基于行为的云计算访问控制安全模型

林果园[1,2,3]，**贺珊**[1]，**黄皓**[2]，**吴吉义**[3]，**陈伟**[1]

（1.中国矿业大学 计算机学院，江苏 徐州 221116；2. 南京大学 计算机系，江苏 南京 210093；
3. 杭州师范大学 杭州市电子商务与信息安全重点实验室，浙江 杭州 310036）

摘 要：针对当前流行的云计算技术，分析了其所面临的安全问题。以 BLP（Bell-LaPadula）模型和 Biba 模型为参考，通过基于行为的访问控制技术来动态调节主体的访问范围，实现 BLP 模型和 Biba 模型的有机结合，提出了 CCACSM（cloud computing access control security model）。该模型不仅能保护云端服务器中数据完整性和保密性，而且使云计算环境具有相当的灵活性和实用性。最后给出了该模型的组成部分、安全公理和实现过程。

关键词：云计算；BLP 模型；Biba 模型；基于行为的访问控制

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)03-0059-08

Access control security model based on behavior in cloud computing environment

LIN Guo-yuan[1,2,3], HE Shan[1], HUANG Hao[2], WU Ji-yi[3], CHEN Wei[1]

(1. School of Computer, China University of Mining and Technology, Xuzhou 221116, China;
2. Department of Computer, Nanjing University, Nanjing 210093, China;
3. Hangzhou Normal University, Key Lab of E-Business and Information Security, Hangzhou 310036, China)

Abstract: In view of the current popular cloud computing technology, some security problems were analyzed. Based on BLP(Bell-LaPadula) model and Biba model, using the access control technology based on behavior to dynamic adjusting scope of subject's visit, it put forward the CCACSM (cloud omputing access control security model). The model not only guarantees the cloud computing environment information privacy and integrity, and makes cloud computing environment with considerable flexibility and practical. At last, it gives the model's part, safety justice and realization process.

Key words: cloud computing; BLP model; Biba model; access control based on behavior

1 引言

云计算是一种新兴的计算模式，它是一种分布式计算，是在网格计算的基础上发展而来的[1]，它体现了“网络就是计算机”的思想，将网络大量计算资源、存储资源与软件资源链接在一起，形成巨大规模的共享虚拟资源池，为远程计算机用户提供服务。

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]。在云计算环境中，数据存储方式打破传统模式，所有数据以托管的方式存储在云端服务器中，用户只需利用云服务商提供的 API（应用程序编程接口），通过浏览器就可以随时随地获取所需要的数据和服务。服务

收稿日期：2011-07-10；**修回日期**：2012-01-10

基金项目：国家自然科学基金资助项目(51104157)；中国博士后科学基金资助项目(20100481181)；教育部博士学科点专项科研基金资助项目(20110095120008)

Foundation Items: The National Natural Science Foundation of China (51104157); The China Postdoctoral Science Foundation (20100481181); The Ph.D. Programs Foundation of Ministry of Education of China (20110095120008)

模式的改变也带来了诸多云计算信息系统的安全问题，例如开放的接口为非法访问提供了可能，非法用户会进入信息系统窃取企业和用户机密数据，因此数据完整性和保密性受到巨大威胁。

目前，云计算安全所面临的3大安全问题主要体现在身份与权限控制、Web安全防护和虚拟化安全方面等。在云计算时代，安全设备和安全措施的部署位置有所不同，安全责任的主体发生了变化。目前，常用的解决云计算安全问题的办法主要有数据备份、建立企业私有云、数据加密后放到云端保存，但这并不能从根本上解决云计算所面临的安全问题。云计算已成为一种崭新的服务模式，针对云端服务器中数据完整性和保密性的问题，需要符合自身特点的安全模型。

2 相关研究

围绕远端用户对云资源进行访问时，如何保证数据的完整性和保密性展开研究是目前云计算安全研究的一个重要方向[2]。

有些学者结合云计算的特点提出了相应的访问控制方法，但是没有综合考虑数据的完整性和保密性。文献[3]认为API是云服务提供者和使用者之间的桥梁，云计算的安全很大程度上依赖API的安全，提出了云计算环境下API层面的一种基于RBAC的两阶段访问控制机制。但是该访问机制只允许白名单中的用户进行访问，与云计算的开放性不相符。Li等人[4]提出了适于SaaS系统的S-RBAC访问控制模型，解决了SaaS系统中的一些访问控制问题，但是对于一些权限许可缺少时间约束。文献[5]在分析云计算环境的特点和安全现状的基础上，介绍了一种安全访问控制服务（SACS, security access control service）的概念，基于SACS提出了一种层次化的云安全模型，但是描述过于简化，没有指出如何保证完整性或者保密性。

20世纪70年代，保护数据完整性或保密性的安全模型被提出。BLP模型是由El-liott Bell和Leonard J La Padula于1973年创立的一种模拟符合军事安全策略的计算机操作的模型[6,7]。在BLP模型中允许下读、上写2个安全特性，这2个特性保证了信息的单向流动，即信息只能向高安全属性的方向流动，BLP模型就是通过信息的单向流动来防止信息的扩散，抵御特洛伊木马对系统机密信息的攻击。BLP模型的不足[8]之处在于对完整性控制不够。可能出现的情况是，已授权的用户对数据进行非法的修改。BLP模型通过提供保证数据保密性的安全策略来保证系统的安全，但它不能有力地保证数据的完整性。因此，20世纪70年代，Ken Biba等人提出了Biba访问控制模型[9]，该模型对数据提供了分级别的完整性保证，类似于BLP保密性模型，Biba模型也使用强制访问控制系统。Biba模型是和BLP模型相对立的模型，Biba模型改正了被BLP模型所忽略的信息完整性问题，但在一定程度上却忽视了保密性。

针对传统安全模型中完整性与保密性相冲突的问题，有些学者提出了相应的解决方案，但是没有深入云计算环境的特点进行展开。李益发[10]提出将BLP模型和Biba模型结合建立操作系统安全模型。由于该模型基于一个特殊可信主体，使得其实用性受到限制。周正等人[11]提出了兼顾保密性与完整性的安全策略，并且为避免通过交互访问操作以及多角色主客体存在造成的泄密与完整性破坏事件提供了理论基础。但没有解释在具体信息系统环境中如何对主客体密级以及安全级进行合理确定。文献[12]针对Sandhu等人提出模型的基础上，引入了辅助角色层次，加强了角色间关系并提供了对可信主体概念的支持，在RBAC中实施了经典的BLP模型及其变种模型。但该文献仅停留在理论证明层面，如何在商业系统中以较小的代价引入强制访问控制并没有详细论述。李凤华等[13]结合角色、时态和环境的概念，给出了行为的定义。然后介绍了行为、时态状态和环境状态的层次结构，提出了基于行为的访问控制(ABAC, action based access control)模型。与已有其他模型相比，ABAC模型更加适用于解决网络环境下支持移动计算的信息系统中的访问控制问题。

本文吸收这些文献的技术成果，以BLP模型和Biba模型为基础，借鉴有关行为定义的思想，结合云计算环境的特点，用行为综合角色、时态和环境状态的相关安全信息，通过基于行为的访问控制技术将BLP和Biba模型相结合，并做了一定的取舍与扩充，提出了CCACSM。通过该模型，力求解决云计算环境下的完整性与保密性的问题。

3 CCACSM

将BLP模型与Biba模型通过访问控制有机结

合，各取其优点，提出了一种保护云端服务器中数据的保密性和完整性的云计算访问控制安全模型(CCACSM, cloud computing access control security model)。该模型主要继承了 BLP 模型的简单安全属性和*属性公理，以此加强了数据的保密性，并且结合了 Biba 模型的严格完整性策略，以此保证了数据的完整性。

3.1　CCACSM 的组成部分

CCACSM 需要刻画用户、服务器及其访问权限和行为所处的时态和环境等，有多个元素、相应关系和规则构成。

1) 元素

为了方便模型的形式化描述，将模型中涉及到的元素进行了数学形式的定义，如表 1 所示。

模型中的环境即用户访问系统时的客观因素，例如平台（硬件平台、软件平台等）、位置（场所物理位置、网络位置等），还有其他与访问控制相关的外部客观信息等。云计算系统可以使用与安全相关的环境信息来限制对系统资源的访问。环境状态对云用户在何种外部客观因素下的权限进行约束，将环境状态的集合通常记为 E。

2) 时态、环境和行为的关系

定义 1　对于相同的环境状态，若 T_i、T_j 是 T 中的元素，角色 r 在时态 T_i 中得到的权限为 D_i 满足 $D_i \in D_j$，则称 T_i 为 T_j 的子时态状态，记为 $T_i \leqslant T_j$。

定义 2　对于相同的时态状态，若 E_i、E_j 是 E 中的元素，角色 r 在环境 E_i 中得到的权限为 D_i 满足 $D_i \in D_j$，则称 E_i 为 E_j 的子环境状态，记为 $E_i \leqslant E_j$。

定义 3　将行为集合记为 A，行为层次结构 $AH \in A \times A$ 是行为集合 A 上的偏序关系。当且仅当 $T_i \leqslant T_j$、$E_i \leqslant E_j$、$D_i \leqslant D_j$ 同时成立，对于任意的 $A_i=\{D_i,T_i,E_i\}$，$A_j=\{D_j,T_j,E_j\} \in A$，$(A_i,A_j) \in AH$。如果 $(A_i,A_j) \in AH$ 成立，则称 A_i 是 A_j 的低级行为，A_j 是 A_i 的高级行为。

3) 状态转换规则

状态转换规则主要是用来保证系统的每一个状态都是安全状态。除了保证初始状态是安全的，还要保证系统的每一次转换都从一个安全状态转移到另一个安全状态。在 CCACSM 中的状态转换主要包括以下 5 个规则。

规则 1　get-read 规则，用于云用户集合对云端服务器集合请求只读访问。

当云用户 S_i 可以对云端服务器 O_j 进行只读访问时，需满足以下条件：

1) S_i 的行为集合中有对 O_j 的只读权限；

2) S_i 的安全等级支配 O_j 的安全等级；

3) S_i 是可信云用户或云用户的当前安全等级与云端服务器 O_j 的安全等级相同。

规则 2　get-execute 规则，用于云用户对云端服务器请求执行访问。

当云用户 S_i 可以对云端服务器 O_j 进行执行访问时，需满足：S_i 的行为集合中有对 O_j 的执行权限，要完成执行操作还必须有读写权限。

规则 3　get-append 规则，用于云用户对云端服务器请求读写访问。

当云用户 S_i 可以对云端服务器 O_j 进行读写访问时，需满足以下条件：

1) S_i 的行为集合中有对 O_j 的读写权限；

2) S_i 的安全等级支配 O_j 的安全等级；

3) S_i 是可信云用户或云用户当前的安全等级支配 O_j 的安全等级。

规则 4　change-subject-current-security-level 规则，用于云用户请求改变当前的安全等级。

当 S_i 可以改变其当前 O_j 的安全等级至 f_o 时，需满足以下条件。

1) S_i 是可信云用户或它的安全等级被改变为 f_o

表 1　**CCACSM 的组成元素**

元素集	元素及其含义	说明
S	$\{S_1, S_2, \cdots, S_n\}$, S_i 表示云计算环境中的某个用户	云用户集合
O	$\{0_1, 0_2, \cdots, 0_n\}$, O_i 表示云计算环境中的某个服务器	云端服务器集合
D	r 表示读权限，w 表示写权限，a 表示读/写权限，e 表示执行权限（即不能查看也不能修改）[注]	访问权限
F	$F=\{f, f'\}$, f_c 为云用户的安全等级；f 为云用户的当前安全等级；f'为云用户的最高安全等级	安全等级集合
$type$	$Type(o, s)$ 表示云用户 s 与云端服务器 o 的对应关系	s 对 o 的访问权限函数
T	$\{T_1, T_2, \cdots, T_n\}$, T_i 表示某个行为的时态	时态状态
E	$\{E_1, E_2, \cdots, E_n\}$, E_i 表示某个行为的环境	环境状态
A	$A=\{D,T,E\}$，　D、T、E 这 3 个要素构成行为	行为集合

注：为防止低密级用户篡改信息读权限要大于或等于写权限

并且导致的状态满足*属性；

2) S_i 的安全等级支配 f_o。

规则 5 resolve-conflict 规则，用于云端数据的机密性与完整性产生冲突时的处理机制。

当云用户 S_i 可以对云端服务器 O_j 进行访问，机密性与完整性发生冲突时，需满足以下条件：

S_i 的行为集合中有对 O_j 的 A_i 权限，O_j 的行为集合中包括 A_j 权限；

当且仅当$(A_i,A_j) \in AH$ 时，即 A_j 是 A_i 的高级行为时，满足简单安全属性和*属性公理；

当且仅当$(A_j ,A_i) \in AH$ 时，即 A_i 是 A_j 的高级行为时，满足严格完整性策略。

CCACSM 侧重于更强的完整性和保密性同时满足，如图 1 所示，其访问控制分为 2 个层次。

1) 权限层次：访问规则——允许同级别的云用户对云端服务器数据有只读权限，高级别云用户对低级别云端服务器数据有所有权限，低级别云用户对高于自己级别的云端服务器数据只具有最小权限（即只可以读取云端服务器中的部分共享的数据）。

2) 行为层次：行为层次包括时态层和环境层，行为的状态随着角色、时态和环境的不同而动态变化，其中，环境状态和时态状态对角色所能享有的权限具有直接影响，如不同的物理位置、网络位置、软件平台等外部环境可以对角色产生影响，同时不同的时态状态如事件发生的起始时间、终止时间、持续时间等也会对角色产生影响。

3.2 CCACSM 的安全定理

定理 1 CCACSM 满足经典 BLP 模型的简单安全属性和*属性公理。

证明 假设$\leqslant_{BLP}$和$\geqslant_{BLP}$都表示偏序关系，L_w 为相应于$\geqslant_{BLP}$的最低安全等级的写权限，f_o 对应 o 的当前安全等级，T 对应云用户 S 的时态，E 对应 S 所处的环境。

1) 对于非可信云用户 S

$\forall o \in O$, $x = F(o)$;

$\forall s \in S$, 令 s 的读权限集为 D_{rs}，写权限集为 D_{ws}，行为集为 A_s；

设 s 具有的访问权限为f'_e、f_r和f_w，即$D(s) = \{f'_e, f_r, f_w\}$，$A_s = \{D(s),T,E\}$，那么有：

$A_{rs} = \{ (o, r) \mid \exists f_o r \leqslant f r [((o, r) , f_o r) \in D]\}$；

$A_{ws} = \{ (o, w) \mid \exists f_o w \leqslant f_w [((o, w) , f_o w) \in D]\}$，

又因为每个云端服务器 o 的访问权限被精确地分配给了角色 $F(x)_r$ 和 $F(x)_w$，即：

即 $D=\{((o, r), f'(o)_r),((o, w), f'(o)_w)\}$；$A=\{D, T,E\}$。

推理得：$A_{rs}=\{ (o, r) \mid \exists f_o r \leqslant f_r [f_o = f'(o)]\}$

$= \{ (o, r) \mid f'(o)_r \leqslant f_r\}$

$= \{ (o, r) \mid f'(o) \leqslant_{BLP} f\}$；

$A_{ws} = \{ (o, w) \mid \exists f_o w \leqslant f_w [f_o = f'(o)]\}$

$= \{ (o, w) \mid f(o)_w \leqslant f_w\}$

$= \{ (o, w) \mid f'(o) \geqslant_{BLP} f\}$。

若 s 能读访问 o,即$(o, r) \in Drs$，必有 $f'(o) \leqslant_{BLP} f = f(s)$，即满足*属性。

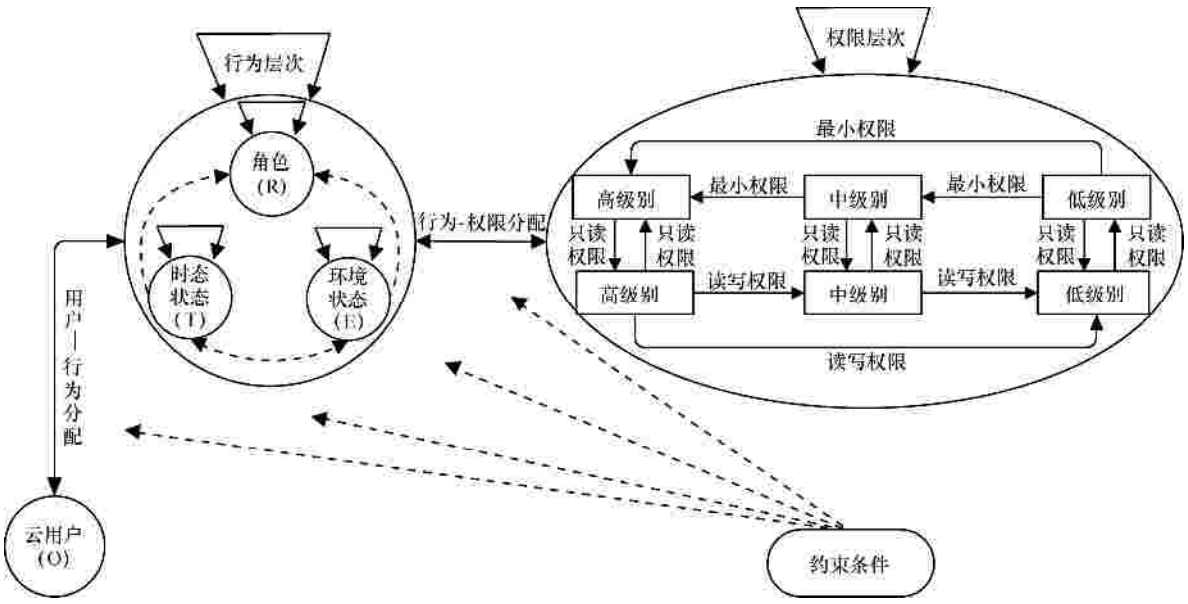

图 1 CCACSM 的访问控制规则

又因为 $f \leqslant BLP\ f' = f'(s)$，所以 $f'(o) \leqslant BLP\ f'(s)$，即满足简单安全属性。

若 s 能写访问 o，即 $(o, w) \in A_{ws}$，必有 $f'(o) \geqslant BLPf = f(s)$，即满足*属性。

又因为简单安全属性并不约束只写操作，所以也满足简单安全属性。

2) 对于可信云用户 S'

$\forall o \in O, x = F(o)$，$\forall\ s \in S'$，令 s 的读权限集为 D_{rs}，写权限集为 D_{ws}，行为集为 A_s。

设 s 具有的权限为 f'_e，f_r 和 L_w，即 $F(s) = \{f'_e, f_r, L_w\}$，与上同理，有 $Ars = \{(o, r) \mid f'(o) \leqslant BLP\ f\}$，$Aws = \{(o, w) \mid f'(o) \geqslant BLP\ f\}$。

若 s 能读访问 o，即 $(o,r) \in D_{rs}$，必有 $f'(o) \leqslant BLP\ f = f(s)$。又因为 $f \leqslant BLP\ f' = f'(s)$，所以 $f'(o) \leqslant BLP\ f'(s)$，满足简单安全属性。

对于可信云用户，*属性对其访问无任何约束，自然被满足。

综上所述，CCACSM 模型保证了系统的保密性。　　证毕。

定理 2　CCACSM 满足 Biba 模型的严格完整性策略。

严格完整性策略主要防止信息从低完整性级别客体向高完整性级别客体传递，即对于任意的云用户 s，若 $(D_{rs}, T_{o1}, E) \in A$，$(D_{Ws}, T_{o2}, E) \in A$，则有 $f_{o1} \leqslant f_{o2}$。

证明　假设 L 为完整性标识，L_r 为完整性标识范围，$D_{xs} = \{D_{x1s}, D_{x2s}, \cdots, D_{xns}\}$ 为云用户 s 对云端服务器 o 的访问权限集合并且 $D_{x1s} < D_{x2s} \cdots < D_{xns}$（表示访问权限依次增大）。

假设当前的 A 集合存在访问权限 $A_r = (D_{rs}, T_{o1}, E)$，$A_{x1s} = (D_{x1s}, T_{o2}, E)$，$A_{x2s} = (D_{x2s}, T_{o3}, E)$ … $A_{xns} = (D_{xns}, T_{on}, E)$

设 o 没有经过 A 访问之前的完整性标识范围为 $L_r^{\,x}$，经过 A 访问后变为 $L_r^{\,x+1}$，有：

经过 A_r 访问后变为 $L_r^{\,r+1}$，经过 A_{x1s} 访问后变为 $L_r^{\,x1+1}$，经过 A_{x2s} 访问后变为 $L_r^{\,x2+1} \cdots$ 经过 A_{xns} 访问后变为 $L_r^{\,xn+1}$，又因为 $D_{x1s} < D_{x2s} \cdots < D_{xns} \Rightarrow L_r^{\,r+1} \subseteq L_r^{\,x1+1} \subseteq L_r^{\,x2+1} \subseteq \cdots L_r^{\,xn+1}$。

所以 $L_r^{\,r+1} \subseteq L_r^{\,x1+1} \subseteq L_r^{\,x2+1} \subseteq \cdots L_r^{\,xn+1} \Rightarrow f_{o1} < f_{o2} < f_{o3} < \cdots < f_{on}$。

综上所述，CCACSM 满足 Biba 模型的严格完整性策略。　　证毕。

CCACSM 中，简单安全属性要求对模型的所有云用户都成立，是为了防止云用户写入安全等级比其当前安全级别高的云端服务器中的信息，并且防止云用户直接从不允许其存取的级别的云端服务器中存取信息。而*属性公理仅要求对非可信云用户成立，此属性防止了云用户有意或无意地把高密级信息写入低密级云端服务器中，从而造成秘密的泄露。定理 2 防止了信息从低级别向高级别云端服务器中传递，保证了信息的完整性。

3.3　CCACSM 的实现过程

假设在该模型中系统管理员为系统定义 k 个安全等级（1,2,3,…,k），安全等级由高向低排列，其中 1 代表最高安全等级，k 代表最低安全等级。系统中云端服务器 o 拥有其中某一个安全等级 $f(o)$ $(1 \leqslant f(o) \leqslant k)$，把云用户 s 划分为几个类型 z，每个云用户属于一种类型，假设每个类型对应某个安全等级 $f(z)(1 \leqslant f(z) \leqslant k)$，则属于该类型的某云用户 s 的安全等级 $f(s) = f(z)$。任务 T' 与云用户 s 之间形成一一对应关系。假设某任务 T' 对应某云用户 s，云用户 s 的安全等级 $f(s) = n$，$1 \leqslant n \leqslant k$，把任务划分为子任务 $T'(i)$ 以后，$T' = \{T'(i), 1 \leqslant i \leqslant n$ 且 $n \geqslant 1\}$，完成该任务 T' 的云端服务器集合 $O = \{O_i, 1 \leqslant i \leqslant n$ 且 $n \geqslant 1\}$，某云端服务器的安全等级为 $f(O_i)$，则可用如表 2 所示的 $\boldsymbol{M}$ 矩阵表示当 o 对 s 的行为是 A 时，$f(s)$ 和 $f(O_i)$ 之间应有的关系。

表 2　　***M* 矩阵**

行为	O				
	O_1	O_2	O_3	…	O_n
R	$\leqslant n$				
W		$\geqslant n$			$\geqslant n$
A			$=n$	…	
E					$\leqslant n$

该模型的总体架构如图 2 所示，其基本实现过程由以下几个步骤组成。

1) 第一次访问云端服务器的云用户需进行以下几个步骤。

Step1　每个申请访问云端服务器的云用户 S_i 都要进行用户注册。

Step2　用户注册完毕后要进行系统认证。

Step3　没有通过认证的用户被强制退出；通过认证的云用户，系统要再次对其进行行为的判断，判断此云用户的时态 T 以及所处环境 E。环境可以分为内部网络 $E1$ 和外部网络 $E2$；时态 T 可以分为

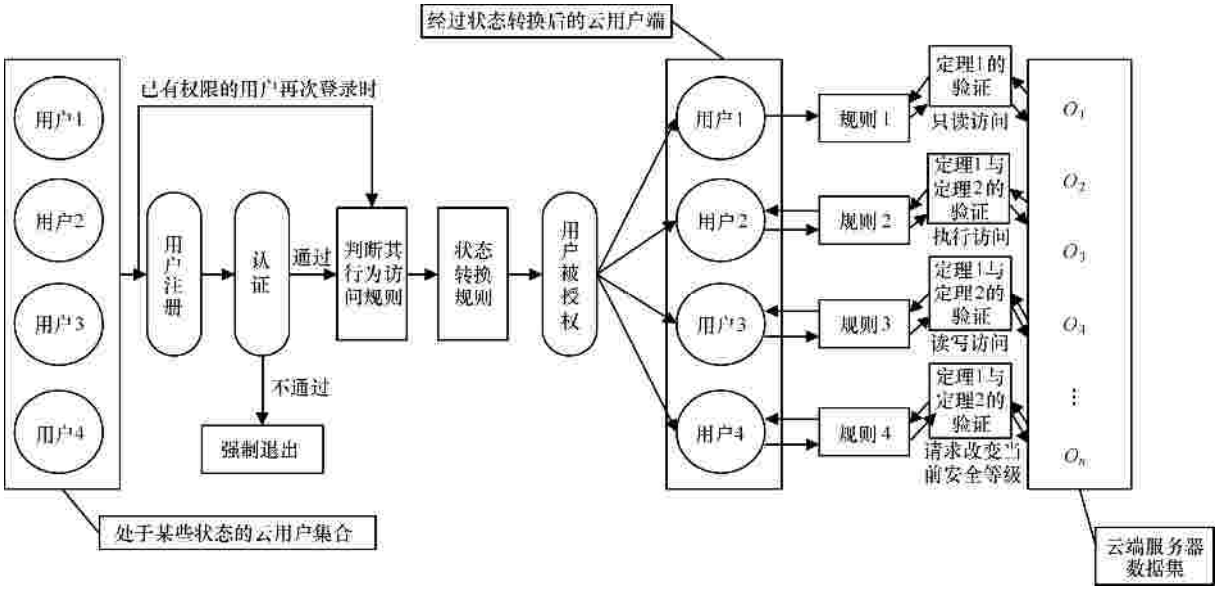

图 2　CCACSM 完整性和保密性规则模型

工作时间 *T*1 和休息时间 *T*2。此时，系统根据 *E*-*T* 的不同对云用户分配相应的权限行为 *A*。

Step4　判断完云用户的行为访问规则后，要进行相应状态转换。

Step5　经过状态转换后的云用户被授权，即被赋予相应的权限，即 *A*= *type*(*o*, *s*)。例如，用户 1 的行为状态为 *E*1- *T*2，那么它对云端服务器的数据集具有规则 1 的只读权限 *A*=*get-read*(*o*, *s*)；用户 2 的行为状态为 *E*2- *T*2，那么它对云端服务器的数据集具有规则 2 的执行权限 *A*=get-execute(*o*,*s*)；用户 3 的行为状态为 *E*1- *T*1，那么它对云端服务器的数据集具有规则 3 的读写权限 *A*=get-append(*o*,*s*)；用户 4 的行为状态为 *E*2- *T*1，那么它对云端服务器的数据集具有规则 4 的请求改变当前的安全等级的权限 *A*=*change- subject- current- security- level*(*o*, *s*)。其中，所有的云用户在进行云端服务器数据集访问之前都要经过定理 1 简单安全属性与*属性的验证，这一步保证了数据的保密性；而被赋予规则 2、规则 3 和规则 4 的云用户在进行云端服务器数据集访问之前都要经过定理 2 完整性验证，这一步确保了数据的完整性。

Step6　云端服务器的数据都要经过完整性验证返回给云用户。

2) 已经注册的云用户再次登录系统时，直接跳过上述步骤的 Step1 与 Step2 进行行为的判断与状态转换等。

3.4　在云计算环境中应用 CCACSM

Hadoop 是 Apache 软件基金会组织下的一个开源项目，提供了分布式计算环境下的可靠和可扩展软件。基于 Hadoop 框架的 Distributed File System 和 Map/Reduce Engine 子系统，本文构建了一个云计算实验平台，在此平台下对 CCACSM 进行了应用。该平台以校园网络中的用户使用环境为背景，假设云用户访问某学校服务器端的数据信息，云用户所处的环境 *E* 可以分为学校内部网络 *E*1 和学校外部网络 *E*2；时态 *T* 可以分为上班时间 *T*1 和下班时间 *T*2，以 2 种访问行为（*E*2- *T*1，*E*1- *T*1）为例进行说明。

1) 云用户 *s* 请求云服务

2) 系统对 *s* 进行用户注册与认证

3) 此云用户合法执行以下程序，不合法则直接强制退出请求系统

4)　判断云用户的访问行为 *A*

5) If(*s*∈*S*)

6) {　　If(*s* 是可信云用户)

7)　{　　If *A*=*E*2- *T*1

8)　　{　　If (*F*(*s*)>*F*(*o*))

//表示 *s* 的安全等级支配 *o* 的安全等级

9)　　{　　If(*o*(*r*)∈*A*(*s*))

//表示 *s* 的访问行为中有对 *o* 的只读权限

10)　　{ *A* = { (*o*, *r*) |∃*for*≤*fr* [((*o*, *r*) *for*) ∈*D*]}　//系统对云用户 *s* 进行状态转换

11)　　*type*(*o*,*s*)=*A*(*r*), *A*=*get- read*(*o*,*s*)

//表示系统为 *s* 分配读权限

12)　　此时执行 *get-read* 规则

并且进行定理 1 的验证，云用户可以在学校云端观看电影，图片等

//保证了云端服务器信息的保密性}

13) }

14) }

15) }

16) }

17) If $A=E1-T1$ and $(o(r,v) \in A(s))$

//s 的访问行为中有对 o 的读写权限

18) $\{A=\{(o, r) \mid \exists for \leqslant fr[((o, r), for) \in D]\}, A=\{(o, w) \mid \exists fow \leqslant fw[((o, w), fow) \in D]\}$,

19) 系统对云用户 s 进行状态转换，$type(o, s)=A(r, w)$, $A=get\text{-}append(o, s)$ //系统为 s 分配读写权限

20) 此时执行 *get-append* 规则并且进行定理 1 与定理 2 的验证，该云用户可以下载、修改或读取云端的文件等

//保证了云端服务器信息的保密性与完整性 }

21) If$(o(e))$ // 表示 s 的访问行为中有对 o 的执行权限

22) { 系统对云用户 s 进行状态转换,$type(o,s)=A(e)$, $A=get\text{-}execute(o,s)$ //系统为 s 分配执行权限

23) 此时执行 *get-execute* 规则并且进行定理 1 与定理 2 的验证，该云用户可以在云端浏览游戏

//保证了云端服务器信息的保密性与完整性}

24) }

25) }

26) Else s 是非可信用户

27) {

28) If(该云用户满足*属性)

29) {

30) If$(A=E1-T1$ and $F(s)>F(o))$ //表示 s 的安全级别高于 o

31) { $A=get\text{-}execute(o,s)$

32) 系统对云用户 s 进行状态转换，执行 *get-append* 规则并且进行定理 1 与定理 2 的验证，该云用户可以读、写云端信息 //保证了云端服务器信息的保密性与完整性}

33) else if$(A=E2-T1$ and $F(s)=F(o))$ //s 的安全级别等于 o

34) {

35) 系统对云用户 s 进行状态转换，并执行 *get-read* 规则并且进行定理 1 与定理 2 的验证，该云用户只可以读取云端的文件等

//保证了云端服务器信息的保密性与完整性}

36) }

37) }

从以上分析中可以看出：当 s 是可信云用户，且 s 对 o 有读访问权限，即$(o, r) \in D_{rs}$，必有 $f'(o) \leqslant BLP\ f=f(s)$，又因为 $f \leqslant BLP\ f'=f'(s)$，所以 $f'(o) \leqslant BLP\ f'(s)$，满足简单安全属性；对于可信云用户，*属性是自然被满足的。

当 s 是非可信云用户，且 s 对 o 有读访问权限，即$(o, r) \in Drs$，必有 $f'(o) \leqslant BLP\ f=f(s)$，即满足*属性，又因为 $f \leqslant BLP\ f'=f'(s)$，所以 $f'(o) \leqslant BLP\ f'(s)$，即满足简单安全属性。

当 s 是非可信云用户，且 s 对 o 有写访问权限，即$(o, w) \in A_{ws}$，必有 $f'(o) \geqslant BLPf=f(s)$，即满足*属性，又因为简单安全属性并不约束只写操作，所以也满足简单安全属性。

4 结束语

云计算的安全问题是云计算中的核心问题之一。本文结合云计算时代所面临的安全问题，提出了 CCACSM，并阐述了该模型的组成部分、安全定理以及典型的实现过程。该模型的优点在于其不仅继承了 BLP 模型严格保密性的特点，而且具备了 Biba 模型保证数据完整性的特点。为了适应云计算用户位置可变性这一特点，模型还引进了基于行为的访问控制技术。针对 CCACSM 的进一步研究主要是改进该模型的“下读，上写”特性，提高系统的可用性。

参考文献：

[1] MILLER M. Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online[M]. Que Print Publication, 2008.

[2] 冯登国, 张敏, 张妍等. 云计算安全研究[J]. 软件学报. 2011, 22(1), 71-83.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011 22(1):71-83.

[3] SIRISHA A, GEETHAKUMARI G. API access control in cloud using the role based access control model[A]. Trendz in Information Sciences and Computing-TISC2010[C]. 2010.

[4] LI D, LIU C, WEI Q, *et al*. RBAC-Based access control for SaaS systems[A]. 2010 2nd International Conference on Information Engineering and Computer Science (ICIECS)[C]. 2010.

[5] XUE J, ZHANG J J. A brief survey on the security model of cloud computing[A]. 2010 Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES)[C]. 2010.

[6] Nat'l Computer Security Center. Trusted network interpretation of the trusted computer system evaluation criteria[A]. NCSC-TG2005[C]. 1987.

[7] BELL D E, LAPADULA L J. Secure Computer Systems: Mathematical Foundations[R]. The MITRE Corporation, Bedford, Massachussetts, 1973.

[8] LIN T, BELL Y, AXIOMS L. A "new" paradigm for an "old" model[A]. Proc 1992 ACM SIGSAC New Security Paradigms Workshop[C]. 1992.

[9] BIBA K J. Integrity Considerations for Secure Computer Systems[R] . Bedford: ESD-TR-76-732, 1977.

[10] 李益发, 沈昌祥. 一种新的操作系统安全模型[J]. 中国科学 E 辑(信息科学), 2006, 36(4): 347-356.
LI Y F, SHEN C X, A new operating system security model[J]. Science in China, Series E, Information Sciences. 2006, 36(4): 347-356

[11] 周正, 刘毅, 沈昌祥.一种新的保密性与完整性统一安全策略[J]. 计算机工程与应用, 2007, 43(34):1-2.
ZHOU Z, LIU Y, SHEN C X. New kind of secrecy/integrity union policy[J]. Computer Engineering and Applications, 2007, 43(34):1-2.

[12] 梁彬,孙玉芳,石文昌等. 一种改进的以基于角色的访问控制实施 BLP 模型及其变种的方法[J].计算机学报. 2004,15(5): 636-644.
LIANG B, SUN Y F, SHI W C, *et al*. An improved method to enforce BLP model and its variations in role-based access control[J]. Journal of Computer, 2004, 15(5): 636-644.

[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, 2008,3(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.

作者简介：

林果园（1975-），男，山东鱼台人，博士，中国矿业大学副教授，主要研究方向为信息安全。

贺珊（1986-），女，山东德州人，中国矿业大学研究生，主要研究方向为数据加密、信息安全。

黄皓（1957-），男，江苏南京人，南京大学教授、博士生导师，主要研究方向为网络安全。

吴吉义（1979-），男，浙江诸暨人，博士，杭州师范大学副教授，主要研究方向为电子服务及信息安全。

陈伟（1978-），男，江苏徐州人，博士，中国矿业大学副教授，主要研究方向为信息处理。