文章编号：2096-1472(2017)-02-50-04

一种基于云计算的网络访问控制方法

杨 波，张 云，王 欣
（兰州文理学院电子信息工程学院，甘肃 兰州 730010）

摘 要：在分析云计算安全研究技术的基础上，以中国墙模型为基础，结合有关访问控制的特点，提出了一种改进的基于云计算的网络访问控制安全方法，该方法使用云端服务器与客体所有者通过作业分配权限的方式，具有清晰的身份管理层次，具有较好的灵活性和安全性，能满足网络访问控制需求。通过仿真实验，实现了强制访问控制下各级用户访问的分级管理，表明了有效性。

关键词：云计算；中国墙模型；网络访问控制
中图分类号：TP393 **文献标识码**：A

A Network Access Control Method Based on Cloud Computing

YANG Bo,ZHANG Yun,WANG Xin
(*School of Electron Information and Engineering,Lanzhou University of Arts and Science,Lanzhou* 730010,*China*)

Abstract: Based on the Chinese Wall model,the paper analyzes the technology of cloud computing security,and then integrates the characteristics of access control to propose an improved network access control method.The cloud server is applied in this method,and assigns authority with the object owner.The methods can satisfy the requirements of network access control with the clear hierarchy management level,good flexibility and high security.The simulation experiment results show that the method can implement the hierarchical management to users at different levels under mandatory access control with good effectiveness.

Keywords:cloud computing;Chinese wall model;network access control

1 引言(Introduction)

随着网络的飞速发展，云计算已经悄然来到我们身边。20个世纪60年代，麦卡锡提出了一种把计算能力作为公用事业提供给用户的理念，这成为云计算思想的起源。随着20个世纪80年代网格计算技术的出现，90年代公用计算技术的发展，以及20世纪初虚拟化技术、SOA、SaaS的广泛应用，云计算作为一种新兴的资源使用和交付模式已经开始逐渐为学界和产业界所认知。云计算一系列的可供所有用户共享访问的资源，这些资源可以被虚拟化，并且可以能够动态升级。即使不懂云计算技术用户，可以按照各自需求以租赁的方式访问云，大大的方便了用户的使用。云计算以互联网为媒介提供服务，提供动态、可伸缩、虚拟化的资源计算模式。这种涉及以互联网来提供动态、可伸缩、虚拟化资源的计算模式通常有基于互联网的相关服务的增加、使用和交付等模式。运用云计算技术可以按照需求方便快捷的从互联网上共享的资源池中获得信息，共享的资源池中的资源可以来自网络、服务器、存储、应用和服务。云计算的这种资源模式和业务资源应该支持通过简洁的管理或交互过程快速地部署和释放[1]。

云计算以动态的服务计算为主要技术特征，以灵活的“服务合约”为核心商业特征[2]。传统的数据存储模式在云计算环境中被打破，云端服务器中存储着所有数据，这些数据以托管的方式存在，用户通过应用程序编程接口(即API)，使用浏览器来获得所需要的数据和服务[3]。这种变化为用户带来了很大方便，同时引发了基于云计算的信息系统存在的安全隐患。如恶意访问者的恶意行为导致的资料外泄；供应商系统遭到大量恶意软件攻击；云端服务器中共享信息的不安全性；以及黑客盗取供应商系统的数据等。近年来，云计算安全问题大致分为三个方面：第一方面，云计算服务提供商提供的网络、存储是否安全，是否会造成数据泄密。第二方面，云计算服务提供商提供的服务是否安全，客户数据本身是否安全。第三方面，客户账户是否安全，是否能够防止他人盗取客户账号使用云中的服务，而让客户埋单[4]。

本文从云计算环境入手，分析了中国墙访问控制模型，RBAC96模型的优缺点，发现由于云计算环境的特殊性，数据存储时采用传统访问控制模型已不适合，突出表现就是用户数据安全的重要隐患体现在访问控制过程。本文提出的基于云计算的网络访问控制安全方法考虑了层次分明的身份方法管理，兼顾访问控制的分布式要求，基于云计算环境下的云端服务器，使作业权限的分配与客体所有者共同完成。

2　相关研究(Correlational research)

中国墙安全模型由Brewer和Nash提出。

中国墙模型又叫做Brewer and Nash model，是一种提供可动态改变的信息安全访问控制的安全模型。运用这种模型进行信息访问控制，可以减轻客户在商业组织中的利益冲突。在这个模型中，如果一个主体和客体在某种方式下能产生利益冲突，那么在它们之间的信息流将是被禁止的。例如，如果一个项目经理在多家企业同时实施同一领域的工程，那么在每个企业中他只能看见有限的信息，如果某个信息对其他企业有利，那么他将被禁止访问。

中国墙模型的创建是基于假设的，然而等价关系并不总是成立的，并且全体对象也并不总是等价类。因此如何防止非法授权访问机密信息就成了网络访问控制的关键。

RBAC96模型由Sandhu等人提出。该模型认为客户不会一成不变，针对变化的客户灵活提供的安全策略。有关研究人员受到该模型客户灵活度的启发，从理论上对客户关系进行了进一步分层化划分，寻找不同客户间隐藏关系，进而分析出可信度。

3　安全模型(Security model)

本文提出的基于云计算的网络访问控制安全模型，通过分析云计算平台下的客户特点，按照客户访问行为特征辨析身份，综合考虑实例和权限等网络访问要素，将其用于中国墙安全策略模型，支持RBAC系统，实现强制访问控制，在客户多层次角色灵活性方面增加了中国墙模型的安全性。

该模型是一种基于云计算的网络强制访问控制形式，它采用中庸策略，也就是说每一个用户在体系里的权限不是确定的，是依据身份的不同而不同的，这样一个系统里的安全策略就变得多元了。模型中的基本要素是身份，有了不同的身份才可能有响应的任务，通过多层次身份的定义，划分出对应的多层次的任务，不同的任务才会被分配到响应级别的权限，同一个客户在不同的场景下访问时，可能由于身份不同而获得不用的权限，从而使得权限与客户分开，实现了强制访问控制，增强了安全性。

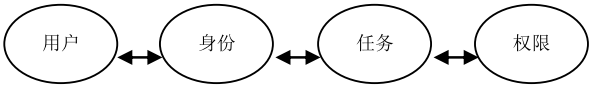

图1 安全模型

Fig.1 Security model

4　基于云计算的网络访问控制安全方法(Network access control security method based on cloud computing)

在本方法中，将整个作业过程看成很多细小的任务，这些任务之间存在关联，相互依赖，然后依据职能和责任将任务分配给身份，身份通过执行任务实例从而得到权限。访问权限的控制通过约束集可以实现，从而实现控制策略。客体的权限的获得是据身份并通过任务，会话通常由用户发起，在面向对象方面，身份间的部分关系可实现继承。

本方法的定义如下：

用户集$V=\{v_j \mid j=1,2,\cdots,n\}$。

身份集$S=\{s_j \mid j=1,2,\cdots,m\}$。

任务集$R=\{r_j \mid j=1,2,\cdots,k\}$。

任务实例$RL=\{rl_j \mid j=1,2,\cdots,k\}$。

权限$Q=\{q_j \mid j=1,2,\cdots,p\}$。

操作P，程序映像，可执行的。

会话T，用户需要身份时，必须发起会话。回话可以激活用户身份，激活的身份仅用于当次访问，该次激活身份的权限也仅用于当次身份。

约束集K，用于限制当次访问控制中的规则集合。

$F-SC$，层次身份继承的部分$S_1, S_2 \in F-SC, S_1 >^* S_2$，$\forall R_j \in S_2$

$R_j \in H \cup A \Rightarrow S_i$继承$R_j$的所有权限和S2的读权限。

$VSB: VSB \subseteq S \times V$,用户身份分配。

$RQB: RQB \subseteq Q \times R$,任务权限分配。

$LQB: LQB \subseteq Q \times RL$,实例权限分配。

$RSB: RSB \subseteq S \times R$,任务身份分配。

$LSB: LSB \subseteq S \times RL$,实例身份分配。

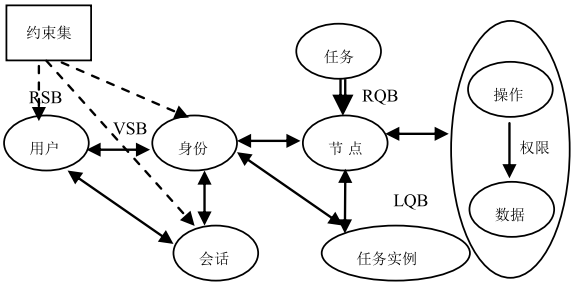

图2 基于云计算的网络访问控制安全方法

Fig.2 Network access control security method based on cloud computing

5　基于云计算的网络访问控制需求(Network access control requirements based on cloud computing)

在云计算平台环境下，数据存储面临网络威胁，相应产生云存储的安全问题。使用云计算平台的用户在存储和读取数据时，也有不用于本地局域网的用户需求。

(1)访问者类型

在云计算平台环境中，数据的访问者不仅仅是存储用户，还包括两类用户，即提供云计算平台的供应商和有相应身份权限的访问者。云计算平台的供应商负责存储用户交付的数据，这里涵盖日常数据的维护、安全性保障、数据一致

性、数据恢复等；有相应身份权限的访问者主要的行为是读取数据，把关的关键就是访问权限，依据身份的不同，任务的不同，获取不同的身份权限，任务权限，需求不同，权限也不同。

(2)数据类型

在云计算平台环境中，用户交付存储的数据的安全性首先取决于服务提供商的网络环境是否安全。云计算平台环境中的服务器自身存储数据也存在着安全性，以及数据完整性的问题。因此，云计算环境下，从数据角度分析，数据的访问控制应当根据不同的安全等级设置不同的访问控制。

6 基于云计算的网络访问控制策略(Network access control policy based on cloud computing)

依据不同用户的访问控制需求，采用作业分解的方式实现对访问权限分配的控制。用户依据行为获得身份，依据身份获得任务，依据任务获得权限，最终权限被分配的不是用户，而是分解后的作业，最后依据作业的不同级别实现安全的分级访问控制。

基于云计算的网络访问控制方法中，将作业分成四大类：私有类作业S、管理类作业G、日常类作业R、活跃类作业H，从而细化对作业权限分配的管理，作业的区别如表1。

表1 作业

Tab.1 Operation

任务	类别	特征
S	私有类	非继承，被动
G	管理类	部分可继承，被动
R	日常类	非继承，主动
H	活跃类	部分可继承，主动

基于云计算的网络访问控制方法的访问控制策略是基于作业的，采用作业分解的方式实现对访问权限分配的控制。用户的身份通过分解了的作业得到，主体的访问权限通过实例权限分配得到。基于云计算的网络访问控制方法的访问控制组件属性如表2。

表2 组件属性

Tab.2 Component attributes

组件名称	组件属性
用户	用户名，用户类别
身份	身份名，身份类别
作业	作业名，作业类别
ZL	作业名，ZL名，执行时间
Q	Q名，对象，访问类别
T	T名，用户名，身份名
SH	身份关联
LSB	ZL名，身份名
VSB	用户名，身份
LQB	ZL名，权限

在实际的云计算服务环境中，来访用户访问行为非常复杂，用于保证网络访问控制的策略需要考虑的问题很多，本文方法主要考虑四个方面：

(1)用户身份类别

云计算平台环境中，数据的访问者不仅仅是存储用户，还包括两类用户，即提供云计算平台的供应商和有相应身份权限的访问者。

本文方法中，提供云计算平台的供应商的身份权限分配策略，可以依据多层次身份管理，从而获得多层次权限管理；提供数据的存储用户身份权限分配策略，可以通过强制访问控制任务实例获得多层次权限管理；有相应身份权限的访问者可以通过对一次访问过程进行工作流作业分解，从而利用实例分配权限，简化了用户管理和权限分配工作，每次为相同的客体访问者创建作业实例(这里考虑的是外部共享访问者对数据的操作大多是读操作)。云计算服务提供商不再拥有对数据的超级权限，预防安全隐患。

(2)作业分解类别

在基于云计算的网络访问控制方法中，作业的分类详细分类了对数据访问控制的安全等级。

本文中使用S、G、R、H对一次访问工作流中的作业分解划分安全等级。一旦用户发出访问请求，就激活了会话，分解后的作业被启动，依据身份的层次，获得相关权限。

(3)信息安全控制

在通常的网络访问控制方法中，网络环境中采用非对称密钥系统进行密文存储，传输的信息安全数据安全取决于私钥。对网络环境中来访者依据身份层次进行划分，多层次涉及安全等级，再依据安全等级设置结果从而实现对信息安全的分级控制。

在基于云计算的网络访问控制方法中，信息安全控制是后续的研究方向。

(4)权限分配过程

在基于云计算的网络访问控制方法中，用户的访问请求由数据存储委托方和云计算平台的供应商共同处理。提供云计算平台的供应商的身份权限分配策略，依据多层次身份管理，从而获得多层次权限管理，不再拥有超级权限。委托存储的数据在云计算平台分级，在信息安全管理方面也采用多层次级别管理。数据存储委托方只负责最高保密级别数据访问请求的监管，提供运算及平台的供应商负责监控网络中来访者对数据保密性较低数据的访问请求。这样既保证数据安全的可控性，又减少了访问管理工作。

本文方法中的相关定义如下：

云服务器名为FS，用户Vi访问用户V_j拥有的客体K_j。

V_i向FS发送访问请求Access。

FS查找K_j权限列表，若权限列表中有此次K_j的访问授权，则验证V_i，并返回授权证书或拒绝，V_i向客体K_j发起访问请求；若客体权限列表中没有该客体的访问授权，就把Access转发给V_j。

V_j验证V_i，V_i验证V_j，依据双方验证结果，选择是否授权。若不授权，向V_i发送reject；若授权，V_j向基于云计算的网络访问控制方法组件申请创建作业，基于云计算的网络访问控制方法组件返回授权证书。

V_j向V_i发送证书。

V_i向客体K_j发起访问请求。

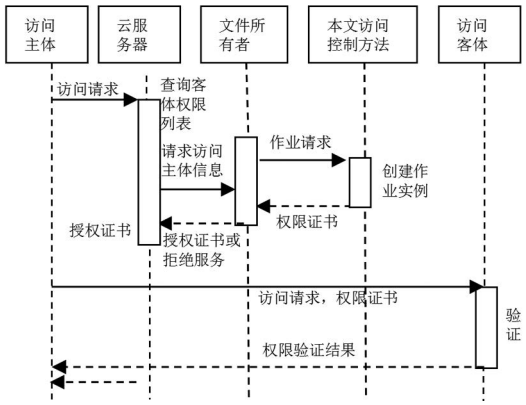

图3 访问授权过程

Fig.3 Access authorization process

7 结论(Conclusion)

本文仿真实验环境为Windows NT 2003，Inter(R) Pentium(R) CPU 2.6GHz，内存2.0GB，采用Macromedia公司的Dreamweaver MX作为程序开发平台，ASP.net为脚本语言，利用SQL Server为后台数据库，按照本文提出的基于云计算的网络访问控制方法开发了一套企业管理信息系统。该系统应用与云计算网络环境后有效地提高了各种用户访问控制的安全性、灵活性。结果表明，该方法是有效的。

本文从云计算环境入手，分析了中国墙访问控制模型和RBAC96模型的优缺点。这些访问控制模型对于云计算环境下的数据存储存在一些潜在的可不忽略的安全问题。本文提出的基于云计算的网络访问控制安全方法是分别从用户角度和数据角度分析了网络访问控制方法中各类身份的访问控制需求，模型中的基本要素是身份，有了不同的身份才可能有响应的任务，通过多层次身份的定义，划分出对应的多层次的任务，不同的任务才会被分配到响应级别的权限，同一个客户在不同的场景下访问时，可能由于身份不同而获得不用的权限，从而使得权限与客户分开，实现了强制访问控制，增强了安全性。本文还分析了基于云计算的网络访问控制安全方法对于云计算平台环境下的适用性，同时构建了一个面向共享安全的访问控制机制，从用户身份类别、作业分解类别、信息安全控制、权限分配管理四个方面分析了安全需求。但是基于云计算的网络访问控制安全方法也有它不足的地方，云计算环境下，数据存储除了网络访问控制，还有其他问题，比如在信任管理方面，还有待于进一步的研究，这也是下一步研究工作的方向。

参考文献(References)

[1] MELL P,GRANCE T,NIST SD.The NIST Definition of Cloud Computing[S].Gaithersburg,MD:NIST Special Publication,2016(3):193−202.

[2] FENG D G,et al.Study on cloud computing security[J].Journal of Software,2015,22(1):71−83.

[3] ZHOU Yu.Data Mining−Based Maintenance Management Framework of Multi−Component System[J].Journal of Donghua University(English Edition),2015,32(6):950−953.

[4] LIANG B,et al.An Improved Method to Enforce BLP Model and Its Variations in Role−Based Access Control[J].Journal of Computer,2014,15(5):636−644.

[5] 冯登国,等.云计算安全研究[J].软件学报,2014,22(1):71−83.

[6] 陈全,邓倩妮.云计算及其相关技术[J].计算机应用,2013,29(9):2562−2566.

[7] 陈丹伟,黄秀丽,任勋益.云计算及安全分析[J].计算机应用研究,2015,22(6):9−11.

[8] 邓集波,洪帆.基于任务的访问控制模型[J].软件学报,2013,14(1):76−81.

[9] 韩若飞,汪厚祥.基于任务−角色的访问控制模型研究[J].计算机工程与设计,2012,28(4):800−807.

[10] 李孟珂,余祥宣.基于角色的访问控制技术及应用[J].计算机应用研究,2010,17(10):44−47.

[11] 王小威,赵一鸣.一种基于任务角色的云计算访问控制模型[J].计算机工程,2012,38(24):9−13.

作者简介：

杨　波(1978−)，女，硕士，副教授.研究领域：网络安全，信息安全.

张　云(1981−)，女，硕士，副教授.研究领域：大数据，云计算.

王　欣(1982−)，女，硕士，讲师.研究领域：云计算，图像处理.