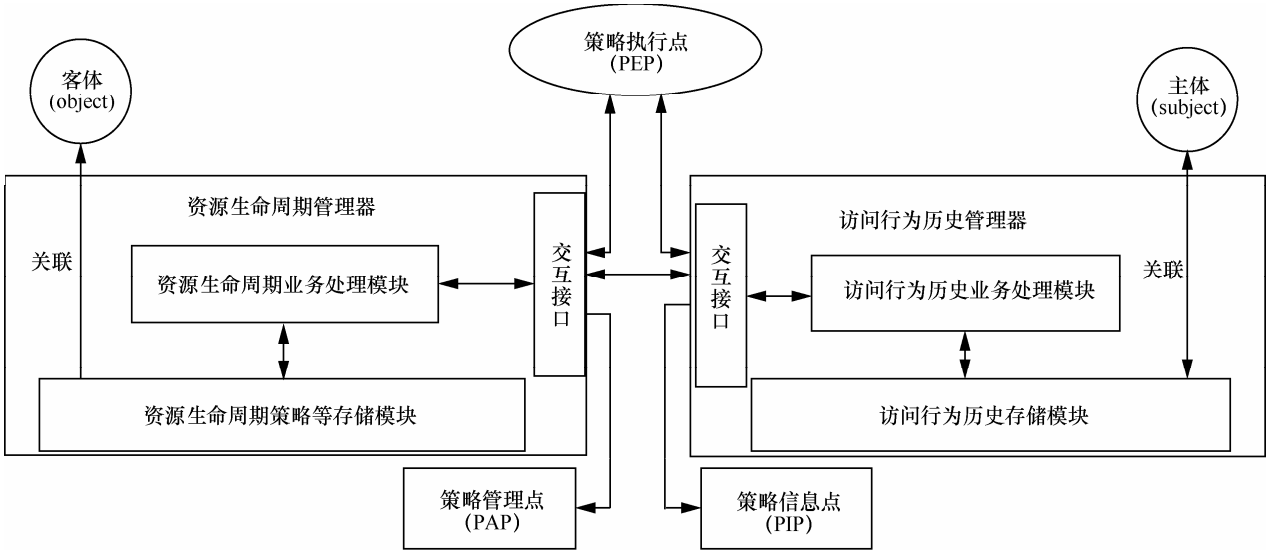



图 3　资源生命周期管理器访问行为历史管理器

**输出** 初始化成功 TRUE

1) $n \leftarrow Ocycle$

//主体设置资源生命周期阶段数

2) while $i<n$ do

3) $Ocycle_i \leftarrow Ocycle(i)$

4) $policy_i \leftarrow policy(i)$

5) $des_i \leftarrow des(i)$

6) end while

7) PacketToPEP(*packet*)

//PEP 接收到相应的初始化数据分组并解析

/*与 PAP 交互接口设置该资源的生命周期第一阶段的访问控制策略。*/

8) $PAPOcycle = Ocycle_1$

9) $PAPPolicy = policy_1$

10) $PAPdes = des_1$

11) output TRUE

当有生命周期调整的触发条件发生时，该服务程序对资源所处的生命周期阶段进行动态调整，同时将存储模块中对应阶段的访问控制策略提交给 PAP，对访问控制策略进行自适应的更新。其算法描述如下。

**算法 2** 资源生命周期动态自适应调整

**输入** 资源生命周期阶段调整触发条件 *condition*：时间 *t*，环境 *e*，属性 *att_h*

**输出** 调整成功 TRUE

1) switch(*condition*)

2) case *t*:

3) *per_O*=*per_ot*;

4) break;

5) case *e*:

6) *per_O*=*per_oe*;

7) break;

8) case *attr_h*:

9) *per_O*=*per_oattr_h*;

10) break;

11) default:

12) break;

13) output TRUE

### 5.2 访问行为历史管理过程

访问行为历史管理器主要功能是将访问控制行为通过上下文处理器交互接口存储在访问行为历史存储模块，访问行为历史处理模块通过访问行为历史数据统计得到恶意用户，将作为一种参考传递给 PIP 用以判断恶意用户访问控制。访问行为历史管理器结构如图 3 右侧所示。它主要分为 2 个过程，初始化过程和历史数据处理过程。

初始化过程主要是为存储和统计主体访问行为历史数据做准备。主体 $S_i$ 向授权服务器第一次发出访问控制请求，PIP 通过访问行为历史管理器与 PIP 交互接口获取对应主体的访问控制历史信息。由于访问行为历史管理器中没有对应主体的行为历史记录，访问行为历史业务处理模块不能获取对应的访问控制历史信息，将该主体的合法访问与非法数据访问初始化为 0。其算法描述如下。

**算法 3** 访问行为历史管理初始化

**输入** 主体第一次发出访问控制请求 *req*

**输出** 调整成功 TRUE

/*用户第一次发出访问控制请求，包含主体 $S_1$、操作 $op_1$ 和客体 $O_1$*/

1) $S=S_1$

2) $op=op_1$

3) $O=O_1$

4) *setLegalFlag*←0

//将该主体的合法访问标识设置为 0

5) *setIllegalFlag*←0

//将该主体的非法数据访问标识设置为 0

6) output TRUE

历史数据处理过程是对主体访问行为进行分析，主要分析 2 个指标，一是授权用户的恶意攻击，二是非授权用户的恶意试探。本文模型中使用阈值 *N*，当主体在规定时间 *T* 内执行了相同的访问的次数 $n>N$ 时，则认为该用户为恶意访问用户。为防止用户的持续的恶意访问，将该分析结果通过 PIP 提供给 PDP，作为主体访问控制的需要考虑的因素之一。其算法描述如下。

**算法 4** 访问行为历史管理历史数据处理过程

**输入** 主体发出访问控制请求 *req*

**输出** 调整成功 TRUE

/*用户发出第 *i* 次访问控制请求，包含主体 $S_i$、操作 $op_i$ 和客体 $O_i$*/

1) $S=S_i$

2) $op=op_i$

3) $O=O_i$

4) if $n>N$ do

5)　*setLegalFlag*=1
//将该主体的合法数据访问标识设置为 1
6)　*setIllegalFlag*=1
//将该主体的非法数据访问标识设置为 1
7) else
8)　*n*++
//访问控制次数+1
9) end if
10) output TRUE

## 6　实验分析

为了验证该模型的实用性和正确性，本文基于云环境设计了一个支持自适应访问控制的资源共享方案。该方案主要包括 3 个过程，即资源创建过程、策略动态调整过程以及资源获取过程。

该方案部署结构如图 4 所示，包括用户、授权服务器以及资源服务器 3 个实体。

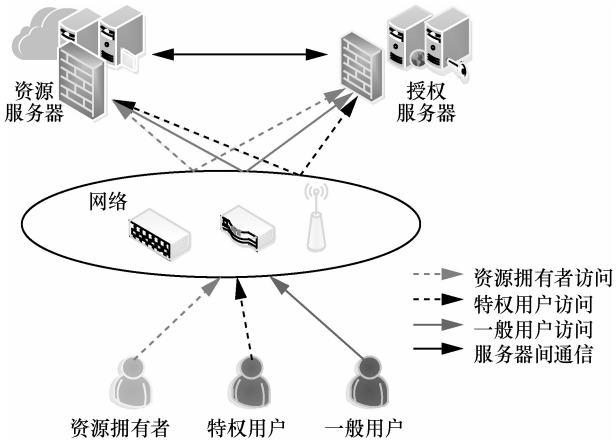
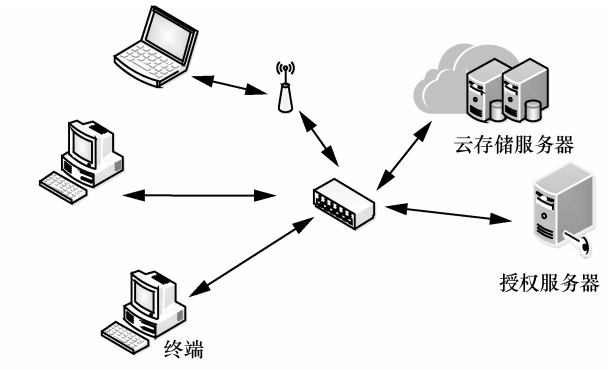


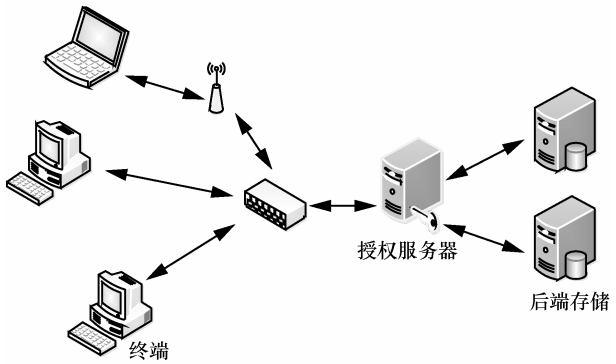

图 4　资源共享方案拓扑

为了对比系统中加入资源服务器与未加入资源服务器性能差异，将这 2 个系统的响应时间进行测试对比分析，各自的部署架构如图 5 所示。其中，云服务器集群采用 3 台主机，每台主机采用双核 2.4 GHz 的 CPU，4 GB 的内存，主机间使用吉比特以太网连接。测试文件大小分别为 500 MB 和 1 GB，即服务器不仅要完成对用户对资源的验证，还要向客户端传输 500 MB 或 1 GB 的资源。

测试结果如图 6 所示，资源共享方案中采用云存储技术，能够很大地提高其并发访问的处理能力，从而提高处理性能。




(a) 已集成云计算访问控制系统




(b) 未集成云计算访问控制系统

图 5　2 个系统部署架构

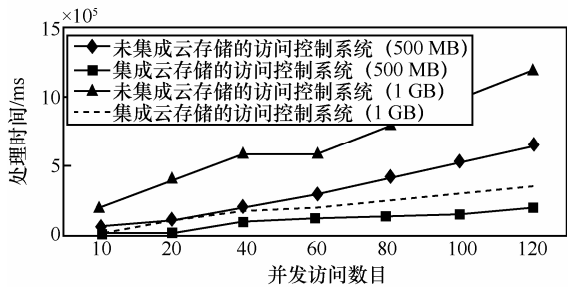



图 6　性能对比

## 7　结束语

本文通过介绍公司文件发布过程，分析了自适应访问控制的需求，引入基于行为的访问控制模型，并分析其在自适应访问控制中存在的问题，设计了一个带有主体的访问行为历史以及资源生命周期的动态自适应访问控制模型。访问控制历史管理器负责主体历史行为的记录与分析，避免用户的恶意访问；资源生命周期管理器负责资源生命周期的调整和相应访问控制策略相应变动。该模型以资源生命周期为核心，访问控制系统依据其变动规则对资源生命周期进行自动调整，并对访问控制策略进行动态自适应调整，能很好地实现资源的自适应访问控制，提高了该模型对开

放网络环境的适应能力。该模型为云端数据访问控制策略动态自适应的实现提供了重要理论和技术支撑。

## 参考文献：


[1] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[2] SANDHU R, BHAMIDIPATI V, MUNAWER Q. The ARBAC97 model for role-based administration of roles[J]. ACM Transactions on Information & System Security, 1999, 2(1): 105-135.

[3] 李凤华, 苏锟, 史国振, 等. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805-813.
LI F H, SU M, SHI G Z, et al. Research status and development trends of access control model[J]. Acta Electronica Sinica, 2012, 40(4): 805-813.

[4] RANISE S, TRUONG A, ARMANDO A. Scalable and precise automated analysis of administrative temporal role-based access control[C]// ACM Symposium on Access Control Models and Technologies. ACM, 2014: 103-114.

[5] XU D, KENT M, THOMAS L, et al. Automated model-based testing of role-based access control using predicate/transition nets[J]. IEEE Transactions on Computers, 2015, 64(9): 2490-2505.

[6] STOLLER S D, YANG P, GOFMAN M I, et al. Symbolic reachability analysis for parameterized administrative role-based access control[C]// ACM Symposium on Access Control Models and Technologies. ACM, 2009: 148-164.

[7] UZUN E, ATLURI V, VAIDYA J, et al. Security analysis for temporal role based access control[J]. Uzun Emre, 2014, 22(6): 177-186.

[8] BERTINO E, BONATTI P A, FERRARI E. TRBAC: a temporal role-based access control model[J]. ACM Transactions on Information & System Security, 2001, 4(3): 191-233.

[9] SHARMA M, SURAL S, VAIDYA J, et al. AMTRAC: an administrative model for temporal role-based access control[J]. Computers & Security, 2013, 39(39): 201-218.

[10] TOAHCHOODEE M, RAY I. On the formalization and analysis of a spatio-temporal role-based access control model[C]//IFIP Wg 11.3 Working Conference on Data and Applications Security. Springer-Verlag, 2008:399-452.

[11] 谭智勇, 刘铎, 司天歌, 等. 一种具有可信度特征的多级安全模型[J]. 电子学报, 2008, 36(8):1637-1641.
TAN Z Y, LIU D, SI T G, et al. A multilevel security model with credibility characteristics[J]. Acta Electronica Sinica, 2008, 36(8): 1637-1641.

[12] BO L, CHUNXIA J, YILIN L. A user access policy based on dynamic sensitivity label[C]//Network Computing and Information Security, International Conference on IEEE. 2011:13-16.

[13] 李凤华, 王巍, 马建峰, 等. 基于行为的访问控制模型及其行为管理[J]. 电子学报, 2008, 36(10): 1881-1890.
LI F H, WANG W, MA J F, et al. Action-based access control model and administration of actions[J]. Acta Electronica Sinica, 2008, 36(10): 1881-1890.

[14] 李良军. PLM 中权限控制的研究与设计[D]. 西安: 西安电子科技大学, 2012.
LI L J. Research and design of access-control in product lifecycle management (PLM)[D]. Xi'an: Xidian University, 2012.


## 作者简介：


**史国振**（1974-），男，河南济源人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为网络与系统安全、嵌入式安全。

**王豪杰**（1991-），男，山东青岛人，西安电子科技大学硕士生，主要研究方向为访问控制与网络安全。

**慈云飞**（1989-），男，安徽池州人，北京电子科技学院硕士生，主要研究方向为访问控制和信息安全。

**叶思水**（1989-），男，江西南昌人，瑞庭网络技术（上海）有限公司技术员，主要研究方向为网络安全。

**郭云川**（1977-），男，四川营山人，博士，中国科学院信息工程研究所副研究员，主要研究方向为物联网安全、形式化方法。