一种面向业务的动态访问控制模型

谭 韧[1] 殷肖川[1] 李晓辉[2] 卞洋洋[1]
(空军工程大学信息与导航学院 西安 710077)[1] (中国人民解放军94789部队 南京 210018)[2]

摘 要 针对基于角色的访问控制(RBAC)模型在业务处理流程中访问控制粒度过粗和无法动态调整授权等方面的问题,提出了一种面向业务的动态RBAC模型(BO-RBAC)。该模型参考基于任务的访问控制(TBAC)模型,引入了业务、业务步和授权步等概念,并形式化定义了模型的基本集合;同时将授权过程分为角色授权和授权步授权两部分,将业务执行视为随机过程,给出了基于马尔可夫链的动态授权方法;最后使用C++14对模型进行了实现。BO-RBAC模型结合了RBAC与TBAC的特点,具有访问控制粒度细、授权动态调整、满足安全规范等优点。

关键词 RBAC,TBAC,动态授权,访问控制,马尔可夫状态机
中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.08.025

Dynamic Business-oriented Access Control Model

TAN Ren[1] YIN Xiao-chuan[1] LI Xiao-hui[2] BIAN Yang-yang[1]
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)[1]
(China PLA 94789 Unit, Nanjing 210018, China)[2]

Abstract Aiming at the problems of rough-grained access control and unable to adjust authorization dynamically in business process of traditional role-based access control (RBAC) model, a business-oriented dynamic RBAC model (BO-RBAC) was proposed in this paper. Taking TBAC model as reference, business step and authorization step are introduced into this model and basic model set is defined formally. Meanwhile, the authorization process is divided into two parts, role authorization and step authorization, and the execution is regarded as random process which shows a Markov chain-based dynamic authorization method. Finally, the model is implemented with C++14 programming language. BO-RBAC model combines the features of RBAC and TBAC, which introduces such advantages of fine-grained access control, dynamically-adjusting authorization and satisfy security specifications.

Keywords RBAC, TBAC, Dynamic authorization, Access control, Markov state machine

1 引言

随着基于云计算的应用系统的不断发展,在云上执行的业务与日俱增,单独使用RBAC模型[1]和TBAC模型已无法满足云环境下的访问控制:RBAC不能有效进行动态授权调整且授权粒度过大,对于已经授权的用户角色发生危险操作时不能及时收回授权,存在安全隐患,且在云任务处理过程中需要频繁变换角色,使用该模型的复杂度过高[2];TBAC过于强调任务流的访问控制,而在基于云的系统中通常以用户作为访问控制主体,该模型不能有效地规定用户所持有的相应权限,难以直接应用于实践。因此,在RBAC和TBAC的基础上,本文重新定义了业务和授权步的概念与它们之间的绑定关系,提出了一种面向业务和用户角色的基于马尔可夫链的动态授权方法,建立了一种面向业务的动态访问控制模型,即BO-RBAC模型。本文描述了BO-RBAC的模型结构,并形式化地定义了该模型的相关集合和授权函数,给出了该模型实现的理论依据和授权算法,用C++14[3]对模型进行了实现,同时对模型进行了分析。

2 相关研究工作

RBAC模型是由NIST的Sandhu等人[4]提出的能够实现基于角色授权的访问控制模型,后来被改进为RBAC96模型[5],但是由于没有对角色授权分配、分布式处理等问题的有效解决方案,研究者对其进行了很多有意义的改进。熊厚仁等[6]针对RABC授权方面存在不安全因素的问题,研究提出了在RABC授权管理中应当遵循的安全准则。吴丽颖等[7]针对分布式处理环境下传统RBAC模型难以处理的问题,研究了在Web集群下运用RBAC进行授权管理的方案。Zhou等[8]针对RBAC角色信息泄露的问题,提出了匿名RBAC模型。蔡婷等[9]针对RBAC角色权限继承的困难,通过引入最小角色集明晰了角色与权限之间的关系,提出了MR-RBAC模型。邓集波等[10]从任务执行的角度出发,给出了TBAC模

到稿日期:2016-09-28 返修日期:2017-01-03 本文受国家自然科学基金(61402510),陕西省工业科技攻关项目(2016GY-087)资助。

谭 韧(1993-),男,硕士生,主要研究方向为网络信息安全,E-mail:bluewingtan@yeah.net;**殷肖川**(1961-),男,教授,硕士生导师,主要研究方向为网络信息安全;**李晓辉**(1979-),女,工程师,主要研究方向为网络与信息安全;**卞洋洋**(1992-),男,硕士生,主要研究方向为网络与信息安全。

型的基本概念和使用场景。Lapin[11]将任务执行表现作为指标，针对能完成同一任务但存在不同执行需求的执行体如何分配权限的问题，提出了满足一种最小权限分配原则的 D-TBAC 模型。施教芳等[12]通过考虑任务内部的子任务授权和关于任务与角色的联系，提出了一种扩展的 TBAC 模型。张庆萍[13]通过任务将 TBAC 与 RBAC 结合起来，提出了包括最小权限原则在内的安全控制原则，给出了基于任务和角色的 T-RBAC 模型，但没有详细说明任务如何将两者结合在一起，且没有给出动态授权方案。

综上，许多研究人员对这两种访问控制模型进行了不同方面的研究，并提出了多种扩展模型。随着人们对安全要求的不断提高，仍然需要深入扩展这两种访问控制模型。本文的目的是解决在具体业务条件下难以通过单一的角色授权方式实现访问控制的问题、在任务执行中的动态权限管理问题和基于业务的细粒度授权问题。我们研究并提出了面向业务的动态 RBAC 模型，给出了模型的形式化定义和基于马尔可夫链[14-15]的动态授权算法，并对模型进行了实现与分析。

3　面向业务的动态访问控制

BO-RBAC(Business Oriented RBAC)模型在面向业务的基础上对 RBAC 模型进行了扩展，修改了授权(Authorization)的定义，引入了业务、业务步、授权步以及它们之间的动态绑定关系。本模型包含用户(Users)、角色(Roles)、业务(Businesses)、业务步集(Business-Step set)、授权集(Authorizations)、授权步(Authorization-Step)、执行路径(Execute-Path)和马尔可夫状态机(Markov State Machine，MSM)等实体以及用户角色指派(User Assignment，UA)、角色授权指派(Authorization Assignment，AA)、业务拆分(Business Split，BS)、上下文监控(Context Monitor，CM)、动态控制(Dynamic Control，DC)、授权步执行(Authorization-Step Execution，EX)和授权与业务步绑定关系(Authorization and Business-Step Binding，ABB)等关系。角色的继承关系表示为角色等级(Role Hierarchy，RH)。模型的结构图如图 1 所示。

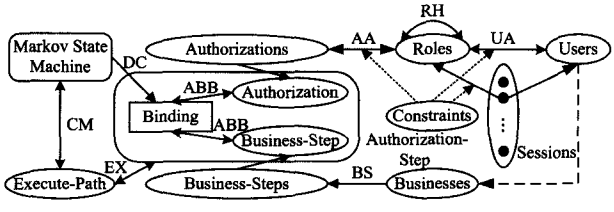

图 1　BO-RBAC 模型

在本模型中，用户想要访问某业务，需首先经过 UA，RH 和 AA 分配权限后，将业务进行细粒度划分操作 BS，将访问授权和业务步进行 ABB 处理。为了满足面向业务的动态访问授权，需要经过 CM 对业务步执行上下文进行监控，对 ABB 进行 DC 处理。相比以往的 RBAC 的静态授权方式，本模型充分考虑了业务执行的粒度和动态性，更适合在实际工作环境中进行访问控制。

3.1　BO-RBAC 核心概念

(1)业务。业务是一项需要处理的事务。它具有可区分性，可能与多个用户角色相关。例如程序开发业务，可能与项目经理、架构师和程序员等多个用户角色相关，多个角色共同参与完成某项业务。业务具体可拆分为多个业务步即 BS 过程，每一个业务步是组成业务的原子单位，即业务步只有两种执行状态，要么被完整执行，要么没有执行。业务步的跳转(Jump)指从某个业务步执行到另一个业务步的过程，在本模型中将其视为一个随机过程。同时，业务步之间的跳转过程是符合马尔可夫链的。

(2)角色授权。角色授权是指给予用户角色相应的权限，通常以业务步为粒度授予，角色拥有的对于业务的所有授权称为对某项业务的授权，即如果角色拥有某项业务中所有业务步的授权，则称角色拥有该业务的授权。这里的授权可看作是一种操作许可而不是操作执行，要执行业务步，必须通过授权步进行。某一角色的所有授权构成一个授权集，授权集中的授权是动态调整的，相关的限制条件可包括允许使用时间和授权使用次数等。若授权使用时间不在允许时间范围内或是使用次数超过限制，则授权将会从授权集中移除。

(3)授权步。授权步是进行访问控制的原子单位，同时也是业务步与角色授权的一种动态绑定关系。角色授权是一种操作许可，授权步则是一种执行许可。只有当业务步与该业务步的角色授权绑定即授权步建立时，才允许进入访问控制过程，业务步才有可能得到执行。当授权步初始化后，ABB 也随之建立。由于将业务步的跳转链视为马尔可夫链，因此前一授权步的访问控制状态会决定后一授权步的访问控制状态。与文献[10]所述授权步不同，本模型中将授权步的执行视作随机过程而非顺序过程。与角色授权类似，所有授权步构成授权步集。

(4)执行路径。执行路径是指某角色处理业务时业务步对应的授权步执行的相应顺序。在业务执行时，系统将其各业务步对应的授权步(如果存在)加入到执行路径的末尾，依次进行访问控制。由于业务步执行为随机过程，因此需要确定沿该执行路径的各授权步的风险状态。即使角色授权有效，执行路径中的授权步也不一定都能够顺利执行，这需要安全状态机对执行路径进行上下文分析判断。执行路径有两种状态：一种是正常态，即能够正常按照路径顺序执行；另一种是终止态，即按照路径执行存在风险，系统终止了执行路径，不允许再加入授权步。

(5)安全状态机。根据授权步执行上下文，动态输出当前状态的状态机。在本模型中，其被实现为马尔可夫状态机，存储各授权步转移概率矩阵(Transition Probability Matrix，TPM)和各状态概率阈值集(State Possibility Threshold，SPT)的状态转移概率计算部件。执行路径中的每一授权步对应的业务步在执行前，依据转移概率矩阵计算出该跳转可能的概率，通过与各状态概率阈值进行比对得出该授权步的访问控制状态。安全状态机与执行路径的设计体现了一种虚拟执行的思想，进一步增强了访问控制的动态性和可靠性。

用户、角色、角色授权指派及角色等级等概念与 RBAC96 模型相近。

3.2　BO-RBAC 访问控制

作为一种面向业务的动态访问模型，BO-RBAC 的授权方式结合了 RBAC 与 TBAC 各自的优点。在 BO-RBAC 中，授权分为两个部分：角色授权和授权步授权。

3.2.1　角色授权

角色授权以五元组(U,S,R,A,C)的形式来表示。其中，

U 表示用户，S 表示会话，R 表示角色集，A 表示授权集，C 表示会话与角色、角色与授权、用户与角色的限制关系。U 启动 S 后，分配一个或多个 R，每个 R 中有与其相对应的 A。而 C 则可能有以下几种。

(1)角色互斥。同一个 U 最多仅可以分配到互斥 R 中的一个。而在 A 进行分配时也有互斥的限制，互斥权限最多分配给一个 R，此时称为静态角色互斥；或是在角色分配时可以给 U 分配不同的 R，但在系统运行时最多只允许 U 扮演分配 R 中的一个，此时也称为运行时角色互斥。

(2)时数限制。在本模型中共存在 3 种限制：1)U 与 R 的映射个数限制，即同一个 U 所拥有的 R 的数量是有限的，对应地，一个 R 对应的 U 的个数也是有限的；2)授权集 A 中授权的使用次数限制，即 A 中的授权只可使用限定次数，当超过使用次数时授权自动从 A 中移除；3)R 或 A 的使用时间限制，即授予 R 和对应 A 中的授权可以规定使用时间段或是使用时长，如果超时，对于 R 则取消 U 对其的映射，对于 A 中的权限则自动移除。

(3)前提角色及前提授权。当且仅当 U 具有某角色 R_i 时才能分配另外的角色 R_j。相应地，当且仅当 R 具有某授权 A_i 时才能分配另外的授权 A_j。

而 R 自身还有层次关系，用 RH 关系表示，即 R 可能存在一定的继承关系。一个 R 中的 A 可分为两个子集，即允许子角色继承的授权集 A_H 和不允许子角色继承的授权集 A_{NH}。子角色可以继承父角色的 A_H 而不能继承 A_{NH} 中的授权。类比面向对象程序的设计思想，可将 A_{NH} 重构为一个新的角色，称其为当前角色 R 的私有角色。

以云平台开发为例，项目经理、产品工程师和质控工程师等 3 个角色都属于项目人员，而由于开发工作要求，产品工程师和质控工程师不能同时由一人担任，因此这两种角色属于互斥角色；而产品工程师又可以分为前端工程师和后端工程师，这体现了 RH 关系；与产品工程师和质控工程师的互斥类似，前后端编程与质量控制的授权是互斥的，而项目经理抓全盘的授权作为前提，可以有前后端编程和质量控制的授权。角色授权如图 2 所示。

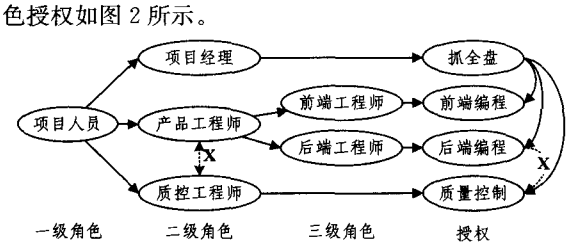

图 2 云平台开发授权示意图

3.2.2 授权步授权

授权步授权以四元组 (a, bs, ms, ABB) 的形式表示。其中，a 表示授权，bs 表示业务步，ms 表示马尔可夫状态，ABB 表示 a 与 bs 的绑定关系。当系统初始化时，通过 BS 过程将业务拆分为各业务步，授权步将 a 与 bs 绑定起来。这种绑定是动态的，在 ABB 关系存续期间，拥有 A 的角色实体可以对绑定的 bs 进行操作；当 ABB 解绑时便无法实施操作，这种动态过程是依靠 ms 来确定的。

ms 由马尔可夫状态机 MSM 通过对当前 bs 对应的授权步 as 的执行路径确定。通过对执行路径进行分析，依据 TPM 计算当前 as 在执行路径中的可能概率，并与 SPT 中的各阈值进行比较得出相应的 ms 状态。通常 SPT 中包含两个阈值，分别是拒绝阈值 spt_r 和警告阈值 spt_w，$0<spt_r<spt_w<1$。通过对当前执行路径概率值 p 与各阈值的比较来确定输出的 ms。MSM 的状态如图 3 所示。

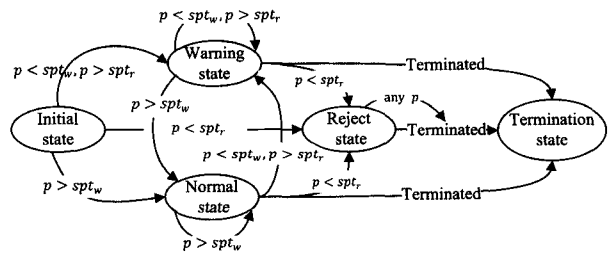

图 3 MSM 状态

随着执行路径的进行，MSM 输出不同的状态。各状态的意义如下：

1)初始态(Initial State，I)，表明 MSM 初始化。

2)正常态(Normal State，N)，表明执行路径正常。

3)警告态(Warning State，W)，表明执行路径发生异常，当前 as 较为可疑，但不至于解绑 ABB，可继续执行。

4)拒绝态(Reject State，R)，表明执行路径发生异常，当前 as 为危险操作，将解绑 ABB 以阻止 as 操作，并终止当前角色的执行路径。拒绝态无法转移至除自身和终止态之外的其他状态。

5)终止态(Termination State，T)，表明 MSM 终止。

需要说明的是，当角色授权撤销后，对应授权的授权步授权也将撤销；而授权步 as 中 ABB 被 MSM 解绑后，终止角色的执行路径同时撤销其所有的角色授权，即 $A_R=\emptyset$。TPM 通常是经过前期大量学习形成的，在实际操作中可以采用动态学习来调整。SPT 可以设置多个阈值来达到更加细粒度的控制。角色授权和授权步授权联动，共同形成面向业务的细粒度动态授权。

3.2.3 授权算法

授权算法主要包括访问控制算法和动态授权算法。

算法 1 访问控制

```
procedure AccessControl(U,S,B,MSM,C)
1. Init(MSM,C)
2. S=StartSession(U,C)
3. R=UA(U,S)
4. bs_set=BS(B)
5. A=Authorize(R,bs_set,C)
6. ABB=Bind(bs_set,A,C)
7. EP=∅
8. while bs in random(bs_set) do
9.    as=ABB(bs)
10.   EP. AddExecutionPath(as)
11.   ms=MSM. DynamicAuthorization (U,S,R,as,EP,C)
12.   if ms ==N then
13.       Execute(R,bs)
14.   elif ms ==W then
15.       Alert(R)
16.       Execute(R,bs)
17.   else
```

```
18.     Terminate(EP)
19.     Unbind(ABB)
20.     Deauthorize(R,bs_set)
21.  end if
22. end while
23. end procedure
```

其中,U 表示用户,S 表示会话,B 表示业务,MSM 表示马尔可夫状态机,C 表示各步骤中的约束条件。

第 1—3 行主要是初始化马尔可夫状态机,用户在约束条件下开始会话,并在会话中分配用户角色;第 4—7 行主要是将业务分为各业务步,并定义相应的授权,绑定为授权步,将执行路径置空;第 8—22 行主要完成了访问控制操作,将业务步执行看作随机过程,首先压入执行路径,随后使用动态授权算法得出相关状态,依据状态完成访问控制操作。

算法 2　动态授权

```
procedure DynamicAuthorization(U,S,R,as,EP,C)
1. if user U with role R in session S have authorization a in authoriza-
   tion-step as with constraint C then
2.   if as in EP then
3.     for i=0 to as count in EP do
4.       probability=probability * TPM[as_i,as_i+1]
5.     end for
6.     if probability < spt_r then
7.       return T
8.     elif probability < spt_w then
9.       return W
10.    else
11.      return N
12.    end if
13.  end if
14. end if
15. return T
16. end procedure
```

其中,U 表示用户,S 表示会话,R 表示角色,as 表示授权步,EP 表示执行路径,C 表示约束条件。

第 1 行主要检查在用户会话中的角色是否执行业务步的授权;第 2—14 行依据 TPM 和 SPT 矩阵对执行路径进行检查,并输出相关状态;第 15 行主要是针对没有相关授权和未在执行路径中的授权步返回终止态。

3.3　BO-RBAC 的形式化定义

(1)BO-RBAC 模型由用户集 U、角色集 R、会话集 S、业务集 B、业务步集 Bs、授权集 A、授权步集 As 以及马尔可夫状态机 MSM 8 部分组成。

(2)$UA\subseteq U\times R$,用户与角色的多对多关系;$AA\subseteq A\times R$,授权与角色的多对多关系;$RH\subseteq R\times R$,角色集的偏序关系;$BS\subseteq b_q\rightarrow Bs, b_q\in B$,业务 b_q 到相应 Bs 的 $1:n$ 关系;$EX\subseteq As\times As$,业务步之间的多对多关系;$CM=\{as\mid as\in EX\}$,已经执行的授权步并按执行顺序排列;马尔可夫状态 $ms\in\{I,N,W,R,T\}$ 即 5 种状态;$As=\{as\mid as=\{a,bs,ABB\},a\in A,bs\in BS,ABB\in\{0,1\}\}$,各 as 之间的关系为 $as\times as=2^{ms}$,$ms\in\{I,N,W,R,T\}$。

(3)$F(s):S\rightarrow U$,每一个会话 s_i 对应的用户 $F(s_i)=u_j$ 的映射;$G(S):S\rightarrow 2^R$,每一个会话 s_i 到角色集 $G(s_i)\subseteq\{r\mid(F(s_i),r')\in UA,\exists r'\geqslant r\}$,而该会话 s_i 具有授权 $A'_{r\leqslant G(s_i)}\subseteq\{a\mid(a,r')\in AA,\exists r'\geqslant r\}$;$T(ms,As):ms_i\rightarrow as_j$,马尔可夫状态对应的授权步的映射,$\forall ms_i\in\{R,T\}$,$as_j(ABB)=0$;$\forall ms_i\in\{I,N,W\}$,$as_j(ABB)=1$;$R(As,TPM,SPT):as_i\rightarrow ms$,每一个授权步执行对应的马尔可夫状态,$ms=cmp(TPM(as_1,as_2,\cdots,as_i),SPT,as_i\in CM)$。

4　模型实现及分析

4.1　模型实现

本文采用 C++14 对所提模型进行编程实现。C++14 标准是对 C++11 标准[16]的修改和完善,主要增加了泛型 Lambda 函数、函数返回类型推导等特性,极大地增强了程序的开发效率和运行效率。

4.1.1　动态授权实现

程序代码包含在 namespace BORBAC 中,由 11 个类组成。其类名和相关说明如表 1 所列。

表 1　程序类说明

类名称	类说明
User	定义程序中用户。是模型中访问业务及业务步的实体
Role	定义用户角色。具有 Authorization 类提供的授权,可继承
Authorization	定义授权的相关属性。包括授权起止时间、允许使用次数等信息
Session	定义用户会话。实现 UA,在 User 访问业务时需要指明所启用的会话
Business	定义业务。在实例化时需要一系列 BusinessStep
BusinessStep	定义业务步。包含实际执行的业务步 callback 函数
Authorization Step	定义授权步。包含业务步、授权和安全状态的绑定关系
ExecutePath	定义执行路径。与特定 Business 相关,记录指定长度的 BusinessStep
SecurityState Machine	定义安全状态机。抽象状态机接口,以支持其他能提供安全状态的算法
MarkovState Machine	定义马尔可夫状态机。是对安全状态机的实现
Client	定义场景类。对实现场景进行定义,提供一体化的验证函数

在模型代码中实现了文中的访问控制措施,程序逻辑如 3.2.3 节中的访问控制算法所述。动态授权主要流程如图 4 所示。

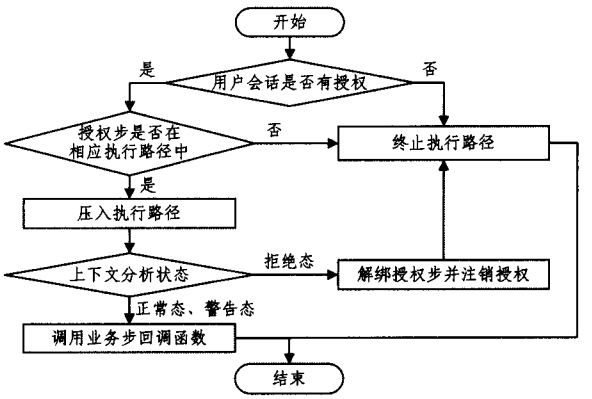

图 4　动态授权的实现流程

具体步骤如下。

1)检查用户会话对特定授权步是否具有相应权限,包括检查权限时间和使用次数等,若为否则转步骤 5)。

2)检查当前授权步是否在相应业务的执行路径中,若为否则转步骤 5)。

3)将授权步压入执行路径但不执行,使用马尔可夫状态机通过 TPM 和 SPT 对执行路径中业务步上下文进行分析。若得出状态为正常态或警告态则转步骤 4),若为拒绝态则转步骤 5)。

4)调用绑定在授权步中的业务步回调函数,执行相应操作,转步骤 7)。

5)解绑授权步,注销用户相应的授权。

6)终止当前执行路径,用户会话无法再次执行该路径中的任何授权步。

7)继续在场景类中执行下一授权步。

4.1.2 模型实例测试

下面以网络开放平台应用接入为场景对模型进行测试。网络开放平台应用接入一般分为两个阶段,分别是开发者管理阶段和应用接入阶段。开发者管理阶段为开放平台对开发者进行注册和授权阶段,在本模型中可视为角色授权;应用接入阶段由创建应用、申请资源、完善应用信息、申请上线和正式上线 5 个步骤构成,可将应用接入视为业务,将 5 个步骤视为业务步,业务步的正常跳转流程如图 5 所示。

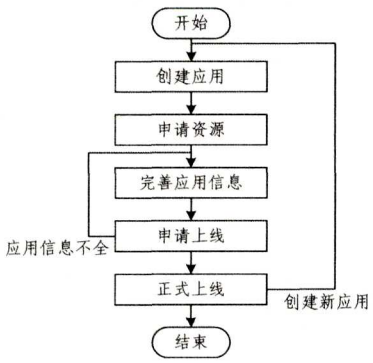

图 5 正常的业务步跳转流程

设开放平台开发者管理阶段将所有业务步对用户进行了授权。将初始转移概率放置在第一行,则可得一个 6×5 的 TPM:

$$TMP=\begin{pmatrix}0.6 & 0.1 & 0.1 & 0.1 & 0.1\\ 0.1 & 0.6 & 0.1 & 0.1 & 0.1\\ 0.1 & 0.1 & 0.6 & 0.1 & 0.1\\ 0.1 & 0.1 & 0.1 & 0.6 & 0.1\\ 0.1 & 0.1 & 0.3 & 0.1 & 0.4\\ 0.6 & 0.1 & 0.1 & 0.1 & 0.1\end{pmatrix}$$

设置 SPT 为:

$SPT=(0.13 \quad 0.1)$

由于计算机位数的限制,当业务执行路径较长时计算得出的概率值可能小于计算机所能表示的最小数量。因此可参考 TCP/IP 协议实现一种计算窗口机制,即选取当前执行路径上一部分授权步的跳转进行概率计算,例如设置窗口大小为 3,则计算从当前授权步前两步跳转到当前授权步的概率情况,窗口随着当前路径上的授权步执行进行移动。授权步的执行计算窗口如图 6 所示。

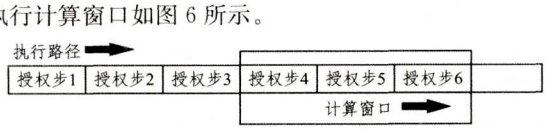

图 6 授权步计算窗口

设图 6 中初始状态跳转到授权步 1 的概率为 p_1,依次跳转的概率为 p_2 到 p_6,当前执行授权步 k,窗口大小为 wl,则可得出当前计算窗口内授权步的跳转概率为:

$$P_w=\prod_{i=k-wl+1}^{k} p_i$$

由于之前的授权步是按概率允许执行的,因此计算当前局部跳转概率也能够说明问题。当窗口大小为执行路径长度时,该算法就成为了经典马尔可夫链的概率计算方法。

事实上应当考虑之前的授权步执行的相关概率,则可得跳转概率 P 的递推公式:

$$\begin{cases}P_1=p_1\\ P_n=f(P_{n-1})\times p_n\end{cases}$$

寻找到合适的 $f(P)$,可将之前所有授权步的跳转概率都计算进去,且不至于使概率值小到无法接受,从而更符合概率计算的要求。当 $f(P_i)=p_i$ 时,该算法成为经典马尔可夫链的概率计算方法。为了简化模型,本文采用计算窗口机制进行计算。

设窗口大小为 3 步。按正常业务步跳转流程,即创建应用、申请资源、完善应用信息、申请上线、正式上线 5 个步骤,则中间任意 3 步的转移概率不低于警告阈值。顺序执行业务步的概率变化如图 7 所示,程序执行结果如图 8 所示。

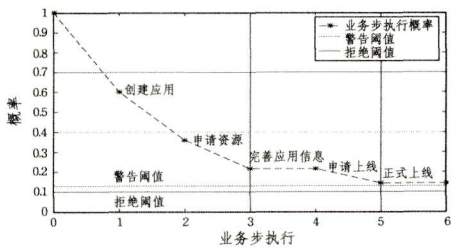

图 7 正常情况的概率变化图

图 8 正常情况的程序执行结果

从概率变化情况来看,正常业务步的执行概率是不低于警告阈值的,程序执行结果也没有任何问题。

如果用户没有按照正常的流程进行,则执行概率可能会低于警告阈值或拒绝阈值。设执行顺序为创建应用、申请资源、申请上线、完善应用信息、正式上线,则业务步执行概率的变化如图 9 所示,程序执行结果如图 10 所示。从概率变化的情况来看,不按照正常顺序执行,概率很快就低于拒绝阈值,导致执行路径终止和 ABB 解绑,同时注销用户对该业务步的授权,阻止当前危险操作和进一步动作。

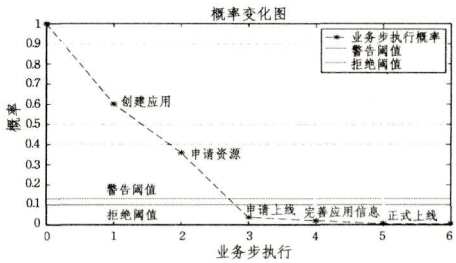

图 9　异常情况的概率变化图

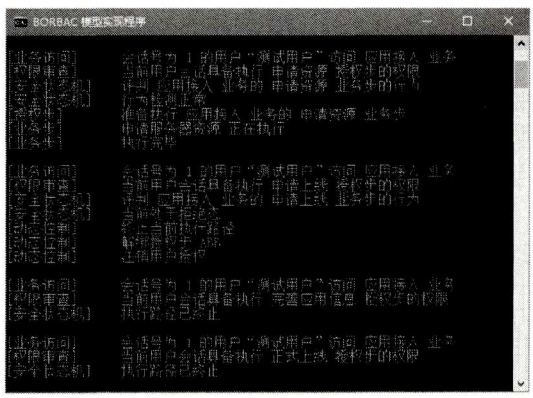

图 10　异常情况的程序执行结果

4.2　模型分析

本模型重新定义了业务与授权步，将授权步所包含的业务步跳转视为随机过程，并用马尔可夫链描述这一过程，更加符合现实中的业务处理流程。将访问控制授权分为角色授权和授权步授权，使本模型更加符合如下访问控制原则。

1)最小特权原则。本模型在角色授权过程中支持角色等级和约束条件，在授权步授权过程中支持基于上下文的动态细粒度授权，一旦出现违例便收回授权。

2)职权分离原则。本模型在角色授权过程中通过约束条件将不相容角色分离，以免导致利益输送等不良授权事件的发生。

3)多级安全原则。本模型在角色授权过程中通过角色等级将角色的权限相应地分为不同等级，可以绑定不同的业务步来执行不同等级的操作。

4)权限抽象原则。本模型授予的权限可以是业务执行过程的所有可能的权限，而不只是传统的“增删改”或者是“读写执行”等权限。

对比文献中的 TBAC 扩展模型或 RBAC 扩展模型，本模型的相应特点和优点如表 2 所列。

表 2　BO-RBAC 模型的对比分析

文献模型	本模型特点	本模型优点
文献[4-5,7-9]	将业务等概念引入模型，授权具有动态性	具有基于业务步的细粒度访问控制授权
文献[10-11]	将用户、角色等概念引入模型，支持分层授权	按角色提供授权，并按照角色等级提供不同授权
文献[12-13]	使用 Markov 链动态调整授权	将业务步跳转视为随机过程，可实现动态授权

从模型实例中的异常情况可以看到，虽然用户依然保持了对完善应用信息和正式上线对应授权步的权限，但是由于当前执行路径已因为异常行为而终止，因此也无法执行。这体现了本模型面向业务动态授权的特点。

TPM 和 SPT 的取值应当依据长期统计分析正常情况下的业务步跳转行为进行设置。在设置 TPM 时，如果将预期执行的业务步概率设置为 1，其余设置为 0，则模型从概率模型退化为白名单模型，在一些严格业务流程的场合下也可以使用。

结束语　在云计算条件下，单独的 RBAC 或 TBAC 已经无法适应当前大数据环境复杂组织架构和多元业务条件下的访问控制授权，其授权粒度过粗、动态授权能力不足、业务流程控制不严等问题凸显。本文结合 TBAC 思想，在 RBAC96 模型的基础上提出了一种面向业务的动态 RBAC 模型，即 BO-RBAC 模型。通过与其他模型的对比分析表明，本文所提模型具有基于业务步的细粒度访问控制授权、按照角色等级提供授权、上下文分析动态授权等优点。下一步将继续深入研究基于深度学习的业务步动态分析方法并寻找合适的 $f(P)$，以进一步提高 BO-RBAC 的动态授权能力。

参 考 文 献

[1] YUAN J B, WEI L L, ZENG Q H. Delegation based cross-domain access control model under cloud computing for mobile terminal[J]. Journal of Software, 2013, 24(3): 564-574. (in Chinese)
袁家斌，魏利利，曾青华. 面向移动终端的云计算跨域访问委托模型[J]. 软件学报，2013，24(3)：564-574.

[2] ZHAO M B, YAO Z Q. Access control model based on RBAC in cloud computing[J]. Journal of Computer Applications, 2013, 32(A2): 267-270. (in Chinese)
赵明斌，姚志强. 基于 RBAC 的云计算访问控制模型[J]. 计算机应用，2013，32(A2)：267-270.

[3] ISO. IEC14882:2014 Information technology—Programming languages—C++ [S]. Geneva, Switzerland: International Organization for Standardization, 2014.

[4] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control: A multi-dimensional view[C]// Computer Security Applications Conference. IEEE, 1994: 54-62.

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

[6] XIONG H R, CHEN X Y, ZHANG B, et al. Security Principles for RBAC-based Authorization Management [J]. Computer Science, 2015, 42(3): 117-123. (in Chinese)
熊厚仁，陈性元，张斌，等. 基于 RBAC 的授权管理安全准则分析与研究[J]. 计算机科学，2015，42(3)：117-123.

[7] WU L Y, LIU S Y, FAN L J, et al. Research on Improved RBAC Model Oriented to Web Cluster Application[J]. Computer and Network, 2015(12): 53-56. (in Chinese)
吴丽颖，刘淑瑜，范霖君，等. 面向 Web 集群应用的改进 RBAC 模型研究[J]. 计算机与网络，2015(12)：53-56.

[8] ZHOU X G, LIU J W, LIU W R, et al. Anonymous Role-Based Access Control on E-Health Records[C]// Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016: 559-570.

(下转第 167 页)

[6] WANG Y, LIU S Y, ZHANG W, et al. Threat Assess ment Method with Uncertain Attribute Weight Based on Intuitionistic Fuzzy Multi-Attribute Decision[J]. Acta Electronica Sinica, 2014,42(12):2509-2514. (in Chinese)
王毅，刘三阳，张文，等. 属性权重不确定的直觉模糊多属性决策的威胁评估方法[J]. 电子学报，2014,42(12):2509-2514.

[7] WANG G G, GUO L H, DUAN H, et al. The Model and Algorithm for the Target Threat Assessment Based on Elman-AdaBoost Strong Predictor[J]. Acta Electronica Sinica, 2012, 40(5):901-906. (in Chinese)
王改革，郭立红，段红，等. 基于 Elman_AdaBoost 强预测器的目标威胁评估模型及算法[J]. 电子学报，2012,40(5):901-906.

[8] MA S D, HAN L, GONG G H, et al. Target threat assessment technology based on cloud model[J]. Journal of Beijing University of Aeronautics and Astronautics, 2010, 36(2):150-153. (in Chinese)
麻士东，韩亮，龚光红，等. 基于云模型的目标威胁等级评估[J]. 北京航空航天大学学报，2010,36(2):150-153.

[9] GAO X G, LI Q Y, DI R H. MPC three - dimensional dynamic path planning for UAV based on DBN threat assessment[J]. Systems Engineering and Electronics, 2014, 36(11):2199-2205. (in Chinese)
高晓光，李青原，邸若海. 基于 DBN 威胁评估的 MPC 无人机三维动态路径规划[J]. 系统工程与电子技术，2014,36(11):2199-2205.

[10] DI R H, GAO X G, GUO Z G. The Modeling Method with Bayesian Networks and Its Application in the Threat Assess ment Under S maII Data Sets[J]. Acta Electronica Sinica, 2016, 44(6):1504-1511. (in Chinese)
邸若海，高晓光，郭志高. 小数据集 BN 建模方法及其在威胁评估中的应用[J]. 电子学报，2016,44(6):1504-1511.

[11] ZHANG Y Y, LI B C, CUI J W. Method of Target Threat Assessment Based on Cloudy Bayesian Network[J]. Computer Science, 2013, 40(10):127-131. (in Chinese)
张银燕，李弼程，崔家玮. 基于云贝叶斯网络的目标威胁评估方法[J]. 计算机科学，2013,40(10):127-131.

[12] ZAIDI A K, MANSOOR F, PAPANTONI-KAZAKOS T P. Theory of Influence Networks[J]. Journal of Intelligent & Robotic Systems, 2010, 60(3):457-491.

[13] ROSEN J A, SMITH W L. Influence Net Modeling with Causal Strengths: An Evolutionary Approach[C]// Proceedings of the Command and Control Research and Technology Symposium. Monterey, 1996:25-28.

[14] CHEN Y X, WU X Y, BU X W, et al. Simulation credibility control based on risk analysis[J]. System Engineering Theory and Practice, 2014, 34(9):2411-2416. (in Chinese)
陈永兴，吴晓燕，卜祥伟，等. 基于风险分析的仿真可信性控制[J]. 系统工程理论与实践，2014,34(9):2411-2416.

[15] MA Y H, ZHANG Y Z, ZHANG Y. Situation Assessment Based on Influence Net[J]. Fire Control & Command Control, 2014, 39(6):90-93. (in Chinese)
马延豪，张耀中，张莹. 基于影响网络的态势估计[J]. 火力与指挥控制，2014,39(6):90-93.

[16] DU Z J, CHEN C, JIANG X. Modeling and solution method of course of action based on influence net and multi-stage games with incomplete information[J]. Journal of National University of Defense Technology, 2012, 34(3):63-67. (in Chinese)
杜正军，陈超，姜鑫. 基于影响网络与不完全信息多阶段博弈的作战行动序列模型及求解方法[J]. 国防科技大学学报，2012, 34(3):63-67.

[17] 娄寿春. 面空导弹武器系统分析[M]. 北京：国防工业出版社，2013:50-230.

[18] ZHENG Y J, TIAN K S, CHEN G, et al. Operational Efficiency Evaluation for Anti-missile Early Warning Radar Based on Grey AHP[J]. Journal of Equipment Academy, 2016, 27(1):111-115. (in Chinese)
郑玉军，田康生，陈果，等. 基于灰色 AHP 的反导预警雷达作战效能评估[J]. 装备学院学报，2016,27(1):111-115.

[19] 李德毅，刘常昱，杜鹢，等. 不确定性人工智能[M]. 北京：国防工业出版社，2005:137-186.

(上接第 145 页)

[9] CAU T, NIE Q B, OUYANG K, et al. Role-extended-based RBAC model[J]. Application Research of Computers, 2016, 33(3):882-885. (in Chinese)
蔡婷，聂清彬，欧阳凯，等. 基于角色扩展的 RBAC 模型[J]. 计算机应用研究，2016,33(3):882-885.

[10] DENG J B, HONG F. Task-Based Access Control Model[J]. Journal of Software, 2003, 14(1):76-82. (in Chinese)
邓集波，洪帆. 基于任务的访问控制模型[J]. 软件学报，2003,14(1):76-82.

[11] LAPIN S. Access control model D-TBAC subject to the requirements to tasks' performing[C]// Proceedings of the 8th International Conference on Security of Information and Networks. ACM, 2015:42-45.

[12] SHI J F, LI J H, XUE Z. Research of Authorization Model Based TBAC[J]. Communications Technology, 2002(11):95-97. (in Chinese)
施教芳，李建华，薛质. 一种扩展的 TBAC 访问控制模型研究[J]. 通信技术，2002(11):95-97.

[13] ZHANG Q P. Research on Tasks and Role Based Access Control Model[J]. Computer Security, 2008(9):74-75. (in Chinese)
张庆萍. 基于任务和角色的访问控制模型研究[J]. 计算机安全，2008(9):74-75.

[14] SCHMIDT P J, PINTAR K D, FAZIL A M, et al. Harnessing the Theoretical Foundations of the Exponential and Beta-Poisson Dose-Response Models to Quantify Parameter Uncertainty Using Markov Chain Monte Carlo[J]. Risk Analysis, 2013, 33(9):1677-1693.

[15] WANG H, YAJIMA A, LIANG R Y, et al. Bayesian Modeling of External Corrosion in Underground Pipelines Based on the Integration of Markov Chain Monte Carlo Techniques and Clustered Inspection Data[J]. Computer-Aided Civil and Infrastructure Engineering, 2015, 30(4):300-316.

[16] ISO. IEC14882:2011 Information technology--Programming languages--C++ [S]. Geneva, Switzerland: International Organization for Standardization, 2011.