云环境下基于BN模型的虚拟机安全部署模型

孙 磊 杨 星 马自堂
(解放军信息工程大学电子技术学院 郑州 450004)

摘 要 针对云计算环境下多用户共享硬件资源带来的安全风险,提出了虚拟机安全部署模型CVDBN,基于BN模型设计了安全部署规则,以满足云计算环境下利益冲突用户对于虚拟机部署的安全隔离需求。最后设计了虚拟机安全部署模块和安全部署算法。仿真实验结果证明了该模型和算法的有效性和可用性。

关键词 云计算,安全,虚拟机,BN模型,利益冲突,服务器安全禁忌列表
中图法分类号 TP309 **文献标识码** A

BN Model Based Virtual Machine Security Deployment Policy in Cloud Computing

SUN Lei YANG Xing MA Zi-tang
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract CVDBN security deployment model of virtual machine was proposed in allusion to security risk caused by multiple consumers' sharing hardware resource in the environment of cloud computing and the security rules of subject server to deploy the object virtual machines were designed based on BN model, which can meet users' isolation requirement on deployment of virtual machines with interest conflict. In the end, the security module of deploying virtual machines and the security algorithm of deploying virtual machines were designed. Simulation was conducted which demonstrates the effectiveness and availability of the model and algorithm proposed in this context.

Keywords Cloud computing, Security, Virtual machine, BN model, Conflict of interest, Security taboo list of servers

云计算具有广泛的应用前景,但由于面临着严峻的信息安全挑战,云计算的安全问题已成为阻碍云计算技术发展的一个关键因素[1]。

云环境尤其是公有云环境是一个多租户的计算资源租借代理平台,不可避免的是提供商往往需要同时为多个具有利益冲突关系的用户(如同行业的企业)提供服务。利益冲突(conflict of interest,COI)是一个商业上的概念,在维基百科有如下解释:当某个个人或组织代理业务涉及到了多个利益方,而其所包含的一个利益方的行动可能会危害到其他某个利益方时,就存在了利益冲突。

如今在解决商业界存在的利益冲突问题时,一般会采用中国墙安全模型(Chinese Wall Security Policy,简称BN模型)[2]。BN模型是一种类似于BLP(Bell Lapudula)模型[3]的多级强制安全策略模型,BN模型既继承了BLP模型的保密性策略,又承接了Biba模型[4]的完整性策略。

在云计算环境下,为了解决利益冲突用户间的安全问题,基于BN模型进行了大量研究。Brian Hay等在文献[5]中对IaaS中虚拟机资源共享安全问题进行了详细的分析,提出了云计算环境下存在利益冲突用户的特点,并建议使用BN模型解决云计算环境下资源共享带来的安全威胁问题。Ruoyu Wu等[6]提出了一种基于BN模型的云计算虚拟机间信息流控制模型,其通过定义利益冲突类,对属于冲突类中各个利益集之间的虚拟机的访问权限进行隔离限制,以避免具有利益冲突关系的用户非法窃取对方的机密信息。林果园等[7]为了保护云端服务器利益冲突用户间敏感数据安全性和保密性,提出了一种适用于云计算环境的BN模型,并给出了模型在云环境中的配置方案。

但现阶段对于利益冲突用户安全的研究主要是在信息流控制层次上。虚拟机的使用为云计算带来了一些新的安全威胁[8,9]。Thomas Ristenpart等在文献[10]提出了在IaaS环境中由于共享物理硬件造成的安全威胁,在亚马逊的EC2云计算环境下,通过发现攻击目标虚拟机位置并在其同一服务器上建立新的虚拟机,实现了使用隐蔽通道的恶意攻击,证明了利益冲突用户间在虚拟机部署阶段安全威胁的存在。因而为了满足虚拟机部署阶段利益冲突用户对于虚拟机隔离的安全需求,本文基于BN模型设计了一种CVDBN虚拟机安全部署模型。

1 CVDBN模型构建

在CVDBN模型中将云计算数据组织结构分为3个层次,这样的结构对于CVDBN模型是非常重要的,是模型安全策略设计的基础,如图1所示。

1) 最底层:客体(object),即独立的虚拟机实体,每一个虚拟机都属于并仅属于一个组织虚拟机集,虚拟机是计算任

到稿日期:2012-05-29 返修日期:2012-09-09 本文受武器装备预研重点基金项目(9140A15060311JB5201)资助。
孙 磊(1973-),男,博士,副研究员,主要研究方向为云计算基础设施可信增强、可信虚拟化技术,E-mail:13523556215@139.com;杨 星(1986-),男,硕士生,主要研究方向为云计算、系统优化;马自堂(1962-),男,教授,主要研究方向为信息安全、密码系统工程。

务和数据的载体；

2）中间层：组织虚拟机集（organization virtual machines set，OVM），由所有属于该组织的虚拟机所构成；

3）最高层：利益冲突类（conflict of interest classes，COI），是所有具有利益冲突关系的组织虚拟机集组成的集合。

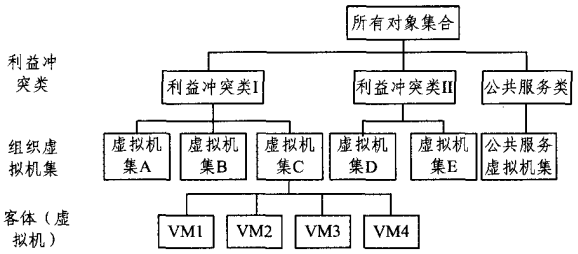

图1　云计算数据组织结构层次图

确定客体之间关系的是客体所属于的组织虚拟机集和组织虚拟机集所属于的利益冲突类。利益冲突类可以按照证券交易所列出的商业领域划分（如石化产业、银行等），组织虚拟机集可以按照不同行业所包含的公司企业划分。为了更加形象地说明，假设一个云计算系统包括4个企业用户，分别为银行A、银行B、石油公司A和石油公司B，会得出以下结论：

1. 云计算环境中的虚拟机可以属于4个公司中的某一个（即虚拟机的组织虚拟机集可以为银行A、银行B、石油公司A和石油公司B）；

2. 此系统中包涵两个利益冲突类，一个是银行（由银行A虚拟机集和银行B虚拟机集组成），一个是石油公司（由石油公司A和石油公司B组成）。因此虚拟机将属于银行利益冲突类和石油公司利益冲突类之一。

CVDBN模型和BN模型具有相同的思想，即设定了一个面虚拟的“墙”，通过制定相应的安全部署规则，使“墙”一面的物理服务器不能部署“墙”另一面的虚拟机。但为了提供系统可用性，与BN模型不同，决定服务器安全标签的是服务器现阶段所部署的虚拟机，而不是服务器曾经部署过的虚拟机。

以上文假设为列，4个公司在云计算系统中的部署状况如图2所示。

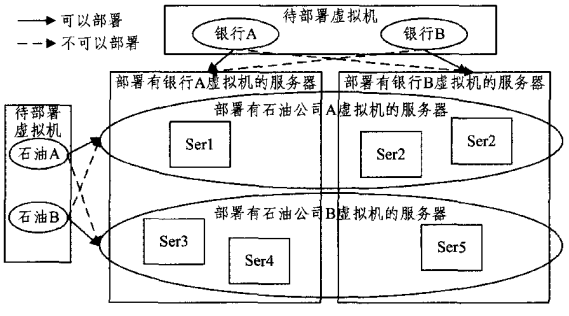

图2　服务器利益冲突类划分

在图2中，部署过同一利益冲突类中虚拟机的服务器被按照不同组织虚拟机集划分为几个并行的集合。初始时，一个服务器可以部署任何虚拟机。但其一旦部署过虚拟机之后，便会产生一面墙，在进行新的虚拟机部署时，不能再部署与该虚拟机具有相同利益冲突类但不同组织虚拟机集的虚拟机。不同利益冲突类间的虚拟机可以部署在同一台服务器上。如银行A的待部署虚拟机不能部署在已部署过银行B虚拟机的服务器Ser2上，但银行A的虚拟机和石油A的虚拟机可以同时被部署在服务器Ser1上。

2　CVDBN形式化模型

2.1　CVDBN模型元素定义

在CVDBN模型中，主要包括客体、主体、部署操作和安全标签4个元素，分别定义如下：

定义1（客体集合O）　是指待部署的虚拟机集合。$O=(o_1,\cdots,o_n)$，其中o_i代表一个待部署的虚拟机。

定义2（主体集合S）　是指虚拟机的载体集合。在云计算系统中，虚拟机载体是物理服务器。$S=(s_1,\cdots,s_n)$，其中s_i代表一台物理服务器。

定义3（部署操作$DEP(i,j)$）　将客体虚拟机o_j部署在主体服务器s_i的操作。

定义4（安全标签）　主要用于定义客体所属的组织虚拟机集合与利益冲突类，L是一个安全标签集(x,y)，其中x代表利益冲突类，y代表组织虚拟机集，每一个客体都配有一组安全标签集。引入函数$X(o)$和$Y(o)$来表示将标签(x,y)赋予某一指定客体。

为了方便表述，下文将x_i、y_i分别表示为$X(o_i)$和$Y(o_i)$，对于一个客体o_i，x_i是它的安全冲突类，y_i是它的组织虚拟机集合。

为了描述主体服务器已经部署的客体虚拟机状态，给出了一个新的定义——部署状态矩阵N。

定义5（部署状态矩阵N）　它是一个布尔型矩阵，由对应于$S\times O$中元素的函数$N(i,j)$构成，当$N(i,j)$值为真（True）时，表示主体s_i已经部署了客体o_j；当为假（False）时，表示还未部署。当新的部署操作$DEP(i,j)$被执行后，相应$N(i,j)$的值要变为真。因而每一个操作$DEP(i,j)$被成功执行，都要对N进行一次刷新。

2.2　安全放置策略制定

在完成对于模型元素的定义后，本节将制定虚拟机部署安全规则。

安全规则的制定都是基于一个基本公理的，该公理如下所述。

公理1　$y_i=y_j\rightarrow x_i=x_j$

对于任意客体o_i和o_j，如果它们属于同一个组织虚拟机集合，那么它们也属于同一个利益冲突集合。其逆否命题如下：

推论1　$x_i\neq x_j\rightarrow y_i\neq y_j$

对于任意客体o_i和o_j，如果它们不属于同一个利益冲突集合，那么它们一定不属于同一个组织虚拟机集合。

在有了上述基本公理后，模型制定了另一个关键的公理，即CVDBN模型的简单安全规则，见公理2。

公理2　主体s_i可以部署客体o_j，当且仅当所有$N(i,r)$为真所对应的客体o_r（即，s_i已部署的客体o_r）满足如下条件：

$x_j\neq x_r\vee y_j=y_r$

客体虚拟机只能部署在没有部署过与其有相同利益冲突类标签的虚拟机，或部署过与其有相同组织虚拟机集标签虚拟机的主体服务器上。该公理可以理解为模型的核心公理，是虚拟机安全部署的基本原则。

实现该安全规则的一个最极端的状态便是服务器还未部

署过任何虚拟机，在 CVDBN 模型中将其定义为初始部署状态。

定义 6(初始部署状态) $\forall o_j \in O, N(r,j)=\text{False}$，即主体 s_r 未部署任何客体，称为主体初始部署状态。

在初始部署状态下的服务器允许部署任何组织虚拟机集的虚拟机，如公理 3 所述。

公理 3 当主体 s_r 处于初始部署状态时，所有 $DEP(r,j)$ 操作都是被允许的。

在以上重要公理基础上，可以推导出下述两个关键的定理，进一步对安全部署规则进行描述。

定理 1 假设主体 s_i 部署过客体 o_j，即 $N(i,j)=1$，则 s_i 只能再部署满足 $x_j \neq x_r \vee y_j = y_r$ 的其他客体 o_r。

证明：使用反证法。假设这个命题是错误的，那么该主体 s_i 可以部署 $x_j = x_r \wedge y_j \neq y_r$ 的其他客体 o_r。也就是说：

$$N(i,j)=1 \wedge N(i,r)=1 \wedge x_j = x_r \wedge y_j \neq y_r$$

主体 s_i 先部署了客体 o_j，那么主体可以部署客体 o_r 时，根据公理 2，有 $x_j \neq x_r \vee y_j = y_r$，从而得出：

$$(x_j \neq x_r \vee y_j = y_r) \wedge (x_j = x_r \wedge y_j \neq y_r)$$

即：

$$(x_j \neq x_r \wedge x_j = x_r \wedge y_j \neq y_r) \vee (y_j = y_r \wedge x_j = x_r \wedge y_j \neq y_r)$$

是恒为假命题，因而与假设矛盾，原命题为真，证毕。

根据定理 1 还可以推出另外一个重要的定理。

定理 2 一个主体最多只能部署同一利益冲突类中的一个组织虚拟机集的虚拟机。

2.3 公共服务类

在云计算系统中，其所包涵的服务类型是多样的，即需要为用户提供私有服务，同时也需要一些不涉及到私有信息安全的公共服务，以对这些私有服务进行支持，减少服务的冗余建设。因而需要部署的虚拟机也不全是面向单独某个用户的，为此制定一个特殊的利益冲突类——公共服务类，记为 y_0。其类似于传统 BN 模型中的洁净信息(主体对洁净信息的访问历史不会改变主体对于其他客体的访问规则)，对于这些虚拟机的部署给出了如下的规则。

定义 7 对于任意客体 o_j，

(1) $y_j = y_0$，则 o_j 是公共服务虚拟机；

(2) $y_j \neq y_0$，则 o_j 是组织私有的虚拟机。

公理 4 $x_0 \leftrightarrow y_0$

如果一个客体被赋予了安全标签 y_0，那么它将同时拥有安全标签 x_0，从而可以得出以下定理。

定理 3 公共服务虚拟机可以部署在任何主体服务器上。

证明：1. 当主体 s_i 部署过 $y_j = y_0$ 的客体 o_j 时，该主体已经部署了与公共服务虚拟机具有相同组织虚拟机集标签的虚拟机，根据公理 2，公共服务虚拟机可以部署在该主体服务器上。

2. 当主体 s_i 未部署过 $y_j = y_0$ 的客体 o_j 时，根据公理 4，该主体未部署过利益冲突类标签为 x_0 的客体，根据公理 2，公共服务虚拟机可以部署在该主体服务器上。

与单节点下的运行互斥规则一样，本模型并不实现原始 BN 模型的 *-安全特性，因为如果使用 *-特性，那么即使两个组织虚拟机集 A 和 B 不属于同一利益冲突类，一旦其中组织虚拟机集 A 的某一虚拟机和组织虚拟机集 C 的虚拟机部署在同一物理服务器上，如果 C 和 B 属于同一利益冲突类，组织虚拟机集 A 的虚拟机将无法再和组织虚拟机集 B 的虚拟机部署在同一物理服务器上，这样最终会导致每个公司都独立使用单独的物理服务器的结果。

3 云计算环境下 CVDBN 模型的应用

为了保障虚拟机部署阶段的安全，在虚拟机部署服务器中设计安全部署模块。安全部署模块的作用主要是管理待部署虚拟机和服务器的安全标签，以及通过 CVDBN 的安全放置规则生成每个待部署虚拟机的不能被部署的服务器安全禁忌列表。

3.1 虚拟机安全部署模块设计

云计算环境下虚拟机安全部署模块设计采用星状模式，可以分为中心安全部署模块(Central Security Deployment Module，CSDM)和节点安全标签管理模块(Local Security Label Management Module，LSMM)两部分。其实现框架如图 3 所示。

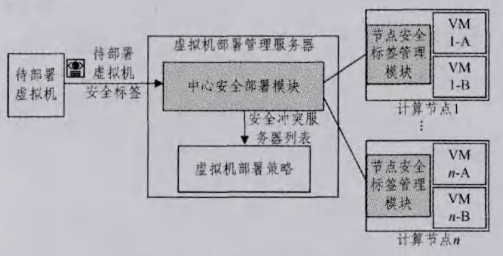

图 3 安全部署模块实现框架

节点安全标签管理模块位于云计算数据中心各个计算节点服务器中，其作用是管理本地服务器上已部署虚拟机的安全标签，并在本地安全标签发生更改后，向中心安全部署模块发送更改信息。中心安全部署模块位于云计算虚拟机部署管理服务器内，其中存储了云计算系统虚拟机安全部署策略以及各个计算节点安全标签状况，主要作用是为虚拟机部署决策提供安全约束。其输入是待部署虚拟机的安全标签，输出是与待部署虚拟机具有安全冲突的服务器列表，待部署虚拟机不允许被部署到列表中的服务器上。虚拟机安全部署模块的具体设计如图 4 所示。

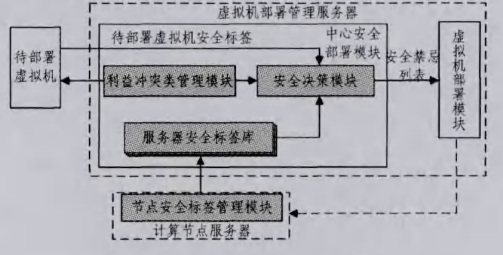

图 4 虚拟机安全部署模块结构

中心安全部署模块主要由 3 部分构成：安全决策模块(Security Decision Module，SDM)、利益冲突类管理模块(Conflict of Interest Classes Management Module，COIMM)和服务器安全标签库(Server Security Label Base，SSLB)。

(1)安全决策模块(SDM)

安全决策模块是执行 CVDBN 安全部署模型中安全部署规则的核心，负责生成虚拟机的安全冲突服务器列表，其具体实现流程将在下一节进行详细介绍，在此不做累述。

(2)利益冲突类管理模块(COIMM)

利益冲突类管理模块管理着云计算系统中所包含的安全标签,包括利益冲突类标签集和组织虚拟机集标签以及它们的组织关系,主要负责为用户发放安全标签,以及管理安全标签的注册变更。安全标签存放在一个按照云计算信息层次组织结构以及公理 1 设计的 XML 格式的文件中,如下所示。

```
〈ConflictClasses〉
    〈Conflict name="Com1"〉
  〈Type〉Com-A〈/Type〉
  〈Type〉Com-B〈/Type〉
〈/Conflict〉
〈Conflict name="Com2"〉
  〈Type〉Com-C〈/Type〉
〈/Conflict〉
……
〈/ConflictClasses〉
```

在上述例子中,定义了两个利益冲突类 Com1 和 Com2:Com1 下有 Com-A、Com-B 两个组织虚拟机集,Com2 下有 Com-C 一个组织虚拟机集。一个组织虚拟机集不能同时属于两个不同的利益冲突类。

同时按照定义 7,添加利益冲突类 Public 作为公共服务类,属于公共服务类的虚拟机会被打上 Public 的标签,利益冲突类格式如下所示。

```
〈Conflict name="Public"〉
  〈Type〉Public〈/Type〉
〈/Conflict〉
```

(3)服务器安全标签库(SSLB)

虚拟机安全部署模块的另一个关键部分是服务器安全标签库,其主要功能是记录每个计算节点服务器上已部署虚拟机的安全标签情况。该模块与节点安全标签管理模块(LSMM)直接进行通讯,实时获得各个计算节点的虚拟机部署状况信息。服务器安全标签列表会根据节点安全标签管理模块变动而刷新。

服务器安全标签库是安全决策模块(SDM)的一个输入,SDM 在做安全决策时,会向 SSLB 调取服务器池中各个节点的安全标签情况,然后将待部署虚拟机与各个服务器轮流进行安全匹配,生成与该虚拟机有安全冲突的服务器列表。

虚拟机安全部署模块的主要工作流程如图 5 所示。

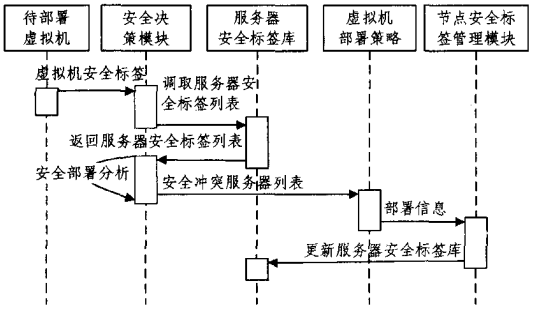

图 5　虚拟机安全部署模块工作时序图

1. 用户提交虚拟机安全标签

根据用户身份向云计算系统提交待部署虚拟机的安全标签。对于用户所能使用的标签,系统应该设置严格的身份认证和权限管理机制,防止用户假冒攻击。

2. 调取服务器安全标签列表

查询最新的服务器安全标签列表,以获得各台服务器已部署虚拟机的安全标签状况。

3. 生成安全冲突服务器列表

通过 CVDBN 安全规则,筛选出与该待部署虚拟机有安全冲突的服务器,将这些服务器生成列表。

4. 提交服务器安全冲突服务器列表

向虚拟机部署决策模块提交生成的安全冲突服务器列表,为最终部署方案的确定提供安全限制。

5. 更新服务器安全标签库

在每一次完成部署任务之后,对服务器安全标签库进行更新。

3.2　虚拟机安全部署算法

为了安全部署规则在安全决策模块中的实现,本节将设计一个安全部署规则判断算法,算法具体步骤如下:

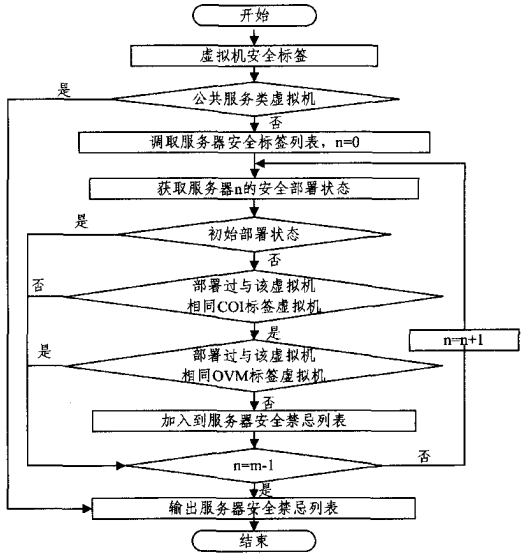

图 6　服务器安全禁忌列表生成流程图

1)用户提交虚拟机安全标签。根据用户身份向云计算系统提交待部署虚拟机的安全标签。对于用户所能使用的标签系统,应该设置严格的身份认证和权限管理机制,防止用户假冒攻击。

2)首先判断该虚拟机是否为公共服务类虚拟机,若是,则跳转到步骤 10)。

3)调取服务器安全标签列表。列表中具有 m 个服务器,服务器 ID 为$(0,2,\cdots,m-1)$,初始化 $n=0$。

4)获取第 n 个服务器的安全部署状态,即其所具有的安全标签。

5)判断该服务器是否为初始部署状态,若是,跳转至步骤 9)。

6)判断该服务器是否部署过与该虚拟机有相同 COI 标签的虚拟机,若否,跳转至步骤 9)。

7)判断该服务器是否部署过与该虚拟机有相同 OVM 标签的虚拟机,若是,跳转至步骤 9)。

8)将该服务器加入到服务器安全禁忌列表。

9)判断 n 是否等于 $m-1$,若否,$n=n+1$,跳转至步骤 4)。

10)当 $n=m-1$ 时,退出循环,输出该虚拟机的服务器安全禁忌列表。

服务器安全禁忌列表生成流程图如图 6 所示。

4 仿真试验与分析

4.1 仿真平台 CloudSim 简介

本文采用澳大利亚墨尔本大学的网格实验室和 Gridbus 项目提出的云仿真平台 CloudSim 作为试验仿真工具，使用版本为 CloudSim-2.1.1。CloudSim 是一个可扩展的仿真工具集，可实现云计算系统和应用环境的模拟与仿真。CloudSim 为研究者提供了可控且易于安装的测试环境，摆脱了复杂的测试环境搭建过程和对于庞大基础设施的依赖。CloudSim 在对云计算仿真时具有以下特点：(1)支持在一个物理节点上模拟和仿真包含数据中心的大规模云计算环境；(2)为模拟云计算环境下虚拟机部署、服务代理、服务分配策略等提供了独立的仿真平台；(3)支持模拟仿真云计算环境中各个组件的网络连接；(4)可以仿真私有云和公共云联合环境。

添加安全部署策略的虚拟机批量部署算法仿真分析。

为了验证添加安全策略后虚拟机部署算法的可行性和系统性能状况，设计系统具有 3 个利益冲突类和 1 个公共服务类，如下所示：

利益冲突类 1={组织虚拟机集 11、组织虚拟机集 12、组织虚拟机集 13}

利益冲突类 2={组织虚拟机集 21、组织虚拟机集 22}

利益冲突类 3={组织虚拟机集 31、组织虚拟机集 32}

公共服务类 0={组织虚拟机集 0}

服务器均视为处于初始部署状态，即各个虚拟机安全禁忌列表均为空。分别为待部署虚拟机打上安全标签，如表 1 所列。

表 1 虚拟机安全标签

利益冲突类 1			利益冲突类 2		利益冲突类 3		公共服务类 0
11	12	13	21	22	31	32	0
vm10	vm13	vm2	vm0	vm4	vm8	vm1	vm9
vm12		vm5	vm7	vm23	vm24	vm3	vm11
		vm6	vm19			vm17	vm15
		vm16	vm20			vm14	vm18
							vm21
							vm22

单个节点上，不同性能间的负载均衡情况是资源利用率的一个重要影响因素。为了更直观地比较系统整体的负载均衡效果，取负载均衡因子 LB 作为系统状态衡量标准，将带安全策略的蚁群算法和不带安全策略的蚁群算法在虚拟机批量部署中的实验进行比较。负载均衡因子算法为：

$$LB.Res=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(Uti_i.Res-SysUti.Res)^2}$$

式中，Res 为服务的某一性能指标(如 CPU、内存等)，$Uti_i.Res$ 为服务器 i 的 Res 利用率，$SysUti.Res$ 为系统总的 Res 利用率，n 为服务器台数。负载因子越小，说明各个节点间的负载越平均，负载均衡效果越好。进行 50 次实验，求平均值，试验结果如图 7 所示。

可以看出，使用基于 CVDBN 安全策略的蚁群算法比不带安全策略的蚁群算法在负载均衡性能方面有少许的下降，但是其下降的幅度在接受范围之内，不破坏系统的可用性。

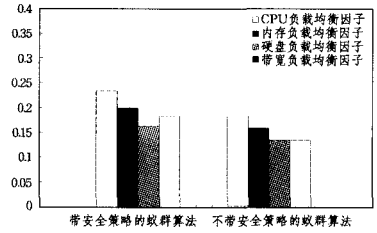

图 7 使用安全策略算法性能比较

结束语 本文在云计算系统在虚拟机部署阶段的安全需求分析基础上，针对虚拟机部署安全问题，基于 BN 模型设计了云计算环境下虚拟机安全部署模型 CVDBN，给出了其详细的形式化模型和公理；并给出了云计算环境下虚拟机安全部署模块的详细设计与服务器安全禁忌列表生成策略，通过仿真试验证明了安全模型的实用性。

参 考 文 献

[1] 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

[2] Brewer D F C，Nash M J. The Chinese Wall Security Policy[C]// Proceedings of the 1989 IEEE Symposium on Security and Privacy. Oakland，CA，USA，1989

[3] Bell D E，LaPadula L. Secure Computer System：Unified Exposition and Multics Interpretation[R]. ESD-TR-75-306. Electronics Systems Division，AFSC，Hanscom AF Base，Bedford MA，1976

[4] Biba K. Integrity Considerations for Secure Computer System [R]. MTR-3153. The MITRE Corporation，Bedford，MA，1977

[5] Hay B，Nance K，Bishop M. Storm Clouds Rising：Security Challenges for IaaS Cloud Computing[C]// Proceedings of the 44th Hawaii International Conference on System Sciences. Hawaii，US，2011

[6] Wu Ruo-yu，Ahnl G-J，Hul Hong-xin，et al. Information Flow Control In Cloud Computing[C]// Collaborative Computing：Networking，Applications and Worksharing. Chicago，Illinois，USA，2010

[7] 林果园，贺珊. 一种云计算环境下的安全模型[J]. 电信科学，2010，26(9)

[8] 朱鸿伟. 虚拟化安全关键技术研究[D]. 杭州：浙江大学，2008

[9] Reuben J S. A Survey on Virtual Machine Security[Z]. Seminar on Network Security

[10] Ristenpart T，Tromer E，Shacham H，et al. Get Off of My Cloud：Exploring Information Leakage in Third-Party Compute Clouds[C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago，Illinois，USA，November 2009

(上接第 174 页)

[11] Heine G. GPRS-signaling & protocol analysis[M]. Inacon，2002

[12] Toh C-K. Associativity based routing for ad hoc mobile networks[J]. Wirel. Pers. Commun. Special Issue Mobile Networking Computing Systems，1997，4(2)：103-139

[13] Johnson D B，Maltz D A，Hu Y-C. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)，July 2004，IETF MANET Working Group. Internet Draft

[14] Sakhaee E，Taleb T，Jamalipour A，et al. A novel scheme to reduce control overhead and increase link duration in highly mobile ad-hoc networks[C]// Proc. WCNC. Hong Kong，Mar. 2007：3972-3977