第38卷　第24期　　计 算 机 工 程　　2012年12月
Vol.38　No.24　　Computer Engineering　　December 2012

• 云计算专题 •　　**文章编号：**1000—3428(2012)24—0009—05　　**文献标识码：**A　　**中图分类号：**TP391

一种基于任务角色的云计算访问控制模型

王小威，赵一鸣

(复旦大学计算机科学技术学院，上海 201203)

摘　要：数据安全问题是云计算推广的一大阻碍，主要来源于数据共享带来的安全问题和云服务提供商的超级特权导致的潜在危险。为此，分析云计算中数据存储和用户群体的特点，提出一种基于任务角色的云计算访问控制模型，对不同访问主体采取不同访问控制策略，以提供分级的安全特性，使云服务提供商不再享有超级特权。分析结果表明，该访问控制模型使得云端数据访问安全无须依赖于服务器的绝对可信，为云计算提供了更为可靠的安全特性。

关键词：云计算；数据共享；访问控制；数据安全；基于任务-角色的访问控制模型；访问控制策略

A Task-role-based Access Control Model for Cloud Computing

WANG Xiao-wei, ZHAO Yi-ming

(School of Computer Science, Fudan University, Shanghai 201203, China)

【Abstract】Data security is a big block for the promotion of cloud computing, which is mainly derived from data sharing and privileges of vendors. This paper analyzes features of data storage and user groups in cloud computing, proposes a kind of cloud computing access control based on Task-role-based Access Control(T-RBAC) model, which provides different access control policy for different object to achieve hierarchical safety. And vendors enjoy no privileges in this mode. Analysis indicates that this cloud computing access control model provides more reliable security feature which can no longer rely on credibility of server.

【Key words】cloud computing; data sharing; access control; data security; Task-role-based Access Control(T-RBAC) model; access control policy

DOI: 10.3969/j.issn.1000-3428.2012.24.003

1　概述

云计算的高速发展提供了大型数据存储和大型计算的服务，打破普通PC机的限制，减弱对大型机的需求，同时也为资源共享提供便利，解决了共享的网络边界、区域等限制，而且云计算的发展从硬件层面增强数据安全，强大的备份机制和容错机制解决了由于硬盘损坏、灾难等引起的数据安全问题。然而云计算在给用户带来便利的同时，却也产生了相应的安全隐患，云模糊了网络安全边界，存储介质位于用户控制之外[1]，被第三方控制，用户对数据安全的可控性减弱，只能被动依赖于服务提供商的可信度[2]。特别是在公有云中，由于云的公共获得性，对其他用户的访问控制能力过弱，数据会担心被非授权用户读取或引用[3]。企业用户可以通过建立私有云解决部分问题，但是私有云的成本对于中小企业来说也是一笔巨大的负担。另一方面，现在大部分云计算提供者都没有服务水平协议(SLA)[4]，也就是说如果你的数据丢失，他们并不负责。这些问题都在一定程度上阻碍了云计算的推广应用。

云计算的发展提供了强大的冗余存储和容错机制，以及更为可靠的数据物理存储安全，但是在访问控制方面却没有一种足够安全的方案，上文所提及的安全问题也都是访问控制安全引起的。访问控制是实现用户数据机密性和进行隐私保护的重要手段[5]，并且由于分布式和共享的特性，云计算中对同一客体的访问主体流动性较大，需要更为灵活的访问控制机制。本文比较了多种访问控制模型的优缺点以及适用场景，并根据云计算中数据存储的特点以及访问控制需求，使用基于任务-角色的访问控制(Task-role-based Access Control, T-RBAC)模型构建了一个安全的云计算访问控制方案。

2　访问控制模型

传统的访问控制模型有自主访问控制和强制访问控制2种[6]。其中，自主访问控制通过建立主客体关联表来组织客体和主体的关系，通常使用访问控制矩阵和访问控制列表来存放访问控制信息，多用于商用、民用系统中；强制访问控制是基于中心结构的访问控制，多用于多级军事系统中[6]，由授权机构为主体和客体分别定义固定的权限，系统为每一个主体赋予访问标签，为客体分配表示敏感级别的标签，通过客体主体相应的标签来决定是否通过访问请求。这2种访问控制模型都存在管理困难的问题，

作者简介：王小威(1987－)，女，硕士研究生，主研方向：密码学，信息安全；赵一鸣，副教授

收稿日期：2012-04-16　　**修回日期：**2012-05-21　　**E-mail：**hklengyan@126.com

随着计算机系统的不断发展，安全需求也不断变化，出现了对灵活性好、适应性强的访问控制模型的需求。

自主访问控制的优点是创建者对自己的客体拥有绝对的自主权，分布式授权管理较为灵活，而缺点是不保护客体副本，安全性低，访问列表的维护管理工作量大，适用于安全要求不高、用户数少的小型C/S架构的个人应用系统，不适用于分布式网络。强制访问控制则强调安全性，有完善的形式化安全模型，信息单向流通，可以有效阻止特洛伊木马的泄漏。但是过于强调保密性导致授权的可管理性不强，并且实现的工作量大，灵活性不足，适用于多级安全的军用系统和操作系统的访问控制，而不适用于主体客体频繁更新的场所。

为了克服标准矩阵模型中将访问权限直接分配给主体的缺陷，20世纪90年代提出的基于角色的访问控制(RBAC)[6-8]模型引进了角色的概念，系统将权限分配给角色，然后用户从拥有的角色中获得权限。这种模型与传统的访问控制模型相比，简化了系统管理，减轻了权限分配的重复劳动，明确责任预授权，加强了安全策略，更具有灵活性和可管理性，而且简化了系统管理。但是基于角色的访问控制模型依然是从系统的角度出发的，在权限控制时没有考虑执行的上下文环境[6]，只适用于角色结构严谨的企业内部访问控制。随着分布式计算的发展，组织任务进一步自动化，使得安全问题从独立的计算机系统静态的主体和客体保护转移到动态授权保护中来。一个合适的访问控制机制应该保证授权只有在任务开始执行时才授予且任务结束授权就要被收回，否则可能导致安全泄露。基于任务的访问控制模型[6,9]就是面向上下文环境的访问控制。

基于任务的访问控制(TBAC)模型通过任务关联角色和权限，系统给用户分配角色，用户通过角色获得任务，然后在任务的某个具体实例中获得客体的访问权限。这是一种动态授权的主动安全模型，主体仅在执行任务时访问客体，任务结束权限就被消耗完，防止主体对客体权限的无限期拥有，同时客体的访问控制权限随着执行任务的上下文环境变化而变化。但是TBAC[6,9]模型授权管理工作繁杂，没有分离角色和任务，不支持角色的层次等级，而且不支持被动访问控制，很难单独模型化，在实际应用中往往需要和其他的访问控制模型相结合。适用于工作流、分布式处理、多点访问控制的信息处理以及事务管理系统。

基于任务-角色的访问控制(T-RBAC)模型结合了RBAC和TBAC的优点，既支持主动访问控制又支持被动访问控制，通过任务来实现上下文环境的权限分配而使用角色来对访问控制进行等级分层，满足了分布式环境下公司的访问控制需求。

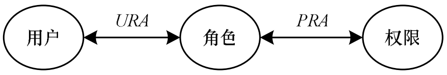
3 基于T-RBAC的云计算访问控制

对云计算来说，在共享环境下，存储于云端的数据访问主体会频繁变动，给系统权限管理带来用户管理上的难度。在T-RBAC模型[10-11]中，使用角色的概念来进行用户管理，具有明晰的角色层次管理，以及高扩展性和适应性。由于云计算中主体对客体的权限需求有明显的角色属性区别，本文根据主体对客体访问的操作需求，把云计算中的访问主体分成所有者、云服务器、共享访问者3类，进行角色分类授权管理，应对共享访问者的频繁变动。

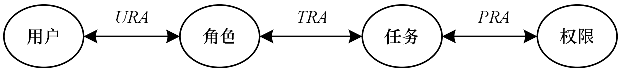
在目前一般的云计算访问控制中，云服务器都是访问控制权限分配主要角色，并且对客体持有最高权限，云计算服务商提供和监管享有特权的管理员方面的具体信息以及控制访问方面的具体信息[5]。而本文方案中通过授权管理转换云服务器在访问控制中的角色，云服务器通过客体拥有者授权获得权限，并在授权过程管理中充当传递访问请求的可信中间人，使得访问控制安全不需要完全依赖于云服务器的可信度，同时利用云服务器分担部分授权工作，减轻用户负担。

3.1 T-RBAC访问控制模型

T-RBAC模型实际上是基于RBAC模型框架上的扩展，继承RBAC的特点，结合TBAC的动态授权，将传统RBAC的3层访问控制模型改为4层，将权限通过任务分配给角色，而不是直接分配给角色，实现了动态分配，如图1所示。



(a)RBAC模型3层结构



(b)T-RBAC模型4层结构

图1 T-RBAC模型对于RBAC模型的扩展

在T-RBAC模型中，将工作流分解为一些相互依赖的任务，然后将任务分配给角色，而角色通过执行任务节点或任务节点的一个实例来取得权限。客体的权限通过PTA或IPA进行分配，用户发起会话后通过角色得到对客体的访问权限，T-RBAC模型中的$S\text{-}RH$实现了角色间的部分角色继承。访问权限的控制则通过约束集来实现控制策略，图2显示了T-RBAC模型框架。

T-RBAC模型的形式化定义如下：

用户集$U=\{u_i|i=1,2,\cdots,m\}$。

角色集$R=\{r_i|i=1,2,\cdots,k\}$。

任务集$T=\{ti|i=1,2,\cdots,n\}$：权限分配对象。

任务实例$TI=\{ti_j|j=1,2,\cdots,k\}$：任务在运行中的实例，即任务的一次执行。

权限$P=\{pi|i=1,2,\cdots,p\}$：权限是主体能对客体进行的操作。

操作Op：操作是一个可执行的程序映像。

会话S：会话是用户与激活角色之间的映射。当用户激活了部分或全部被授予的角色时，就建立了一个会话，

用户实际上执行的权限是在这次会话期间被激活的角色权限。

约束集 C：指对于访问控制中各种指派所作的规则限制。

$S\text{-}RH$：部分继承的角色层次，如下：

$R_1, R_2 \in S\text{-}RH$，$R_1 >^* R_2$，$\forall Ti \in R_2$

$Ti \in S \cup A \Rightarrow R_1$继承$T_i$的所有权限和$R_2$的读权限

URA：$URA \subseteq R \times U$，用户角色分配。

TPA：$TPA \subseteq P \times T$，任务权限分配。

IPA：$IPA \subseteq P \times TI$，实例权限分配。

TRA：$TRA \subseteq R \times T$，任务角色分配。

IRA：$IRA \subseteq R \times TI$，实例角色分配。

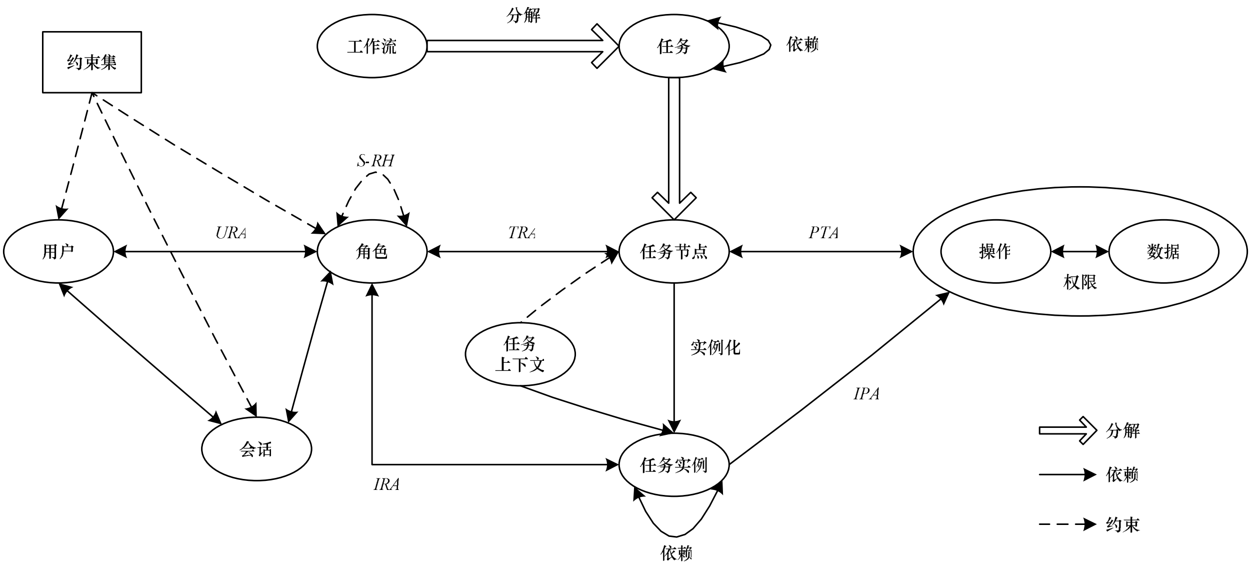


图 2　T-RBAC 模型

3.2　基于 T-RBAC 的云计算访问控制模型

3.2.1　云计算访问控制需求

云端存储的数据不同于公司本地存储的数据，在公开的网络环境中不受公司局域网的保护，其对访问者的访问控制策略也有其特定的需求。云计算中数据的访问控制需求主要如下：

(1)用户角度：在云计算环境下，数据的访问者主要包括云服务提供商、共享访问者和公司内部访问者 3 类，这 3 类访问主体的权限需求各不相同。其中，云服务提供商负责数据的维护，通常执行的操作为灾难恢复和数据一致性管理，由服务器执行。而共享访问者对数据的访问权限多数为读操作，极少数项目合作者需要进行编辑，而公司内部访问者的访问权限取决于访问主体在公司内部的角色等级。

(2)数据角度：由于云环境的公开性以及云服务器这个第三方的存在，数据的访问控制应当根据不同的安全等级设置不同的访问控制管理。如可公开共享的客体的访问授权可交由云服务器来执行，而机密文件的访问控制主权由客体创建者持有。

3.2.2　云计算访问控制策略

在本文的访问控制机制中，使用 T-RBAC 模型，将这些访问控制需求通过任务来实现。将客体的访问权限分配给任务，而后通过任务的安全级别来完成分级访问控制。在本文的 T-RBAC 机制中，将任务分成四大类：私有类任务 P，监管类任务 S，工作流类任务 W 和活动批准类 A，来简化对任务权限分配的管理，4 种任务的区别如表 1 所示。

表 1　T-RBAC 模型中 4 种任务

任务类别	作用	特点
P	私有	不继承，被动访问
S	监管	可继承，被动访问
W	面向工作流	不继承，主动访问
A	活动批准	可继承，主动访问

T-RBAC 机制下的访问控制策略主要通过任务来实现，对客体的一次访问被定义为一次工作流，而工作流分解为任务，每次任务的执行可通过任务实例实现。而对主体的访问权限通过 IPA 分配给任务实例，用户在 URA 关系下得到角色，并通过 IRA 执行相应的实例角色分配得到任务实例和权限。云计算访问控制的组件属性如表 2 所示，带下划线属性代表关键属性。

表 2　各组件属性

组件	属性
用户	用户 ID，用户类别
角色	角色 ID、角色类别
任务	任务 ID、任务类型
任务实例	任务 ID、实例 ID、执行时间
权限	权限 ID、对象、访问类型
会话	会话 ID、用户 ID、角色 ID
RH	角色关联
IRA	任务实例 ID、角色 ID
URA	用户 ID、角色
IPA	任务实例 ID、权限

在云计算环境下，访问控制的安全策略主要通过以下 4 个角度的管理实现：

(1)用户管理。在云计算环境下，角色可分为客体所有者、内部访问者、外部共享访问者和云计算提供商，客体所有者管理系统的权限分配过程，而内部访问者的角色对于公司来说可根据员工的层次管理。而外部共享访问者对数据的操作大多是读操作，在 T-RBAC 框架下通过任务实例分配权限，每次为相同客体的访问者创建任务实例，简化了用户管理和权限分配工作。云计算提供商对数据的操作通常为数据备份和恢复，系统或客体所有者向云计算提供商定时激活特定的数据备份和恢复任务，来防止提供商随意访问数据、滥用超级权限。

(2)任务管理。任务的分类细化了访问控制的安全等级，在 T-RBAC 模型中，P、S、W、A 4 个类别对任务的安全等级进行了划分。系统根据主体的访问请求启动相应任务，分配对应的权限，对权限实现了细粒度管理。面向工作流的 W 类任务具有权限不继承，主动访问控制的特点，把共享访问者的访问任务设置为 W 类，可控制访问者的权限不会二级授权给其他用户，同时任务的时间属性消除了权限无限期持有导致数据安全的隐患。

(3)数据管理。数据安全通常采用公钥系统进行密文存储，并通过对客体的安全等级设置对数据进行分级管理，对不同级别的数据设置不同的权限最大集，细化了安全等级。数据安全管理的相关工作是下一步的研究工作。

(4)授权过程管理。在本文的访问控制方案中，云计算提供商不再拥有超级权限，用户的访问请求也不再直接由云计算提供商处理，而是由客体所有者和云计算提供商共同来处理访问请求。由于云端数据进行了分级安全管理，客体拥有者可将低安全级别的数据访问请求授权给云端服务器管理，而监控高安全级别的数据访问请求，既保证了数据安全的可控性，又减少了访问管理工作。

定义云服务器 ID 为 CS，用户 Ui 访问 Uj 拥有的客体 Oj 的过程如下：

(1)Ui 向 CS 发送访问请求 Acc。

(2)CS 检查客体权限列表，若拥有该客体的访问授权，则验证 Ui，并返回授权证书或拒绝，转第(6)步；若没有，把 Acc 转发给 Uj，转第(3)步。

(3)Uj 与 Ui 相互验证对方信息，判断是否给 Ui 授权，若不授权，向 Ui 发送 reject；若授权，转第(4)步。

(4)Uj 向 T-RBAC 组件申请创建任务，T-RBAC 组件返回授权证书。

(5)Uj 向 Ui 发送证书。

(6)Ui 向客体 Oj 发起访问请求。

图 3 为一次访问授权过程的序列图表示。

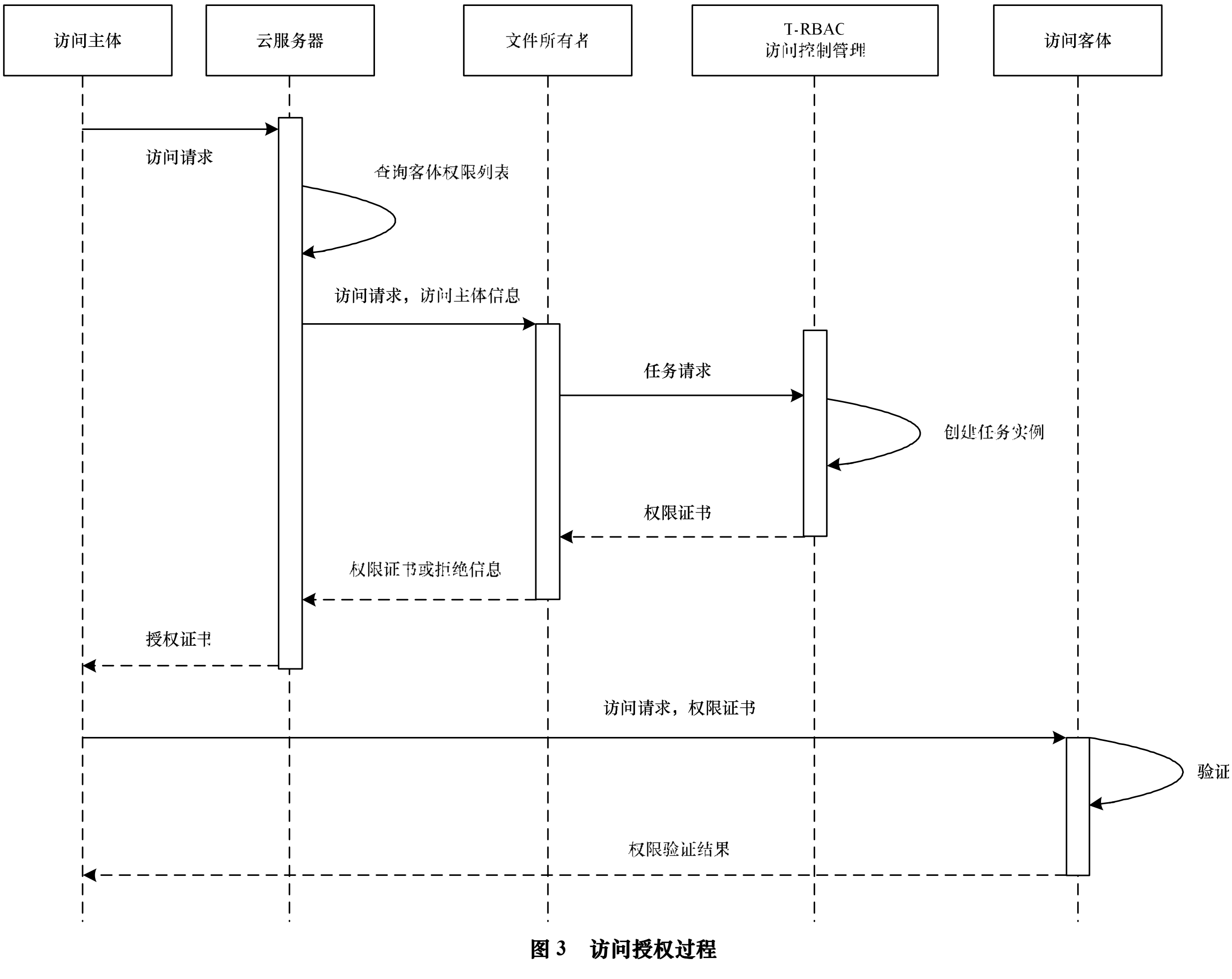


图 3 访问授权过程

4 结束语

云计算下的数据存储目前还存在一些不可忽略的安全问题，特别是对数据的访问控制问题一直是用户担忧的重点，这种模糊了网络边界、访问控制由云端服务器控制的存储方式在一定程度上阻碍了云计算的推广。而基于任务-角色的访问控制(T-RBAC)能够利用云端服务器，与客体所有者一起通过任务分配权限的方式，既满足了分布式访问控制的要求，同时也具有清晰的角色层次管理。本文比较了目前各种典型访问控制模型的优缺点，分析了 T-RBAC 模型对于云计算访问控制的适用性，同时使用 T-RBAC 模型构建了一个面向共享安全的访问控制机制，从数据管理、任务管理、用户管理和授权管理 4 个方面来解决云计算访问控制中的安全要求。但是 T-RBAC 模型也有它不足的地方，在未来的研究工作中期望能不断改进完善，而云计算存储除了访问控制之外，还有如信任管理等问题，同样有待进一步的研究。

参考文献

[1] 洪 澄, 张 敏, 冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报, 2011, 32(7): 125-132.

[2] Chow R. Controlling Data in the Cloud: Outsourcing Computation Without Outsourcing Control[C]//Proc. of ACM Workshop on Cloud Computing Security. New York, USA: ACM Press, 2009: 85-90.

[3] 孙国梓, 董 宇, 李 云. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报, 2011, 32(7): 145-152.

[4] 陈 全, 邓倩妮. 云计算及其相关技术[J]. 计算机应用, 2009, 29(9): 2562-2566.

[5] 陈丹伟, 黄秀丽, 任勋益. 云计算及安全分析[J]. 计算机技术与发展, 2010, 20(2): 99-102.

[6] 沈海波, 洪 帆. 访问控制模型研究综述[J]. 计算机应用研究, 2005, 22(6): 9-11.

[7] 李孟珂, 余祥宣. 基于角色的访问控制技术及应用[J]. 计算机应用研究, 2000, 17(10): 44-47.

[8] Sandhu R S. Role-based Access Control Models[J]. Computer, 1996, 29(2): 38-47.

[9] 邓集波, 洪 帆. 基于任务的访问控制模型[J]. 软件学报, 2003, 14(1): 76-81.

[10] 韩若飞, 汪厚祥. 基于任务-角色的访问控制模型研究[J]. 计算机工程与设计, 2007, 28(4): 800-807.

[11] Oh S, Park S. Task-role-based Access Control Model[J]. Information Systems, 2003, 28(6): 533-562.

编辑 任吉慧

(上接第 8 页)

6 结束语

本文从云计算模型出发，提出了支持网络体系结构和协议研究的网络创新实验平台设计方案，并给出了其原型实现系统 TUNIE。TUNIE 利用云计算平台和虚拟化技术提供高性能的虚拟网络节点和网络连接，并通过底层的链路隔离支持拓扑定制与多虚拟网络并行。

TUNIE 目前仅是一个初级的原型系统。未来进一步的开发工作将集中在以下 3 个方面：更简单便捷的操作，更高性能的虚拟路由器支持和更稳定的平台运行保障。层次化和模块化的结构设计使得 TUNIE 易于部署和进一步持续开发。今后将扩大 TUNIE 部署范围，增强其对网络体系结构创新实验的支持，成为具有广泛认同度的网络体系结构研究方案验证平台。

参考文献

[1] Bavier A, Feamster N, Huang M, et al. Realistic and Controlled Network Experimentation[J]. ACM SIGCOMM Computer Communication Review, 2006, 36(4): 3-14.

[2] The GENI Project Office. About GENI[EB/OL]. (2011-12-03). http://www.geni.net/?page_id=2.

[3] 陈 全, 邓倩妮. 云计算及其关键技术[J]. 计算机应用, 2009, 29(9): 2562-2567.

[4] Amazon com, Inc.. Amazon Elastic Computing Cloud(Amazon EC2)[EB/OL]. (2011-12-22). http://aws.amazon.com/ec2/.

[5] Handley M, Hodson O, Kohler E. Xorp: An Open Platform for Network Research[J]. ACM SIGCOMM Computer Communication Review, 2003, 33(1): 53-57.

[6] Kohler E, Morris R, Chen Benjie, et al. The Click Modular Router[J]. ACM Transactions on Computer Systems, 2000, 18(3): 263-297.

[7] The Cacti Group, Inc.. What is Cact?[EB/OL]. (2012-02-23). http://www.cacti.net/what_is_cacti.php.

[8] Digium, Inc.. About the Asterisk Project[EB/OL]. (2012-02-10). http://www.asterisk.org/asterisk.

[9] Michel de Boer. Twinkle-SIP Softphone for Linux[EB/OL]. (2012-02-03). http://www.twinklephone.com/.

[10] The VideoLAN Organization. VLC Media Player[EB/OL]. (2012-01-08). http://www.videolan.org/vlc/.

编辑 任吉慧