doi:10.3969/j.issn.1000-436x.2013.z1.027

云计算下可信虚拟群体内访问控制研究

梁鹏，沈昌祥，宁振虎
（北京工业大学 计算机学院 北京市可信计算北京市重点实验室 北京 100124）

摘 要：针对缺乏适合基于云计算的生产型重要信息系统内部隔离机制的问题，对云计算模式下现有的访问控制技术进行了比较，提出了基于两级密钥管理的访问控制方案。第一级构造了一个基于单项散列函数的访问控制多项式实现了子群体间信息流的隔离，即实现了生产型重要信息系统内部门间的信息隔离；在第一级密钥管理的基础上，提出了子群体间层次密钥管理，实现不同部门间信息流的访问控制。然后对该方案的安全性和复杂度进行了分析。最后，通过实例和仿真实验对基于两级密钥管理的访问控制方案进行了验证。
关键词：云计算；密码学访问控制；密钥管理；生产型信息系统
中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2013)Z1-0207-09

On access to trusted virtual group under cloud computing

LIANG Peng, SHEN Chang-xiang, NING Zhen-hu
(Beijing Key Laboratory on Trusted Computing, College of Computer Science, Beijing University of Technology, Beijing 100124, China)

Abstract: There is no appropriate internal isolation mechanism for important production information system based on cloud computing. Here the main access control technologies were compared thoroughly and then two-layer key management scheme was put forward. In terms of the first layer, access control polynomial based on one-way hash function was constructed to achieve the separation of information flow between subgroups, that is, the information isolation within any department of a company was accomplished. Based on the first layer, a hierarchical key management was presented for different subgroups so as to realize the access control between different departments of a company. Then the security and complexity were analyzed. Finally, through the example and simulation experiment, the access control model based on two-layer key management scheme was verified.
Key words: cloud computing; cryptographic access control; key management; production information system

1 引言

1.1 研究背景

生产型重要信息系统（也称为 Hyposys 系统）是一个大型分布式的信息系统，该类系统是一个安全性要求较高的重要信息系统，其安全需求与很多专用业务网络平台相同，由分布在全国各地的若干个网络节点组成，上面运行有完成多个业务功能，这些业务软件运行过程中，生成大量的文件和数据库需要进行严格的访问控制，该系统内部安全程度要求很高，但由于业务特点，又不得不连接到互联网，这样系统成为攻击和渗透的重点对象。系统依然面临着来自内部的非法篡改和来自外部病毒木马干扰等一系列重大安全问题[1,2]。基于云计算技术的生产型重要信息系统本质是基于虚拟架构的分布式计算环境，其主要特点是，数据集中存储处理和桌面虚拟化，通过搭建中央服务器集群构建“内部云”，并采用桌面虚拟化技术来实现。

收稿日期：2013-07-05
基金项目：国家科技重大专项“新一代宽带无线移动通信网”基金资助项目（2012ZX03002003）；国家高技术研究发展计划（“863”计划）基金资助项目(2009AA01Z437)；国家核高基金资助项目（2010ZX01037-001-001）
Foundation Items: Major Projects of the Wireless Mobile Communications (2012ZX03002003); The National High Technology Research and Development Program of China (863 Program) (2009AA01Z437); Core Electronic Devices, High-end General Purpose Chips and Basic Software Products (2010ZX01037-001-001)

生产型重要信息系统是高安全的信息系统，龚备、沈昌祥等首先在生产型重要信息系统的可信证明中引入群体的概念[3,4]。其基本思想是，将生产型重要信息系统视为一个复杂巨系统[5,6]，引入社会生态学的理论对生产型重要信息系统进行研究。重视研究群体的内部层次结构对信息系统安全的影响，并在可信证明中强调群体的参考性作用，类似于社会中涉密部门对员工政审时需要对周围的亲戚朋友进行考察。本文是对上述工作的延续，因此，采用群体的概念。生产型信息系统，比如涉密系统中用户的身份和操作通常是比较固定的，不像一般信息系统中的用户可以随意变动，这些用户具有可信性的特点，所以在研究中称这些群体为可信群体。

借鉴社会生态学中群体的概念，针对生产型信息系统定义云计算模式下可信虚拟群体的概念。可信虚拟群体，是指为了完成一个特定的目标而动态形成的由一个或者多个物理计算节点上虚拟计算节点组成的动态集合，该动态集合是由单个虚拟机计算节点组成的，反过来影响着每个虚拟计算节点，并且该动态集合内部有特定的层次组织结构。在可信虚拟群体概念基础上，为了更好地实现细粒度的访问控制，本文进一步给出了可信虚拟子群体，是指为了完成一个群体内某个特定的目标而动态形成的由群体内的部分虚拟计算节点组成的动态集合。

1.2 云计算模式下访问控制研究现状

传统的访问控制模型在特定的应用领域下的应用是有效的，在一定的条件下能够满足用户对信息安全的保护性需求。比如 DAC[7]在个人操作系统中的应用，MAC 在军队信息系统中的应用，RBAC 在商业领域的成功应用等。但是随着分布式应用的广泛发展和深入应用，各种分布式系统的出现，如云计算以及基于互联网的其他应用等，传统的访问控制模型在面对网络的开放性和动态性等特征时难以适应，主要表现在以下几个方面。

第一，传统的访问控制[8~11]BLP、Biba 等型本质上是静态的访问控制模型，它们都是针对集中式、静态环境下的应用而被提出的。在这样的系统中，系统资源和用户都是已知的，用户只能访问已知的系统资源，但是在开放的分布式互联网络中，用户和资源的提供者来自不同的安全域，彼此是陌生的，出于某种需求关系需要临时建立访问和被访问的关系。因而任何系统的访问请求者都可能是分布在整个互联网中的任何用户，传统的访问控制模型根据自身的访问控制策略无法给出一个合理的授权。

第二，在分布式环境下，规模庞大的面向不同领域的用户需求差异较大，因而客观上要求细粒度的、动态的访问控制，然而，在商业领域被广泛使用的访问控制模型 RBAC[12~14]中，如果用户获得了某个角色，就获得了该角色被指派的所有权限，这有可能超出用户完成某项任务所必需的最小权限，因而它是粗粒度的。另外，用户到角色、角色到权限的映射关系是相对稳定的，不便于经常修改，因而 RBAC 是静态的。RBAC 的灵活性较差，如果系统结构或需求发生了变化，就需要修改原有的用户到角色、角色到权限的多对多映射关系来满足这种变化后的需求，当系统规模比较大并且用户到角色和角色到权限变化频率较高的时候，就大大加重了系统管理的负担。

由于传统的访问控制模型如 DAC、MAC、RBAC 等都是基于集中式的应用需求而被提出的，它们适用于集中式、静态、封闭的应用环境。包括 DAC、MAC、RBAC 等在内的传统的访问控制模型不能适应开放的网络环境下的访问控制问题，它们面临着这样的问题：由于它们的访问控制策略的差异性，因此不能被良好地执行。而分布式系统的主要特点是分散性、动态性、开放性、大规模性等，这客观上对传统的访问控制模型构成了巨大挑战。有很多研究者在传统的访问控制模型尤其是 RBAC 的基础上对其进行了改进和扩展，试图解决这些问题，但无法从根本解决它们的不足。

基于密码学的访问控制技术[15,16]是伴随着分布式应用的发展而被提出的一种访问控制机制，目的在于解决分布式环境下的访问控制问题，因而先天对分布式环境有更好的适应性。它的基本思想是：访问控制以群体内部的层次结构作为基础进行授权决策(不仅仅依赖于标识)，它可以随着实体的属性的变化，动态地更新访问控制决策，从而能够提供一种更加细粒度、灵活的动态访问控制方法。

采用密码学的方法还有：基于层次密钥生成与分配策略实施访问控制的方法[17]，利用基于属性的加密算法(如密钥规则的基于属性加密方案(KP-ABE)[18]、基于代理重加密的方法[19]以及在用

户密钥或密文中嵌入访问控制树的方法等[20]。

基于密码学方案面临的一个重要问题是权限撤销。在基于密码学的访问控制模型中，群组成员不仅能够自由地加入和离开通信群组，也可能在不同的用户组之间切换，为了保证所有资源仅能被授权用户访问，群组中每个成员仅能获取拥有访问授权资源的加密密钥。因此，为了保证系统的安全性，基于密码学访问控制模型中需要考虑前向安全性和后向安全性。在新成员加入某用户组时，系统分配给该用户组的密钥需要进行更新，以保证该新成员不能获取其加入之前的群组通信（后向安全性）；当某用户组中有成员离开时，系统分配给该用户组的密钥也需要进行更新，以保证离开的成员不能获取其离开之后的群组通信（前向安全性）。

2　两级密钥管理方案设计

在云计算环境下，可信虚拟群体内部虚拟机成员为了达到负载均衡等目的具有很强的动态性，传统的访问控制机制无法适应虚拟机成员频繁地加入退出以及可信虚拟群体内不同层次子群体的群体通信需求，而基于密码学的访问控制可以根据其所具有的密钥并结合访问控制策略判断是否允许其通信或数据访问请求。

结合分布式系统群组通信的点，考虑了可信虚拟群体内部多对多的通信方式。在本文的两级密钥管理方案中将子群体视为群组通信中的一个群组。在本文阐述中子群体、节点是相同的含义可以互相替换。

基于以上两方面的考虑，本文提出了基于两级密钥管理的访问控制策略模型。其中两级密钥管理方案（TLKMS, two lay key management scheme）由两级组成：第一级实现动态子群体间的隔离及密钥分发问题；第二级基于第一级密钥管理实现群体内部的层次访问控制（hierarchical access control）。

2.1　第一级密钥管理

假定子群体中的每一个有效的成员（记为 U_i）被分配了一个秘密密钥。当一个虚拟机加入一个群体时，虚拟机群体控制者（VMG master）把相应的策略发给该虚拟机，包括该虚拟机在群体生命周期中使用的永久秘密密钥。假定 P 是一个大的素数，它可以构成一个有限域 F_p。

无论什么时候有虚拟机准备加入一个可信子群体中，云管理中心群体管理组件的密钥管理服务器（简记为 CM-KMS）将会在有限域 $F_p[x]$上构造一个多项式 $A(x)$。

$$A(x)=\prod_{i=1}^{m}(x-f(sk_i,z)) \tag{1}$$

其中，m 表示参与子群体 $\boldsymbol{\Phi}$ 的成员的个数，sk_i 是群体中成员的永久密钥，将被分发给子群体中的所有成员。$H(x,y):Z_p^*\times\{0,1\}^n\to Z_p^*$ 为密码学安全散列函数，z 是一个取自于 $\{0,1\}^n$ 上的随机整数。$A(x)$ 称为访问控制多项式（access control polynomial）。正如式(1) $A(x)$ 以合法客户虚拟机的密钥的 $H(sk_i,z)$ 为根，当取合法客户虚拟机密钥时，$A(x)$ 的值为零；否则 $A(x)$ 的值是一个随机值。

CM-KMS 为子群体 $\boldsymbol{\Phi}$ 随机地选取群组密钥 K 以及保护密钥 $\hat{K}$（$\hat{K}$ 主要用于在分层访问控制中，群成员退出所引起的子群体密钥 K 更新），计算多项式

$$P(x)=A(x)+\hat{K} \tag{2}$$

$$K=H(\hat{K},\hat{z})$$

其中，$\hat{z}$ 为随机数。最后，CM-KMS 公开 $(z,\hat{z},P(x))$。

通过这个公开信息，任何组员 U_i 可以得到群组密钥

$$\hat{K}=P(H(sk_i,z)) \tag{3}$$

$$K=H(\hat{K},\hat{z}) \tag{4}$$

对于任何别的不属于 $\boldsymbol{\Phi}$ 的成员 U_r，$P(H(sk_i,z))$ 是一个随机值，因此成员 U_r 不能得到密钥 $\hat{K}$，进而不能得到群组密钥 K。这个密钥管理机制可以保证只有当客户虚拟机的 SID_i 包含于 $A(x)$ 中时，该客户虚拟机才可以从 $P(x)$ 中提取出密钥来。

利用该方案，可以便于动态组的管理，如对于撤销客户虚拟机或加入新客户虚拟机时的密钥问题，可以较容易解决。当新客户虚拟机 U_t 加入群 U，CM-KMS 只需创建一个新的 sk_t 并把它分配给 U_t。然后，CM-KMS 按照以下方式更新 $A(x)$：

$$A'(x)=A(x)(x-H(sk_i,z)) \tag{5}$$

$A'(x)$ 通过计算 $P'(x)=A'(x)+\hat{K}$ 来隐藏密钥 $\hat{K}$。然后，发送 $(z,\hat{z},P'(x))$ 发送给 U_t。接收到 $(z,\hat{z},P'(x))$ 之后，U_t 利用 sk_t 从式(3)中推导出密钥 $\hat{K}$，进而由 $K=H(\hat{K},\hat{z})$ 得到 K。

当前成员 U_t 从子群体 $\boldsymbol{\Phi}$ 中退出时，CM-KMS

选择 2 个新随机数 $z,\hat{z},$，然后，CM-KMS 按照以下方式更新 $A(x)$

$$A'(x)=\frac{A(x)}{x-H(sk_i,z)} \tag{6}$$

然后，根据 CM-KMS 新的群组密钥 K' 以及保护密钥 $\hat{K}'$，计算 $P'(x)=A'(x)+K'$，而后在群体内广播 $(z',\hat{z}',P'(x))$。此时删除的客户虚拟机 U_t 不能从 $P'(x)$ 中提取出密钥 K'。

2.2 第二级密钥管理

第二级是在第一级的基础上的解决群体内不同层次子群体间的访问控制问题，即密码学中的 HAC（hierachical access control）问题的。在层次结构中，一个在较高层的节点具有访问它的子孙节点的权限。但是，相反是禁止的。基于密码学技术的 HAC 工作原理如下。在层次结构中的每一个节点分配一个加密密钥。更高层次上的节点可以根据自己的密钥推导出子孙节点密钥。相反的，是不正确的。下面介绍一个由 Lin 提出的典型的 HAC 方案[21]。假设每个节点分配了一个公开的身份和私有节点密钥。2 个节点之间的每个边被分配一个公开边权值，该值通过一个单向散列函数计算得出。例如，假定节点 v_i 和 v_j 的公开身份分别为 ID_i 和 ID_j，其私有节点密钥分别为 k_i 和 k_j，则从 v_i 到 v_j 的公开边权值将是 $p_{i,j}=k_j\oplus H(k_i,ID_j)$，其中，$f(x,y)$ 是单项散列函数。因此，v_i 可以计算 v_j 的密钥 $k_j=\ p_{i,j}\oplus H(k_i,ID_j)$。此外，如果 v_i 是 v_j 的祖先节点，v_i 可以沿着从 v_i 到 v_j 路径上的边权值进行迭代计算进而推导出 v_j 的密钥。但是 v_j 反过来不能推导出 v_i 的密钥。该方案的好处是因为节点的密钥是独立的，一个节点密钥的改变不会影响到它的子孙节点密钥，但是会引起公开边权值的更新。

本文采用上述 Lin 的方案作为第二级 HAC 机制。Lin 的方案中存在的重要问题是当一个成员离开一个节点比如 v_i，不但 v_i 的密钥 k_i 需要改变并分配给节点 v_i 中剩余的成员，而且 v_i 所有的子孙节点的密钥需要改变，这是因为被撤销的成员已经知道这些密钥。这明显是一个密钥更新问题。为了解决这个问题，采用如下解决机制，为每个节点增加了一个密钥并且多使用散列函数 $H(x,y)$ 一次。该机制的原理如下：假定每个子群体节点 v_i 有一个保护密钥的密钥 $\hat{k}_i$，如第一级所述在分配 k_i 的时候，同时将该密钥 $\hat{k}_i$ 安全地分配给节点 v_i 的每个成员。由于上层节点成员的退出而导致本节点更新密钥时，$\hat{k}_i$ 不变，子群体私有密钥 k_i 定义为 $k_i=H(\hat{k}_i,\hat{z}_i)$，$\hat{z}_i$ 由 CM-KMS 产生并分发给各个成员。因此节点 v_i 的成员拥有密钥 $\hat{k}_i$，此外 $\hat{z}_i$ 是公开的，v_i 中的每一个成员可以自己计算私有密钥 k_i。正如前面所述，公开边权值是依据私有密钥定义的。父节点可以导出他的子孙节点 v_i 的私有密钥 k_i 但是不能导出保护密钥 $\hat{k}_i$。$\hat{z}_i$ 的改变可以很容易地改变 k_i。因此，当有成员离开时 v_i，$\hat{k}_i$ 和 k_i 按照第一级重新分配。总之，第二层的 HAC 方案定义如下。

1) 上层节点成员的退出而导致本节点更新密钥时，对于每个节点 v_i，利用本身存储的保护密钥 $\hat{k}_i$，一个公开的 $\hat{z}_i$，计算（由它自己计算得出）

$$k_i=H(\hat{k}_i,\hat{z}_i) \tag{7}$$

2) 对于每个从 v_i 到 v_j 的边权值，公开的边权值 $p_{i,j}$ 为二元组 $(p_{i,j}^1,p_{i,j}^2)$ 定义如下

$$\begin{cases}p_{i,j}^1=k_j\oplus H(k_i,ID_j\oplus p_{i,j}^2)\\ p_{i,j}^2=r\end{cases} \tag{8}$$

其中，r 为 CM-KMS 选择的随机数。

图 1 显示了访问的层次结构，密钥和边权值。每个节点表示一个由第一级成员组成的一个子群体。

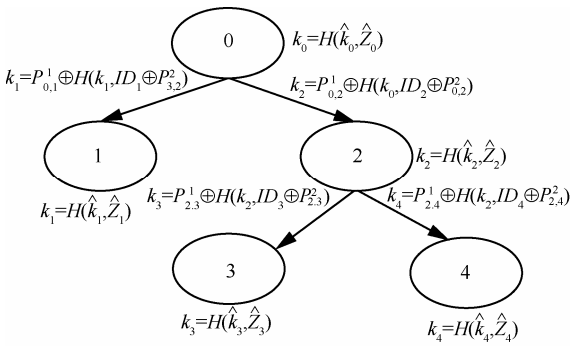


图 1 层次访问控制密钥推导

现在开始阐述两级密钥管理方案的具体的操作。

1) 密钥推导：假定节点 v_i 是节点 v_j 的父节点，v_i 可以通过利用它自己的私有密钥 k_i 和公开信息 $p_{i,j}$ 及 ID_j 导出 k_j

$$k_j=p_{i,j}^1\oplus H(k_i,ID_j\oplus p_{i,j}^2) \tag{9}$$

但是因为函数的单向性，节点 v_j 不能计算出 k_i。

2) 类似地，如果节点 v_i 是节点 v_j 祖先节点，沿着从 v_i 到 v_j 的路线，v_i 可以通过它自己的私有密钥经过迭代地导出 v_j 的密钥。

3) 当一个节点密钥需要更新，更新不会影响其他节点的密钥，除了与他相邻的点之间边权值。假设节点 v_i 的密钥 k_i 需要改变，分 2 种情况进行。上层节点成员的退出而导致本节点更新密钥时，各节点 v_i 按照式(7)产生；其他情况更新密钥时，按照第一级重新分配密钥。然后，对于 v_i 的父节点 v_t，重新计算 $p_{t,i}=(p^1_{t,i},p^2_{t,i})$ 用作公开信息。类似地，到 v_i 得子节点 v_j，重新计算 $p_{i,j}=(p^1_{i,j},p^2_{i,j})$。

4) 增加或者删除一个节点进行类似地处理。如果一个新的节点 v_i 需要增加，仅需要选择密钥 $\hat{k}_i$、z、$\hat{z}$，并按照第一级方法把它们分发给节点 v_i。节点 v_i 接收到后，按照第一级公式计算出 $\hat{k}_i$，k_i。然后，计算并把边权值公开给它的父节点和子孙节点。类似地，如果一个现存的节点 v_i 需要被移除，删掉 v_i 邻接的边权值，然后删除掉 v_i。

5) 增加/删除一个边。增加一个边意味着计算和公开边权值。至于删除一个边，比如从 v_i 到 v_j，如果存在从 v_i 到 v_j 别的路径，什么都不需要做，因为 v_i 仍然可以通过别路径计算出 v_j 的密钥。但是如果只有一条路径从 v_i 到 v_j，v_i 在删除完成之后不能计算 v_j 的密钥(所有 v_j 子孙的密钥)。这意味着 v_j 的密钥 k_i 和 v_j 子孙的密钥 k_i 需要按照式(7)改变。这种改变无须改变他们的公开 ID，也不需要重新生成或发送保护密钥。

2.3　两级密钥管理方案的好处

通过两级相结合，由 v_i 表示子群体的所有成员在第二级共享一个子群体保护密钥 $\hat{k}_i$。每个成员 u_j 在第一级加入子群体进行注册时被分配一个私有密钥 sk_j。每个节点 v_i 有唯一的子群体保护密钥 $\hat{k}_i$ 和 $A_i(x)$。$A_i(x)$ 由 V_i 中的所有成员的 sk 构成，通过 $P_i(x)$ 的多点传送把 $\hat{k}_i$ 分发给 v_i 的所有成员。所有节点 v_i 上的成员可以推导出子群体保护密钥 $\hat{k}_i$。在初次分配和由于子群体成员更新时，导致的密钥重新分配，k_i 按照式(1)计算；上层节点成员的退出而导致本组更新密钥时，k_i 通过式(7)计算。

在第一级，当一个成员 u_r 离开子群体 v_i，通过计算不含 $(x-H(sk_r,z'))$ 的 $A_i'(x)$ 并在子群体内多点传送 $P_i'(x)$，新的子群体密钥 $\hat{k}_i'$ 和 k_i' 将会被分配。然后，剩下的组成员可以通过式(3)和式(4)导出新的子群体密钥 $\hat{k}_i'$ 和 k_i'，但是 u_r 不可以。新的 $\hat{k}_i'$ 和 k_i' 将会在第二级导致相应的改变。2 种类型的更新将会进行。1）所有 v_i 父节点的边权值。2）v_i 的子树上所有边的权值。这些更新步骤可以有效地防止已删除的客户虚拟机 u_r 从它之前的子孙节点提取新的密钥。

TLKMS 明显的优点通过结合两级。在第一级，利用 $A(x)$ 和 $P(x)$ 保证高效、安全地进行密钥分配。此外，通过分配 SID_i 以及在 $A(x)$ 中添加/删除相应的项使得处理子群体内成员动态变化变得简单。在第二级，从一个单向散列函数计算的边权值保证更高层的节点可以对低层的节点实现访问控制。此外，更新节点的私钥可以很容易地通过重新选择随机数实现。因此，两级密钥的组合可以确保改变到一个节点不影响其他节点（例如他们的私有节点密钥）。

3　虚拟群体内部访问控制研究

第 2 节提出的 TLKMS 可以保证云计算群体内的数据通信和访问控制安全。如图 2 所示为云计算群体内基于 TLKMS 访问控制结构示意图。

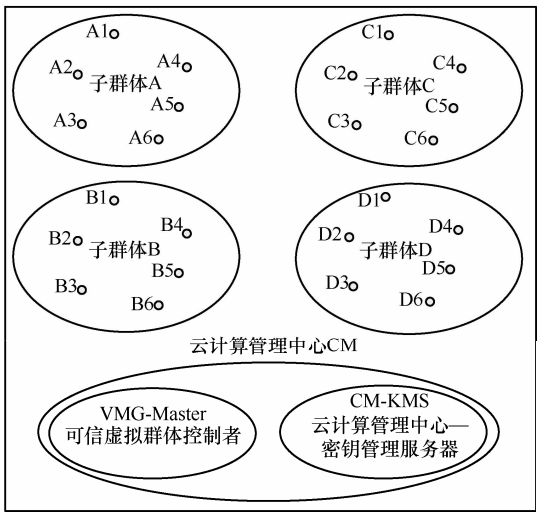


图 2　云计算群体内 TLKMS 结构示意

当一个虚拟机第一次加入到某个可信虚拟群体中时，CM-KMS 给他颁发证书。TLKMS 中第一步给参与者分发密钥的工作，可以借助于 CM-KMS

颁发证书来实现。由于加入注册是一个 CM-KMS 和该虚拟计算节点之间的点至点过程，任何两方的公钥/私钥方案可用于加密初始的信息。

结合图 1 说明在云计算虚拟机群体中如何利用 TLKMS 实现访问控制。

基于上述分析，云计算可信虚拟群体内部访问控制步骤如下。

1) 一个子群体中的虚拟机向可信虚拟群体控制者请求访问特定子群体的资源。

2) 可信虚拟群体控制者检测该资源（包括计算资源和数据资源）是否存在。

3) 可信虚拟群体控制者通知 CM-KMS。CM-KMS 随机生成一个密钥 K_1，然后使用节点 v_i 的私有密钥 k_i 加密 K_1，这里节点 v_i 是指拥有这些资源的节点。

4) CM-KMS 向这些资源和可信虚拟群体控制者多播加密密钥。

5) 具有 k_i 的资源利用 k_i 解密 K_1。可信虚拟群体控制者可以首先导出 k_i。CM-KMS 在层次结构的顶层，v_i 是其子孙节点。所以可信虚拟群体控制者也可以得到相同的 K_1。

因此，这些资源及可信虚拟群体控制者可以一起使用这个共享密钥 K_1 进行通信。

4 安全性分析

本节对所提出的基于两级密钥管理的访问控制方案的安全性进行分析。

4.1 子群体内部攻击

内部攻击是指在同一个节点上的客户虚拟机单独或勾结其他客户虚拟机试图去发现他们不知道的东西。然而，在本文的方案中，在同一个节点 v_i 的客户虚拟机共享相同的密钥 $\hat{k}_i$ 和私有密钥 k_i。节点中的客户虚拟机仅仅知道 sk_i，而不知道其他客户虚拟机的信息。因此顶点成员唯一可能采用的攻击方式是从 $P(x)$ 中找到同一顶点中的其他客户虚拟机的 sk_s。然而，本文方案在第一级中设计可以很好地应对这种类型的攻击：例如内部成员可以得到 $\hat{K}$，然后从 $P(x)$ 中减去 $\hat{K}$ 得到 $A(x)$。通过设置 $A(x)=0$，试图找到根。即使内部成员可以某种方式找到一个根，这个根将会是 $H(sk,z)$ 但不是 sk。此外，由于 $H(sk,z)$ 是密码学安全散列函数，因此任何人不能从 $H(sk,z)$ 得到 sk。知道的 $H(sk,z)$ 唯一的用处是得到 $\hat{K}$，方法是通过把它插入到这个 $P(x)$ 中（对任何其他 $P'(x)$，z' 是不同的，$H(sk,z')$ 也是）。但是，内部成员已经得到了 $\hat{K}$。因此，本方案利用了一个单向函数，可以有效地防止内部单个成员的攻击。

多个内部客户虚拟机串通情况如下。设 w 个内部的成员勾结串通企图得到其他成员的个人秘密，他们利用自己的 sk_i $(i=1,2,3,\cdots,w)$，本文设计的 $A(x)$ 可以使恶意串通毫无意义。这不同于其他多项式使用的技术[22,23]。之前的以多项式为基础的方案中，$t+1$ 及以上个内部成员能发现整个多项式，通过对他们的 $t+1$ 点进行插值（比如 $(ID_i,h(ID_i))$）（其中，t 为系统的安全性参数同时也是多项式的次数）。然而，本方案中多项式插值是没用的，因为可以得到成员的信息只有一个值（即 $H(sk,z)$，但不是 $A(H(sk,z))=0$。因此，恶意客户虚拟机可以得到 $H(sk_{\text{root}},z)$，但是得不到 sk_{root}。在接下来的构造中，随机值 z 更改为 z'，这使得 $H(sk_{\text{root}},z)$ 变得无用。总之，TLKMS 方案是很好应对任何程度的子群体内部勾结。

4.2 子群体合谋攻击

子群体合谋攻击意味着在不同节点的成员相互串通，企图找到其他的子群体的私有群组密钥 k_i 或其他客户虚拟机的秘密密钥 sk_i。可能发生的攻击场景如下，例如在不同的子节点上 2 个客户虚拟机相互串通，企图获得他们的父节点中所使用的密钥，在兄弟节点的一个客户虚拟机和在子节点上另一个客户虚拟机相互串通，攻击父节点等。但是，无论他们是什么样的组合，在本文的 TLKMS 方案中他们的攻击是没有用的。在第一级密钥管理中，外部勾结是毫无意义的，因为所有的 $P(x)$ 是独立的，无论它们是在不同的或相同的节点。这是因为随机数 z 是每次重新选择的。内部攻击如上所述已经被证明是无用的。同样地，在第二级密钥管理中，尝试提取另一子群体的私有群组密钥 k_i，将会违反单向函数的性质，因此是不可能的。

4.3 信息收集攻击

恶意攻击者可能试图搜集许多公开的 $P(x)$，希望通过分析 $P(x)$ 之间的关系来攻破系统。正如上面所讨论的，该手段针对本方案是行不通的，因为所有的 $P(x)$ 是独立的。

总之，本文所提出的 TLKMS 可以很好地防御内部或外部勾结的攻击。

5　实例及仿真

在示例中包含 2 部分：第一部分初始化，用 2 个例子来说明密钥生成、分发、推导过程，并对两级密钥管理方案中多项式的计算复杂度进行了仿真验证；而另一个例子是关于敏感信息访问控制的执行情况。假设大素数是 P=17 和一个单向函数是 $f(x,y)=2^{x\oplus y} \bmod P$。

假设第二级的层次结构设计如图 3 所示。假设节点 6 代表的子群体中有 m 个客户虚拟机。为了更好地说明，以 m=2 个客户虚拟机来说明问题。客户虚拟机 1 自己的密钥为 $sk_1=3$，客户虚拟机 2 自己的密钥为 $sk_2=7$。然后，需要将子群体的密钥分配给这 2 个客户虚拟机（假设 $\hat{k}_6=11$ 并且 $z=5$）。通过等式（1）和（2），可以生成如下多项式

$$\begin{aligned} P(x)\% &= \{A(x)+K\}\%17 \\ &= \{(x-2^{7\oplus 5})(x-2^{3\oplus 5})+11\}\%17 \\ &= x^2+12 \end{aligned} \tag{10}$$

多项式（8）的系数通过数组 {1,0,12} 进行公开。客户虚拟机 1 计算 $H(sk_1,z)=2^{7\oplus 5}=4$ 并且将 4 代入方程(8)得到 $28\%17=11$。客户虚拟机 2 也得到 11。因此，他们两都得到 $\hat{k}_6=11$。假设另一个客户虚拟机 $sk_3=6$ 不在本子群体中，将他的 $H(Sk_3,z)(=48)$ 代入等式(8)中，得到 $48\%17=14$，所以他得不到该密钥。

以上仅仅是一个说明性的例子。在实际用例中，系统的素数 P 是 160 bit。一个子群体中的客户虚拟机的数目 m 也应该是远远超过 2 个，且多项式次数也不只是 3。此外，采用更加安全的单向散列函数。

在本方案中，产生多项式所需计算量最大。选择 GridSim 作为模拟实验平台，该模拟实验平台是个基于 Java 的仿真平台[24]。本质上，Gridsim 是基于 SimJava，SimJava 是一个基于 Java 的离散事件仿真工具，利用多线程模拟各种实体。这很符合云计算的虚拟机的随机性。仿真环境是由 4 台电脑组成，电脑配置为 P43.0 CPU，2GB 内存。图 6 给出了随着子群体数目的增长，产生多项式所耗费的时间。其中图 5 是对图 4 的数据进行拟合后的结果，直接验证了产生多项式耗费的计算量为 $O(m^2)$。

下面给出另外一个例子来说明第二级的密钥的产生和推导，介绍客户虚拟机如何用收到的子群体的保护密钥）来计算子群体私有的群组密钥，以及客户虚拟机如何利用自身的密钥和公开信息来推导出一个子孙节点的私有群组密钥。实例采用猪肉食品安全追溯系统[25]作为实例，每个子群体的相关计算值如图 4 和图 5 所示。

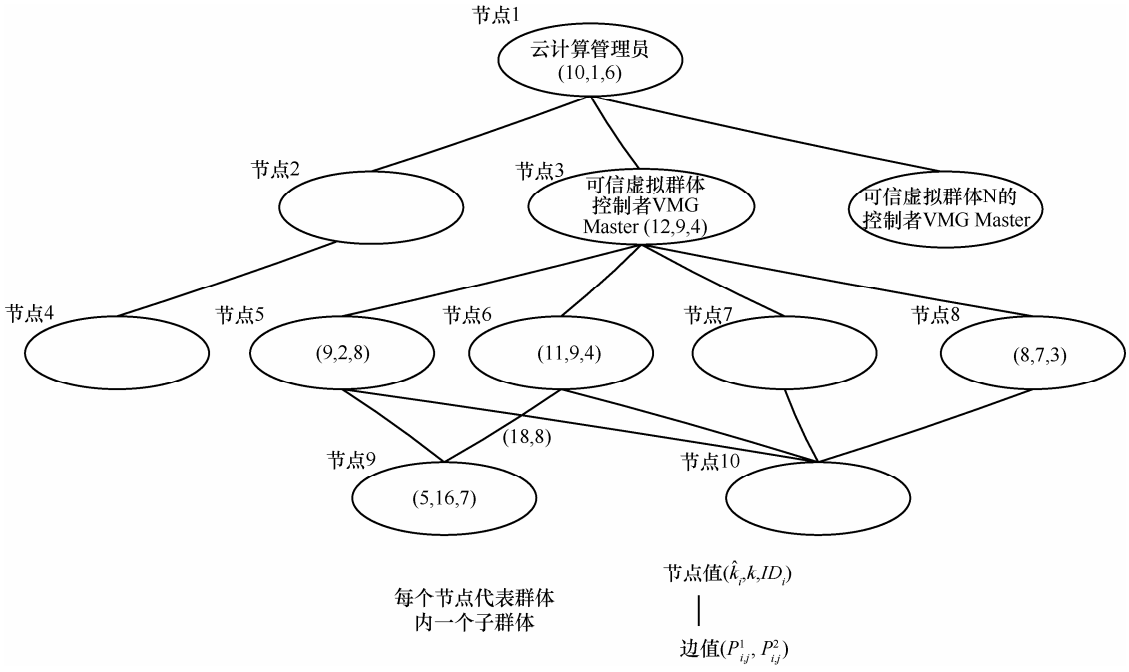


图 3　两级密钥管理实例

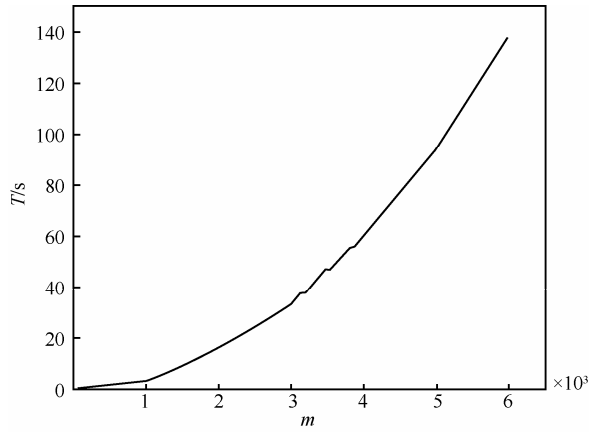


图 4　耗时与子群体数目 m 的关系

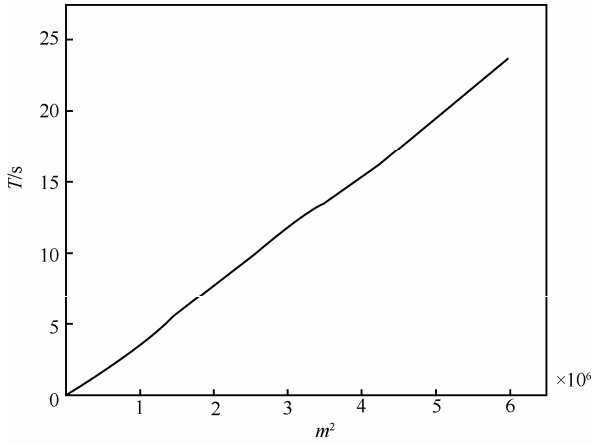


图 5　耗时与子群体数目 m 的平方的关系

假定 $z_6=4$，$\hat{k}_6$ 为 11。节点 9 的 $z_9=7$，保护密钥 $\hat{k}_9=5$。当保护密钥分发给 2 个节点上的客户虚拟机时，子群体 6 使用的私有密钥可以由 2 个客户虚拟机计算得出，$k_6=H(\hat{k}_6,z_6)=2^{11\oplus 4}\%17=9$。类似地，子群体 9 中的每个客户虚拟机可以计算私有密钥 $k_9=H(\hat{k}_9,z_9)=2^{5\oplus 7}\%17=16$。此外，CM-KMS 计算和公开从节点 6 到节点 9 的边值，记 $p^2_{6,9}=ID_9=8$，则 $p^1_{6,9}=k_9\oplus H(k_6,ID_9\oplus p^2_{6,9})=18$。当节点 6 中的任何客户虚拟机想要访问节点 9 中的资源时，他只需要计算 $k_9=p^1_{6,9}\oplus H(k_6,\ ID_9\oplus p^2_{6,9})$ 即可。一旦得到这个子群体私有组密钥，节点 9 中的资源都可以访问。

6　结束语

本文重点讨论可信虚拟群体内虚拟机之间的信息流的访问控制，所采用的是基于密码学的访问控制方法，不但灵活性高而且安全性强，满足了基于虚拟架构的分布式计算环境下，虚拟机群体复杂多变的信息交互需求。实现了群体内不同子群体间以及群体成员间的信息流的隔离和访问控制需求，最后通过实例对基于两级密钥管理的访问控制策略进行了研究，表明该访问控制策略满满足云计算模式下基于虚拟架构的分布式计算环境中的可信虚拟群体内部访问控制要求。

参考文献：

[1] 张兴. 无干扰可信模型及可信平台体系结构实现研究[D]. 解放军信息工程大学, 2009.
ZHANG X. Doctoral Dissertation: Researches on Non-Interference Trusted Model and the Implementation of Trusted Computing Platform Architecture[D]. The PLA Information Engineering University. 2009.

[2] 沈昌祥, 张焕国, 王怀民等. 可信计算的研究与发展[J]. 中国科学, 2010, 40(2):139-166.
SHEN C X. ZHANG H G. WANG H M. *et al*. Research and de-velop-ment on trusted computing[J]. Science China Press, 2010, 40(2):139-166

[3] GONG B, SHEN C X. Behavior Measurement Model Based on Prediction and Control of Trusted Network[C]. China Communications, 2012, 9(5):117-128.

[4] 公备. 支持可信群体构建的可信网络连接架构及关键技术研究[D]. 北京工业大学, 2012.
GONG B. Doctoral Dissertation: Trusted Network Architecture With Support Trusted Group Established and Key Technologies Research[D]. Beijing University of Technology.2012.

[5] 戴汝为, 操龙兵. Internet—一个开放的复杂巨系统[J]. 中国科学, 2003, 33(4):289-296.
DAI R W. CAO L B. Internet—an open complex giant system[J]. Science in China, 2003, 33(4): 289-296.

[6] 张文红, 陈森发. 生态工业系统——一个开放的复杂巨系统[J]. 系统仿真学报, 2004, 16(3):432-440.
ZHANG W H. CHEN S F. Eco-industry—an open giant complex system[J]. Journal of System Simulation, 2004, 16(3):432-440.

[7] 卿斯汉, 刘文清. 操作系统安全[M]. 北京:清华大学出版社, 2004. 8.
QING S H. LIU W Q. Operating System Security[M]. Beijing, Tsinghua University Press, 2004.8.

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

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

[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 security model for operating system[J]. Science in China Ser 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. A new unified security policies between confidentiality and integrity[J]. Computer Engineering and Applica-tions, 2007, 43(34):1-2.

[12] SANDHU R S, COYNE E J, HAL L. *et al*. Role-based aeeess control models[J]. IEEE ComPuter, 1996, 29(2):38-47.

[13] ZAHIR TARI, SHUN-WIJ CHAN A. Role-based access control for intranet security[J]. IEEE Intranet Computing, 1997. 24-25.

[14] FERRAIOLO D F, BARKLEY J F, *et al*. A role based access control model an reference implementation within a corporate[A] ACM Transactions on Information and System Security (TISSEC)[C]. l999.

[15] HARRINGTON A, *et al*. Cryptographic access control in a distributed file system[A]. Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies[C]. Como, Italy, 2003. 158-165.

[16] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06)[C]. New York, NY, USA: ACM, 2006. 89-98.

[17] BONEH D, BOYEN X, GOH E J. Hierarchical identity based encryption with constant size ciphertext[A]. Advances in Cryptology-EUROCRYPT 2005[C]. Berlin, Heidelberg: Springer-Verlag, 2005. 440-456.

[18] ATTRAPADUNG N, IMAI H. Dual-policy attribute based encryption[A]. Proc of the Applied Cryptography and Network Security[C]. Berlin, Heidelberg: Springer-Verlag, 2009. 168-185.

[19] PARNO B, RAYKOVA M, VAIKUNTANATHAN V. How to delegate and verify in public: verifiable computation from attribute-based encryption[A]. TCC 2012[C]. 2012. 422-439.

[20] YAO D F, FAZIO N, DODIS Y, *et al*. Id-Based encryption for complex hierarchies with applications to forward security and broadcast encryption[A]. Proc of the ACM Conf on Computer and Communications Security[C]. New York: ACM Press, 2004. 354-363.

[21] LIN C H. Dynamic key management scheme for access control in a hierarchy[J]. Computer Communications 1997, 20(15):1381-1385.

[22] BLUNDO C, SANTIS A D, HERZBERG A, *et al*. Perfect secure key distribution for dynamic conferences[A]. Advances in Cryptology, CRYPTO’92[C]. Springer, Berlin, 1993. 471-486.

[23] BLUNDO C, MATTOS L A F, STINSON D R. Generalised beimelchor scheme for broadcast encryption and interactive key distribution[A]. Theoretical Computer Science 200[C]. 1998. 313-334.

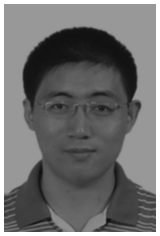
[24] BUYYA R, MURSHED M. GridSim: a toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing[J]. Journal of concurrency and computation practice and experience, 2002, 14(13-15):1175-1220.

[25] 梁鹏等. 肉类食品安全追溯系统的可信体系结构[J]. 网络安全技术与应用, 2010. 8.
LIANG P, *et al*. Meat food traceability system for reliable architecture[J]. Network Security, Technology & Application, 2010.8.

作者简介：

梁鹏（1985-），男，山西长治人，北京工业大学北京市可信计算重点实验室博士，主要研究方向为可信计算，信息安全，预测控制论，云计算及应用数学等。

沈昌祥（1940-），男，浙江奉化人，中国工程院院士，北京工业大学博士生导师、主要研究方向为计算机信息系统，密码学，信息安全体系结构，系统软件安全（安全操作系统，数据库等）和网络安全等。



宁振虎（1983-），男，河北邯郸人，北京工业大学博士生，主要研究方向为可信计算、密码学、信息安全体系结构、应用数学、云计算及物联网安全等。