第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

多租户环境下基于可信第三方的云安全模型研究

王佩雪[1] 周华强[2]

(中原工学院计算机学院 郑州 450007)[1] (中原工学院理学院 郑州 450007)[2]

摘 要 针对云计算中多租户环境特点,将可信第三方引入云计算的安全解决方案中,提出了一种新型的基于可信第三方的云安全模型。在该模型基础上,讨论了认证协议,并设计了基于TTP的多租户资源分配算法。采用CloudSim模拟工具进行仿真实验和性能比较分析,将短任务先行策略、先来先服务策略与本策略在资源成功执行率方面进行比较。实验结果表明,该模型能将可信度最高的云节点资源提供给云用户,有效构建了实体之间的信任网,可验证数据的正确性和数据交换的正确性,提供了多层次、分布式环境下端对端的安全服务。

关键词 云计算,多租户,可信第三方,云安全

中图法分类号 TP393 **文献标识码** A

Research on Cloud Security Model Based on Trusted Third Party on Multi-tenant Environment

WANG Pei-xue[1] ZHOU Hua-qiang[2]

(College of Computer Science, Zhongyuan University of Technology, Zhengzhou 450007, China)[1]

(College of Science, Zhongyuan University of Technology, Zhengzhou 450007, China)[2]

Abstract Aiming at multi-tenant environments for cloud computing, introducing the trusted third party is into cloud security solutions, this paper proposed a new cloud security model based on trusted third party. Then we designed the authentication protocol and a multi-tenant resource allocation algorithm based on TTP. Finally, the CloudSim simulation tools were used for simulation and performance analysis, and Short Jobs First strategy, First-come First-served policy were compared with TTP strategy in successful implementation rate of resources. The experimental results show that the model provides the highest credibility cloud node resources to cloud users, builds a trust web between entities effectively, verifies the correctness of the data and the correctness of the data exchange, and provides a multi-level, end-to-end security services in the distributed environment.

Keywords Cloud computing, Multi-tenant, Trusted third party, Cloud security

云计算的出现,大大改变了人们对基础设施架构、软件交付和发展模式的看法[1]。在云市场条件下,云资源被视为商品,供应商生产商品并将其分租给消费者,多租户可以在全球范围内根据自己的需求按照一定的付费方式通过经纪人从供应商中购买商品[2]。云计算概念有别于客户端那样的传统网络的拓扑结构,它能够缓解网路的数据拥堵问题,其管理层能够监测数据的网络运作情况,实现了安全监控和管理。随着信息技术的快速发展,从安全角度来看,传统机械装置保护的有效性不断减弱,云计算概念面临着许多风险的挑战。尤其是多租户的多任务,对用户的隐私和密码造成了威胁,对象的可重用性是云计算设施的一个重要特点,但可重复使用的对象必须仔细控制,以免它们产生严重的漏洞。

本文首先介绍了多租户、虚拟化、信任的相关知识,阐述了可信第三方的概念、安全域、密钥,然后提出了一种新型的基于可信第三方的云安全模型,设计了认证协议、新的资源管理算法,最后将短任务先行策略、先来先服务策略与本策略进行资源成功执行率比较,采用CloudSim模拟工具进行仿真实验。结果证明该模型可以解决传统安全领域的弊端,提供多层次、分布式环境下端对端的安全服务,有效提高资源分配的效率、可信度。

1 相关知识

1.1 多租户

云系统结构,是一种生产者——消费者模型,计算资源可作为商品进行流通,多个计算云、存储云抽象为资源提供者,云用户被视为资源的消费者。现实环境中出现多个租户(用户)共享云资源的情况,虽然用户被隔离在一个虚拟的水平,但是硬件是不分开的。随着多租户架构的形成,应用软件在分区的数据和配置中被设计出来,以便能使每一个客户都可以使用一个虚拟的工程定制应用程序实例。

论文提出了多租户云资源管理架构,如图1所示[3]。供应商给出价格制定机制,主要根据用户需求、资源利用现状、市场条件来制定当前资源价格。经纪人通过从供应商中购买资源并将其分租给消费者,来协调多租户和供应商之间的价格,经纪人可以接收来自许多用户的请求。经纪人含有谈判模型,此模型根据资源的当前条件和当前需求做出决定[4]。

本文受河南省软科学(122400450154)资助。

王佩雪(1979—),女,硕士,讲师,主要研究方向为计算机基础教学工作;周华强(1979—),硕士,讲师,主要研究方向为计算机基础教育。

多租户的多任务对用户的隐私和密码造成了一定威胁，此模型存在一定的安全漏洞。

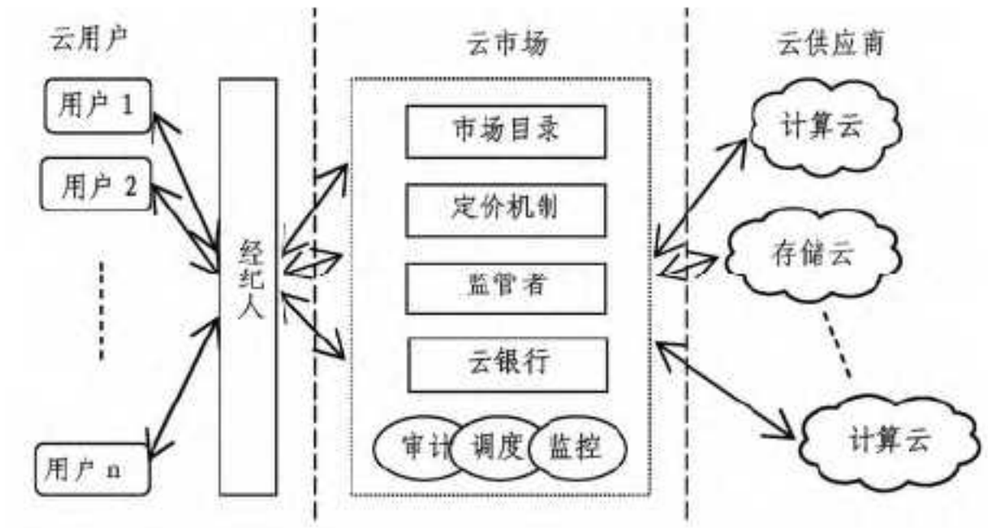

图 1　多租户云资源管理架构

1.2　虚拟化

虚拟化技术是云计算的重要特征之一，云计算利用虚拟化最大限度地提高了终端机的计算能力。虚拟化技术可通过分离逻辑与物理概念来解决云计算所面临的诸多难题。虚拟化需要一个动态数据服务中心，其由许多数据服务器组成，服务器提供一个可根据需要使用资源的资源池。多个虚拟机可将在同一物理机上资源的不同分区配置到服务请求的不同要求上面，可在单一的物理机上动态地被启动或停止，为应用程序提供了最大限度的灵活性。

在硬件设施的水平上，许多设置在数据中心的设备，包括处理器、硬盘驱动器和网络设备，不受其在电脑中位置的影响，这满足了存储和处理的需要。在此基础上，软件层、虚拟层和管理层的结合保证了用户对服务器的有效操作。虚拟化是云计算得以实现的关键因素，它提供了独立地址和资源共享平台，能对输入数据做出快速的反应。

1.3　信任

在计算机科学领域中信任涵盖了安全性和访问控制等计算机网络的众多领域，如：分布式系统的可靠性、博弈论和代理系统，以及在不确定情况中的决策定位。

在双方交易的前提条件下，可以对信任的概念作如下描述："当实体 A 认为实体 B 将会完全按照自己的期望和要求运作时，我们称实体 A 信任实体 B"[5]。如果当事人或在交易中涉及的人依赖于它的实体信誉，这个实体可以被视为值得信赖。一个组织的可信任程度可以描述为：消费者相信该组织有能力准确无误地满足消费者的各种需求，也可以表述为客户对其道德操守、运作的稳健性、机制的安全有效性的信赖，以及在该组织专业知识层次的掌握、运作过程的合法性、安全性方面的信赖。

2　可信第三方

2.1　概念

云计算环境属于独立的行政实体域，TTP(trusted third party)是一个在分布式云计算环境下的理想的安全协调员，引入一个可信的第三方可以解决传统安全领域的亏损，降低危险因素。主体可通过可信第三方交换消息，保证实现各种安全目标，例如原子性、非否认性、可追究性、公平性、隐私性等。主体相信公证中心能提供正确的证据，并为他们验证数据的正确性和数据交换的正确性[6]。

将可信第三方引入云计算，如图 2 所示，使用加密来确保数据的保密性、完整性和真实性及沟通的权威性，并尝试修补特定的安全漏洞。依赖方客户信任 TTP 的安全并支持它应该提供所有交易。TTP 基于标准与领域、地理区域和特殊用途，其不同范围内的信息系统可提供端对端的解决方案，这是可扩展的端到端的安全服务，TTP 的本质是授权一个受信任的权威来解决在多层次的分布式环境下的许多安全方面的问题[7]。

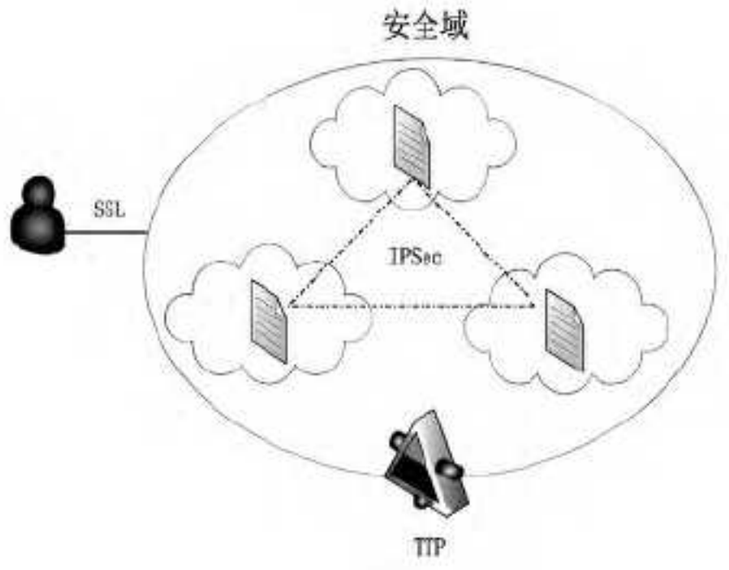

图 2　可信第三方

2.2　安全域

在云计算中，一个 TTP 的任务是确保特定的数据安全，同时在相关实体之间构建起云计算安全信誉网，将公钥加密、单点登录技术和 LDAP 目录结合起来，能对相关联的实体进行安全的识别和验证。

受信任的第三方的可依赖性表现在如下方面：高、低层次上的保密性；服务器和客户端身份验证；安全域生成____服务供应商的证书用来对所有的连接进行安全加密，通过其与个人证书的结合，用户可以使用云计算服务对自己进行验证；分离加密的数据；基于授权的证书。

2.3　密钥

密钥管理是云计算基础设施的一个关键性问题，因为传统的保护机制被禁用，虚拟化的服务就掩盖了对物理密钥的存储位置的鉴定过程。原则上密钥的存储和保护主要是在硬件基础设施的水平上。特别是关键的公共基础设施需要密码，以确保认证的完整性以及相关数据和连接的机密性[5]。

公钥基础设施能够实现 IPSec 或 SSL 的安全连接。IPSec 是一个 IP 层协议，它使得发送和接受的任何形式的加密保护包(TCP、UDP 和 ICMP 等)不会被做任何修改。SSL 协议支持端到端加密的加密方式，它可以在应用软件和 TCP/IP 协议中提供客户端_服务供应商的认证，对客户端之间的连接渠道进行加密。随着云计算基础设施在多项服务中的应用，不同的端口可以支持多个 SSL 到一个虚拟服务器的连接。如图 2 所示，该模型实现了连接加密的 IPSec 方案，并支持 SSL 方案，能够实现主机到主机的连接，以及客户端和云系统之间的连接。

3　基于可信第三方的云安全模型

3.1　安全模型

针对云计算环境下多租户共享资源的特点，本文提出基于可信第三方的云安全模型，如图 3 所示，该模型通过可信任的第三方将客户从安全负担中解放出来，可以解决传统安全领域的弊端，提供多层次、分布式环境下端对端的安全服务。

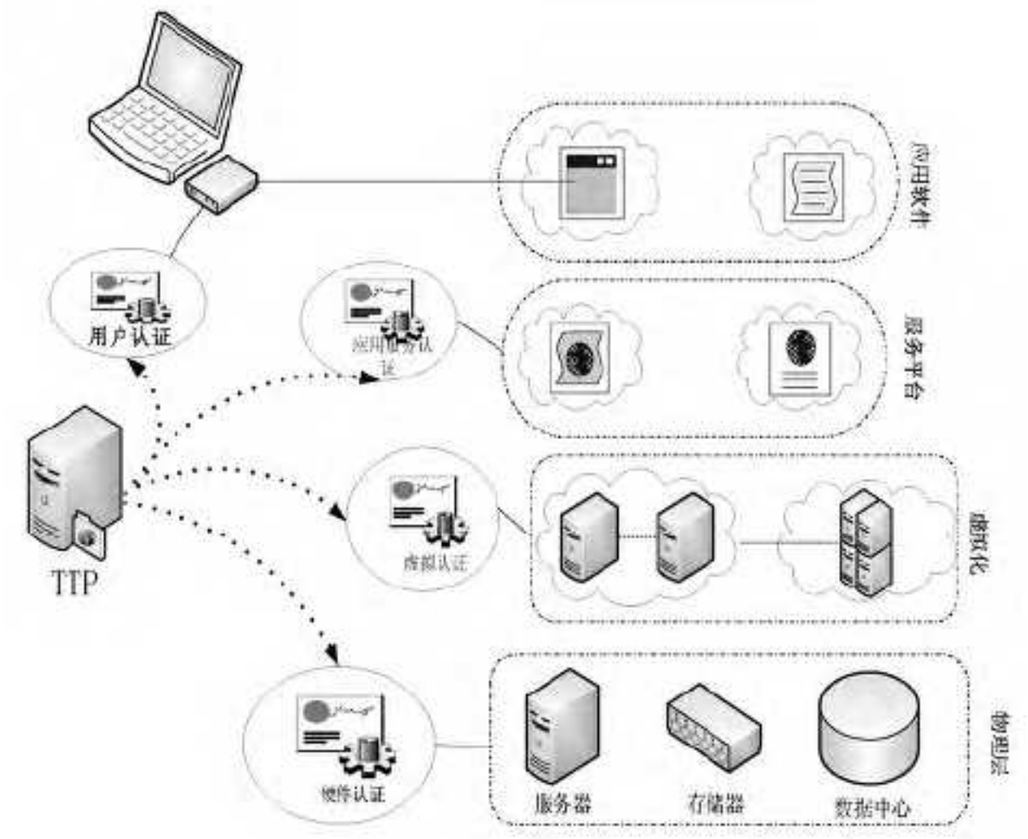

图 3　基于可信第三方的云安全模型

在分布式云计算环境中，TTP 是一个理想的安全协调员，它属于独立的实体管理域，需要建立安全的相互协调关系。如图 3 所示，云环境中分为用户层、服务层、虚拟层、物理层基础设施供应商。TTP 提供证书服务，受信任的证书服务可以作为一个可靠的电子护照，建立一个实体的身份。信任在本质上是以自上而下的方式进行操作的，因为每一层需要信任它紧接着的下一层，而且每一层需要在业务、技术、程序和法律水平上实行安全保障，因而利用它来进行安全连接。信任可以被视为连接用户终端和应用程序所有者的锁链。

3.2　认证协议

云用户需要使用自己的个人数字证书，并利用云计算服务对自己进行身份验证和对访问所需的资源权限进行强力的认证。基于 TTP 的认证协议如图 4 所示[6]。

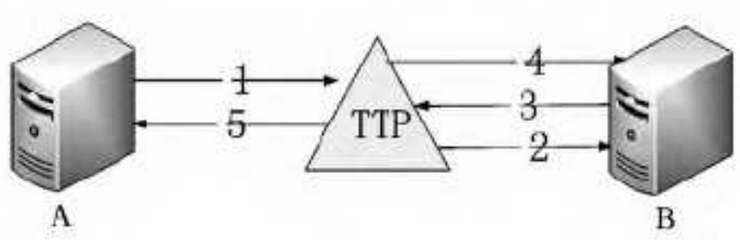

图 4　基于 TTP 的认证协议

基本符号说明：

(m,n)：表示消息 m 与消息 n 进行级连。

f_X：字段名，其中下标表示字段的含义，用于标识消息交换的目的。

EOO(evidence-of-origin)：发送方非否认证据，用于证明发送方发送过某个消息。

EOR(evidence-of-receipt)：接收方非否认证据，用于证明接收方收到发送方发送的某个消息。

Ka：主体 A 的公开密钥，用于验证 A 的数字签名。

Ka^{-1}：是与 Ka 对应的 A 的秘密密钥。

$h(m)$：应用于消息 m 的单向散列函数。

Step 1　A 生成发送消息 m 的非否认证据 EOO；生成随机会话密钥 k，并使用 k 对 EOO 进行加密；计算消息 m 的摘要 $h(m)$；然后使用 TTP 的公开密钥加密 k，A 向 TTP 发送 m 与 EOO。

Step 2　TTP 向 B 方发送接收消息 m 的请求。

Step 3　B 生成收到满足 $h(m)$ 的消息的非否认证据 EOR，并向 TTP 发送 EOR。

Step 4　TTP 通过两次解密运算获得 EOO，并校验 A 签名的有效性。同时，TTP 校验 EOR 的 B 签名的有效性。TTP 通过由 EOO 获得的 m 计算摘要 $h(m)$，并与 EOR 中的 $h(m)$ 进行结果比较。如果二者一致，则立即向 B 发送 $(m,$ EOO)。

Step 5　同时向 A 方发送 EOD。

3.3　基于 TTP 的多租户资源分配算法

依据经济学的理念，在云市场条件下，云资源被视为可销售商品，企业生产商品后由代理商将商品分租给消费者，在全球范围内的每个云用户可以根据自己的需求按照一定的付费方式通过销售人员从代理商中购买商品。图 1 提出了云资源管理经济模型，经过上文分析，它存在一定的安全隐患，因此本文提出将 TTP 引入云安全模型中，TTP 可以代替“销售人员”的作用进行改进与优化，扮演认证中心角色。云用户相信认证中心能为双方验证数据的正确性和数据交换的正确性提供正确的依据，这可解决潜在的网络安全隐患。云资源供需双方先根据各自的策定价略确定价格，TTP 将云资源提供方定价降序排列，云资源需求方则按定价升序排列，TTP 担任仲裁的角色，选择能提供最大效用的供应商[8]。

下面具体介绍基于 TTP 的多租户资源分配算法。

形式化描述如下：

设服务请求集 $D=\{d_1,d_2,\cdots,d_i,\cdots,d_n\}$，$i=1,2,\cdots,n$，$t_d$ 为用户要求服务完成的时间，e 为用户代理完成该任务的预算费用，将服务完成时间与用户预算成本加权的方法作为效用函数，有下式[8]：

$$u(t_d,e)=\alpha\ln(kt_d)+\beta\ln e$$

其中，k 为完成用户服务所需要的服务类型向量；α,β 是由用户给定的系数，α 代表时间偏好，β 代表费用偏好，满足条件为 $0\leqslant\alpha,\beta\leqslant1$，且 $\alpha+\beta=1$，表示用户对服务质量的要求，是偏好完成时间更短还是偏好费用更低。

具体算法流程如下。

Step 1　初始化云计算资源分配的环境和资源供需双方节点的信息，其中 d_i 为用户 A，B 为资源提供方。

Step 2　A 加密消息，向 TTP 发送 m 和 EOO。

Step 3　通过 TTP 选择可信度高并且效用高的资源 r_j 作为供应方 B。

对服务请求集 D 中的每个服务请求 d_i 进行调度，重复执行以下步骤：

```
{ For each t
  in order u(t_d,e)
      //按效用值从小到大对资源排序
  if minimum α<βand ETC(d_i,t)<T_di then
    if P_ij<<e_ij
  then allocate t to r_j
      //把任务分配给最便宜的资源 r_j
  else if α>β and P_ij<e_ij then
    if ETC(d_i,t)≪T_di
  then allocate t to r_j
      //把任务分配给执行时间最短的资源 r_j
  end if
end for
}
```

（下转第 382 页）

Science,1982,11(5):341-346

[2] Pawlak Z. Rough set approach to multi-attribute decision analysis[J]. European J of Operational Research, 1994,72(3):443-459

[3] 徐章艳,杨炳儒,宋威. 基于简化的二进制差别矩阵的快速属性约简算法[J]. 计算机科学,2006,33(4):155-158

[4] 支天去,苗夺谦. 二进制可辨识矩阵的变换及高效属性约简算法的构造[J]. 计算机科学,2002,29(2):140-142

[5] 舒文豪,徐章艳,等. 一种快速不完备决策表的差别矩阵属性约简算法[J]. 小型微型计算机系统,2011,32(9):103-110

[6] 徐章艳,杨炳儒,宋威,等. 几种不同属性约简的比较[J]. 小型微型计算机系统,2008,29(5):848-853

[7] 黄丽宇,徐章艳,等. 基于改进的 FP 树的快速属性约简算法[J]. 计算机工程与应用,2010,46(35):152-191

[8] Yang Ming, Yang Ping. A novel condensing tree structurefor rough set feature selection[J]. Neurocomputing,2008,71(4-6):1092-1100

[9] Yang Ming, Yang Ping. A novel approach to improving。C-Tree for feature selection[J]. Applied Soft Computing,2010,11(2):1924-1931

[10] 杨明,吕静. 一种基于 C-Tree 的属性约简增量式更新算法[J]. 控制与决策,2012,27(12):1769-1775

[11] 高静,韩智东. 利用差别矩阵构造决策树[J]. 计算机工程与应用,2011,47(33):18-21

[12] Kryszkiewicz M. Rough set approach to incomplete information system[J]. Information Science,1998,112(1):39-49

[13] Kryszkiewicz M. Rules in incomplete information systems[J]. Information Sciences,1999,113(2):271-292

(上接第 365 页)

其中,T_{di} 为完成服务 d_i 的最终期限,$ETC(d_i,t)$ 为服务请求 d_i 在资源 r_j 上的预期执行时间,e_{ij} 为完成服务 d_i 用户愿意支付的服务费用,P_{ij} 为服务 d_i 使用资源 r_j 的价格。

Step 4 TTP 向 B 发送接收消息 m 的请求。

Step 5 B 向 TTP 发送 EOR。

Step 6 TTP 通过两次解密并校验有效性,来向 B 发送 (m,EOO)。

Step 7 同时向 A 发送 EOD。

Step 8 交换信息 m 完毕。

4 仿真实验与性能分析

本文采用 CloudSim 模拟工具进行了仿真实验来验证基于可信第三方的云资源管理模型的有效性和性能。

CloudSim 软件是澳大利亚墨尔本大学的网格实验室和 Gridbus 项目联合开发设计的云计算仿真软件。在 SimJava 离散事件模拟的包基础上开发了函数库,同时采用虚拟化技术将数据中心的资源进行整合,将其虚拟化为资源池,使其支持云计算的安全认证、资源管理和调度模拟。本文以 CloudSim 为基础进行二次开发,搭建基于可信第三方的云资源管理建模的实验环境。云主机上安装 Red Hat 9.0 Linux 版本操作系统,并配置 jdk1.6.0_13 软件。通过将 CloudSim 1.0 beta 版解压到 jdk1.6.0_13 软件安装目录下后,在 ClassPath 中加入路径“C:\CLOUDSIM\jars\cloudsim.jar;C:\CLOUDSIM\jars\gridsim.jar;.\CLOUDSIM\jars\simjava2.jar;”,完成了 CloudSim 的配置。仿真实验的基本步骤如下:初始化 GridSim 函数库、创建数据中心、创建 TTP、创建虚拟机、创建云任务、建模仿真、结果统计。

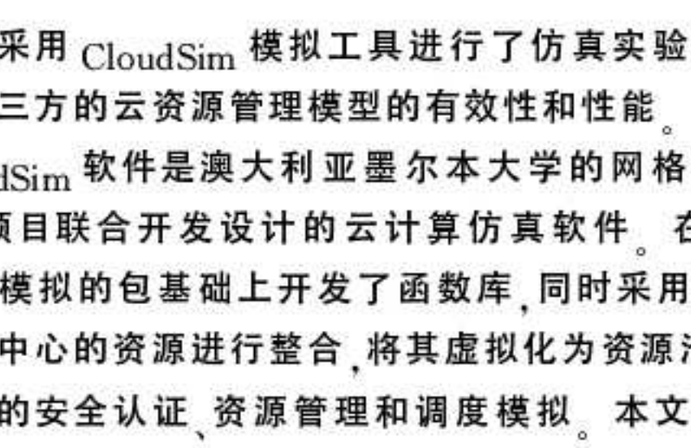

图 5 SJF、FCFS 与 TTP 策略任务成功执行率比较

本文将短任务先执行(Shortest Job First,SJF)策略、先来先服务(First Come First Serve,FCFS)策略,与本文基于 TTP 的策略做任务成功率的比较。由图 5 看出,随着云用户的增多,任务执行成功率有所下降,但是本文策略的成功率要高于 SJF、FCFS 策略。由此得出结论,基于 TTP 策略构建的云环境中,将可信度最高的云节点资源提供给云用户,能够有效提高资源分配的效率、提高可信度。

结束语 信任与安全成为云计算面临的重大威胁,本文将可信第三方引入云安全的解决方案,通过第三方的信誉监督解决了客户的安全负担,第三方的任务是在分布式信息系统中保证特定的安全特性,从而构建实体之间的信任网。改进的基于 TTP 的资源分配算法可有效提高资源分配率、可信度。本文工作只是个起点,下一步研究工作的重点是:模型的细节实现;基于证书的授权问题;进一步完善系统的完整性、保密性、真实性等。

参 考 文 献

[1] 刘鹏. 网格计算与云计算(PPT)[EB/OL]. http://www.chinacloud.cn/download/PPT/GridCloudComputing.ppt

[2] Buyya R, Abramson D, Giddy J, et al. Economic models for resource management and scheduling in grid computing [J]. Concurrency & Computation,2002,14(13-15):1507-1542

[3] 高宏卿,邢颖. 基于经济学的云资源管理模型研究[J]. 计算机工程与设计,2010,31(10):4139-4142

[4] Geimer M, Shende S, Malony A D, et al. A generic and configurable source-code instrumentation component[C] // Allen G, Nabrzyski J, Seidel E, et al., eds. ICCS (2), Vol. 5545 of Lecture Notes in Computer Science. Springer,2009:696-705

[5] International Telecommunication Union. X-509|ISO/IEC 9594-8, The directory: Public-key and attribute certificate frameworks [S]. ITU, X-Series,2001

[6] 卿斯汉. 电子商务协议中的可信第三方角色[J]. 软件学报,2003,14(11):1936-1943

[7] Lekkas D, Gritzalis S, Katsikas S. Quality assured trusted third parties for Deploying secure Internet-based health care applications[J]. International Journal of Medical Informatics,2002,65(2):79-96

[8] 陈冬娥,杨扬,刘丽. 基于效用最优的网格计算资源调度算法[J]. 计算机工程与应用,2006,42(2):191-193