云计算的按需防护安全框架

丁鲜花 赵卫栋 俱 莹 李建平 王晓明 刘国英
(国家无线电监测中心陕西监测站 西安 710200)

摘 要 安全问题已成为制约云计算发展的重要因素。分析了服务持续可用性、服务真实性、数据完整性、信息保密性、可用性、不可抵赖性6方面的云安全目标,将云计算中6个层次的安全风险归纳为7类:物理安全风险、计算安全风险、可信计算安全风险、网络安全风险、管理安全风险、存储安全风险和应用安全风险等,并分别阐述了各类风险的安全对策。越安全的服务,在安全防护方面消耗的计算能力、存储、网络带宽就越多,指出应根据用户使用的服务类型、用户指定的安全要求以及接入网络特点等使用不同的安全保护措施,提出了按需防护的安全框架。分析了按需防护的安全框架的优点。最后给出了框架实际使用的方法。

关键词 云计算,云模型,云安全,云安全框架,云安全目标,访问控制

中图法分类号 TP309 **文献标识码** A

On Demand Security Framework for Cloud Computing

DING Xian-hua ZHAO Wei-dong JU Ying LI Jian-ping WANG Xiao-ming LIU Guo-ying
(Shaanxi Radio Monitoring Station, The State Radio Monitoring Center, Xi'an 710200, China)

Abstract Security has become an important factor restricting the development of cloud computing. This paper analyzed the cloud security objectives from 6 aspects: service constancy, service authenticity, data integrity, data confidentiality, data availability and non repudiation. It summed up the cloud computing risk in seven categories: physical security risk, computing security risk, trusted computing security risk, network security risk, management security risk, storage security risk and application security risk, and elaborated the corresponding security strategies for every security risk. The stronger the securityis, the greater the consumption of computing, memory, and bandwidth resourcesis. This paper provided on-demand security framework for cloud computing which uses different safety protection measurement according to service type, security level and access network risk. The advantage of the framework was analyzed and the application method was provided.

Keywords Cloud computing, Cloud model, Cloud security, Cloud security framework, Cloud security objective, Access control

1 概述

云计算(Cloud Computing)是一种新近提出的计算模式,是分布式计算(Distributed Computing)、并行计算(Parallel Computing)和网格计算(Grid Computing)的发展。云是一个包含大量可用虚拟资源(例如硬件、开发平台以及I/O服务)的资源池。这些虚拟资源可以根据不同的负载动态地重新配置,以达到更优化的资源利用率。这种资源池通常由基础设施提供商按照服务等级协议(Service Level Agreement, SLA)采用按时付费(Pay-Per-Use, PPU)的模式开发管理[1]。云计算因其经济性、高扩展性、用户友好性、按需服务和按服务收费等独特优势而在各行业应用中快速兴起。对于企业用户而言,可显著降低计算和存储的维护成本;对个人用户而言,通过将信息的存储和计算放在云端,降低了自身存储和计算资源有限所带来的很多约束[2]。

但当前,云计算发展面临许多关键性问题,而安全问题首当其冲,并且随着云计算的不断普及,安全问题的重要性呈现逐步上升趋势,已成为制约其发展的重要因素。2012年4月,VMware关于ESX Hypervisor的源代码泄漏,被泄露的源代码可能会被黑客利用,从而增加VMware用户的风险;2013年3月,Vmware合作伙伴Terremark宕机7小时,据报告只有2%的客户没有受到影响;2013年4月,亚马逊在弗吉尼亚州北部的云计算中心宕机,导致包括Quora、新闻服务Reddit、Hootsuite和位置跟踪服务FourSquare在内的众多网

丁鲜花(1980—),女,硕士,工程师,主要研究方向为云计算、云安全等,E-mail:dingxianhua@srrc.org.cn;赵卫栋(1977—),男,工程师,主要研究方向为云计算、云安全等;俱 莹(1986—),女,博士,工程师,主要研究方向为无线电通信链路安全、云安全等;李建平(1988—),男,硕士,助理工程师,主要研究方向为并行计算、云安全等;王晓明(1988—),男,硕士,助理工程师,主要研究方向为并行计算、云安全等;刘国英(1988—),女,硕士,助理工程师,主要研究方向为计算机网络、云安全等。

站都受到了影响等。因此，要让企业和政府放心地将自己的服务和数据运行和存放在云端，就必须全面地分析并着手解决云计算所面临的各种安全问题。

本文首先分析了云安全的6个目标；第2节分析了云安全目标；第3节分析了云计算的6层框架中7方面的安全风险及其相应防范对策；第4节提出了按需防护的安全框架并分析其优点；最后总结并分析了该安全框架的实际使用方法。

2 云安全目标

2.1 服务持续可用性

Gartner分析师称，最大的问题不是在云环境中数据可能被破坏，而是可能出现云中断，从而导致数据丢失。容灾与恢复技术主要解决的是云计算服务持续可用的问题，容灾与恢复技术可以帮助云系统在自然灾害、系统故障、人为失误中快速恢复丢失的数据和间断的服务，以提高云计算服务的持续性。

在Hadoop中，HDFS的本地冗余备份可以解决一般的故障恢复问题[3]；机架感知技术虽然解决了跨机架的安全问题，但是面对如大地震这样的大范围灾难时却无能为力。像银行、政府这样需要高安全性的机构，需要解决灾后服务恢复的问题。因此像银联数据中心这样的金融机构采用了“两地两中心”或者“两地三中心”这样的异地灾难备份机制[4]。

2.2 服务真实性

云计算环境下虽存在大量功能相同或相似，服务质量(QoS)各异的云服务，但是网络中服务使用者或服务提供者所宣称的QoS属性难以鉴别，用户选择的有效性受到限制，难选择高质量的组合服务。

文献[5]提出基于单声誉系统的方法，该算法依赖服务消费者(consumer)的回馈，不能处理消费者不汇报回馈的情况。文献[6]提出基于双层的声誉系统，该算法两层反馈的信息不一致时，难确定谁是真正的撒谎者。文献[7]提出一种黑板与白板信任演化模型，该模型可以帮助用户得到可信的、高质量的服务组合。通过黑白板结合，能够避免以往信任演化系统中前期信任匮乏的现象，同时，能够有效识别共谋欺骗，改进信任演化系统中直接信任关系稀小的问题。文献[8]提出了一种基于声誉的推荐者发现方法，在传统协同推荐机制的信息收集步骤中增加一个预处理过程，首先引入一个相关因子量化不同上下文中的推荐信任关系，得到近似的信任可传递空间，然后应用信任子网分割算法得到评估发起者的可信推荐者群，最后通过主体群内的信任传递与迭代计算确定具有高声誉值的推荐信息源。文献[9]针对云计算环境下因服务资源的可信度参差不齐常导致用户很难获得高质量的组合服务问题，提出了一种基于信任生成树的可信服务演化机制，使得虚假和恶意服务经演化后能排除在系统之外，实现了服务组合过程在可信的环境中进行。

2.3 数据完整性

云存储是云计算的重要内容，云存储减少用户存储空间的消耗，节省因为存储空间升级带来的资源、时间和精力的消耗。数据的完整性是数据存储安全的基本要求，破坏数据的完整性是影响数据安全的常用手段。数据完整性是指数据的正确性、有效性和一致性。在这里如果数据本身具有完整性，当未授权第三方对数据进行了修改而未被检测出时则认为数据仍具有完整性。在信息系统中，很多情况下数据本身的内容不需要保密，但必须要保证其完整性，如果数据被非法篡改，将造成重大损失，影响重大，比如在电子商务中商品的报价、校园管理系统的学生成绩[10]。

文献[11]针对云计算应用中的数据完整性检测问题，提出了一种交互式解决方案。该方案构造满足特殊计算关系的函数对，使得用户在同步存储校验信息的前提下，能够以常数量级的计算、存储占用量和网络交互量正确检测云中数据的完整性。

2.4 信息保密性

云计算中的信息保密性分为两类，一类是对机器存储和处理的信息的保密，另一类是对用户行为习惯的保密。文献[12]采用与传统经典载体信息隐藏相类比的方法，根据量子态利用量子力学性质设计秘密信息编码方案隐藏秘密信息。文献[13]提出了一个基于输入编码和同态加密的简洁、高效的多方保密协议。

2.5 可用性

所有云计算平台的核心目标都是为合法用户提供信息和资源的服务，可用性差势必会对用户造成声誉、客户、竞争优势、收入、运营等各方面损失。可用性保证了合法用户对信息和资源的使用不会被不正当地拒绝。

2.6 不可抵赖性

不可抵赖性是指在云计算平台中建立有效的责任机制，防止用户否认其行为。不可抵赖性有两个方面，一方面是发送信息方的不可抵赖(身份认证)，也就是说，A传送了资料到云平台上，A不能否认这个事实；另一方面是信息的接收方的不可抵赖性，A从云平台上下载了信息和资料，A不能否认这个事实。

3 云模型中的安全风险及其对策

一方面，因为云服务提供者可以更好地集中进行安全管理，云计算模式在某种程度上提高了安全性；另外一方面，因为云计算采用的云服务模型、运行模式的技术特点，云计算面临着与传统IT解决方案相比所不同的安全风险。除了要解决传统IT系统的安全风险，云服务还需要解决更多新的风险。CSA的云安全参考模型分析了各类云服务之间的关系，并把它们和与其相关的安全控制和顾虑放在一起考虑[20]。

3.1 云安全风险及其对策

CSA的Security guidance for critical areas of focus in cloud computing v3.0[20]提出云的安全控制模型，将云安全风险分为7类：物理安全风险、计算安全风险、可信计算安全风险、网络安全风险、管理安全风险、存储安全风险和应用安全风险等。

图1描述了各类安全风险及其对策。

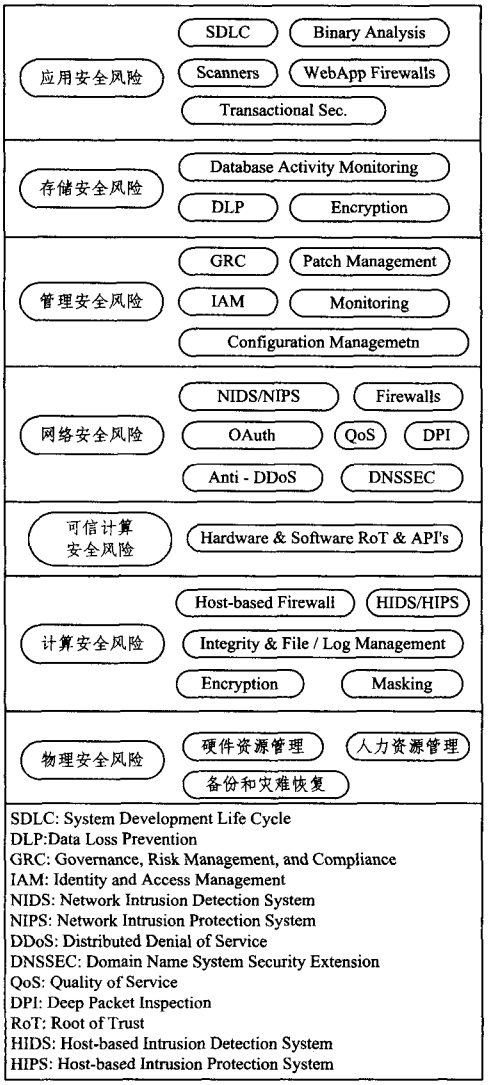

图 1　各类安全风险的安全控制方法

3.1.1　物理安全风险

云计算的本质要求使云计算中心的软、硬件极其集中，云计算服务提供商的业务连续性、灾难恢复能力需要多层安全机制来达到其安全目标。物理保护是多层安全防御战略的一个最初步骤。如果物理保护不存在或没有正确实施，那么最安全的逻辑层面措施也无法弥补物理安全上的弱点，最终可能导致安全防护整体失败。

应对物理安全风险，要建立一个传统的安全机能，做好人力资源物理安全管理，最小化能接近数据干扰正常运行的相关人员。一个能够接触到控制台的有经验入侵者能够通过重启系统或者访问当前已经是 root 或者管理员权限的系统绕过大多数逻辑保护措施。应对物理安全风险，还要求最终交付使用的云服务不含有未授权的后门留存，要求不同人员管理不同的关键基础设施组件。

另外，要建立云备份和灾难恢复机制。云灾难恢复构建于以下 3 个基础要素：一个完全虚拟化的存储基础架构、一个可扩展的文件系统以及一个可以应对客户紧急业务需求的自服务灾难恢复程序。在恢复过程中要明确如何控制备用站点的物理安全。

3.1.2　计算安全风险

服务的计算处理过程中对数据的主要危胁之一是来自于虚假的服务进程的访问和恶意的服务中段。应对计算安全风险，可以实施的安全防御机制包括基于主机的防火墙、主机入侵检测系统、主机入侵防御系统、数据一致性管理、日志管理、数据加密、honeypot 技术[16]。

3.1.3　可信计算安全风险

为了保证云基础设施中数据和计算的完整性，专家们提出了可信云计算的概念。可信云计算通过可信的外在协调方对云端网络中的节点进行认证和维护，保证客户虚拟机仅在可信节点上运行。每个经协调方认证的可信节点上都安装有可信虚拟机监测器[2]。应对可信计算安全风险，安全专家和 IT 专家需要共同合作决定在日益复杂的计算环境中，可信平台应该使用什么基础设施和软硬件才能使用户放心高效利用可信平台，这是建立可信环境的最核心问题[17]。

3.1.4　网络安全风险

数据在网络层传输过程中的主要危险有虚假身份用户、中间人攻击、拒绝服务攻击等。文献[18]提出了一种针对多租客云基础设施的拒绝服务攻击。当攻击者与正常的云用户被分配到同一个子网内时，如果攻击者发送大量数据包将该子网与外界相连的瓶颈链路堵塞，那么就会对正常用户造成网络服务的拒绝服务攻击。应对网络安全风险，网络入侵检测系统、网络入侵防御系统、深度包检测、anti-DDoS 技术、DNS 安全扩展、OAuth 等是常用的技术手段。

3.1.5　管理安全风险

在云环境中，Web 服务的聚合导致安全性脆弱，暴露在云环境中的应用面对的威胁远超在传统数据中心中经历的威胁。在云环境下，对于所有实体使用身份并采用基于风险的决策，不仅可以缓解风险，同时可以潜在地提高安全性。应对管理安全风险，身份管理是一个重要问题。对身份管理概念的理解可以分成 3 个独立的部分：身份、授权和授权访问管理。此外，还要考虑补丁管理、配置管理等。

3.1.6　存储安全风险

云存储是通过集群应用、网格技术或分布式文件系统等功能，将网络中大量不同类型的存储设备通过应用软件集合起来协同工作，共同提供数据存储和业务访问功能的一个系统[19]。存储过程对数据的主要危胁是未经授权的访问、数据更换和偷窃。应对存储安全风险的保护机制有数据备份、数据校验、加密、访问权限控制、文件完整性监控和日志监控。利用备份技术可以防止数据丢失，备份技术包括独立磁盘冗余阵列、数据恢复。通过定期对数据进行校验可以保证数据的完整性。

3.1.7　应用安全风险

应用安全领域关注的焦点有：安全软件开发生命周期控制、云计算应用的监控、Web 防火墙等。在向云中迁移和部署应用时应确保其开发过程和整个应用的生命周期中贯彻应用安全、身份管理、数据管理和隐私管理。云中的应用监控包括日志监控、性能监控、监控恶意使用、监控违规、监控违反策略行为。

3.2　云模型中的安全风险

文献[21]提出了云的 6 层模型，包括硬件层、虚拟化层、云管理层、云服务层、访问/接入层、客户端应用层等。

图 2 将各类安全风险映射到云的 6 层架构模型中。

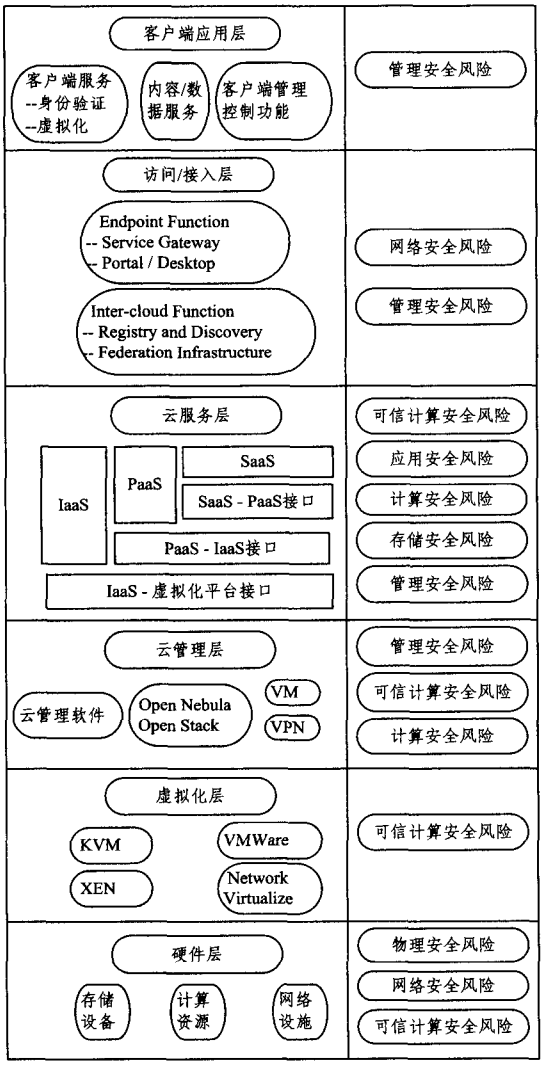

图 2　6 层云模型中的安全风险

4　按需防护安全框架

无论是加密、扫描或是防火墙，都增加了云服务的复杂程度。虽然在电子商务或电子政务等系统，安全性是最重要的因素，但是在更多的公共信息服务，比如公共论坛、电影在线播放、电子书阅读等云服务中，信息安全问题就不那么重要。即使在同一种服务中，不同的用户也会需要不同的安全服务需求。例如：在聊天软件中进行商务洽谈需要考虑安全防护，而进行朋友聊天则不用考虑安全防护。同样，商务活动的邮件需要考虑加密，而普通邮件则不需要考虑加密。

目前通用的架构基本上都是用强安全加密措施来保护所有的网络服务，但是这样的方法降低了云服务的使用效率。越安全的服务，在安全防护方面消耗的计算能力、存储、网络带宽就越多。因此，对安全需求较低的服务提供过高的安全保护会降低云计算平台的优势。另外，高安全性需要复杂的认证机制，例如，要求用户设置复杂密码，或定期更换密码，或需要提供 U 盾验证或指纹验证。这些都降低了服务的使用便利性。

综上所述，给所有服务制定强安全防护策略是不合理的。因此需要根据用户使用的服务类型、用户指定的安全要求以及接入网络特点等区别使用不同的安全保护措施。本文提出的按需防护安全框架根据不同的用户服务，针对 7 种安全风险，采用不同的安全方法。

按需防护安全框架共分 3 层：用户输入层、风险评估层、安全方法层。用户输入层接收用户指定的安全等级、服务类型和接入网络的风险等级，风险评估层根据用户输入层的输入参数决定每种安全风险的防护机制。安全方法层根据安全策略层提供的参数提供具体的安全防护办法。

图 3 描述了框架的细节。

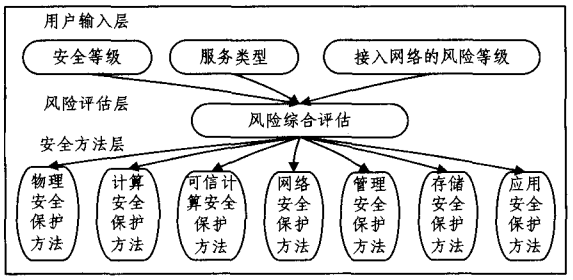

图 3　云计算的按需防护安全框架

4.1　三层架构

用户输入层共有 3 个参数：安全等级、服务类型和接入网络的风险等级。3 个用户输入参数决定了最终使用什么样的安全保护方法对服务进行安全防护。

安全等级必须既反映服务本身对安全的要求，也反映应用系统提供服务的风险。每一种服务都设定了默认的安全等级，即使用户没有对安全等级进行设置，也能得到基本的安全防护。

服务类型是用户正在使用的云服务的类型。不同类型的服务需要不同的安全防护，比如，多媒体服务讲求速度，可以允许一定的丢包率，所以不需要进行完整性验证；相反，对于文件传输服务，完整性验证是非常关键的。

接入网络的风险等级取决于用户正在使用网络的场所和网络类别，比如无线网络、办公有线网络和公共有线网络等相比，公共 Wi-Fi 接入的风险大于公共有线网络，公共有线网络的接入风险大于办公有线网络。接入网络的风险等级不需要用户手动指定，云服务可以根据接入网络的终端位置、终端 IP 地址范围等进行判断。

在风险评估层，风险评估模块从用户输入层接收参数，综合考虑安全等级、服务类型和接入网络的风险等级这 3 个参数，从而生成一个风险等级，安全方法层根据风险评估层提供的风险等级决定具体采用什么样的安全保护方法。比如对于数据存储服务，不需要保密的信息可以明文存储，需要保密但不需要在云端进行运算的数据可以使用传统加密方法加密，而某些数据不但需要保密，还需要在云端对数据进行搜索、转换、基于内容的访问控制等计算和加工，那么可以使用完全同态加密方法对数据进行加密后存储在云端，或者使用通过浏览器进行密钥传输的方法访问以密文形式存储在云端的数据。

4.2　合理性和优势分析

按需防护的安全框架是一种灵活、易布署的方案。云计算的优势之一在于由规模经济、重用和标准化带来的成本效益，为了达到这一目标，云提供商提供的服务必须足够灵活，以服务最大可能的用户群。在不同的云服务模式中，云服务提供商和用户的安全职责有很大的不同。例如，IaaS 云基础

（下转第 312 页）

[22] 张婕,山岚. CBC 算法在网页分类中的应用研究[J]. 北京化工大学学报:自然科学版,2013(1)
[23] 左敬龙,余桂兰. 具有量子特性的 ACA-SVM 网页分类方法[J]. 计算机工程与应用,2011(12)
[24] 张青. 移动互联网场景中客户特征分类技术研究[J]. 电信科学,2014(1)
[25] 傅向华,刘国,陈冬剑. 一种核心子集选择训练的大规模中文网页分类方法[J]. 小型微型计算机系统,2011(8)
[26] 宋军涛,周铜,杜庆灵. 支持向量机和蚁群算法的网页分类研究[J]. 计算机工程与应用,2009(17)
[27] 陈沧. 基于大规模类别体系的网页分类及在商品分类中的应用研究[D]. 扬州:扬州大学,2010
[28] 孙聪凯. 语义模型、近似推理算法及其在网页分类的应用[D]. 上海:上海交通大学,2009
[29] 余桂兰,陈珂,左敬龙. 基于云模型的并行蚁群-SVM 分类方法[J]. 计算机技术与发展,2014(4)
[30] 秦兵,郑实福,刘挺,等. 可分性判据在中文网页分类中的应用[J]. 微处理机,2002(1)
[31] 王天江,孔华武. 一种基于定性推理的网页分类方法[J]. 计算机工程与应用,2007(9)
[32] 阎红灿,李敏强,任蕴丽,等. 结构和内容联合提取的 XML 网页分类研究[J]. 天津大学学报:社会科学版,2009(3)

(上接第 287 页)

设施作为服务,提供商负责 Hypervisor 层以下层次的安全责任,即只负责物理安全、环境安全和虚拟化安全等这些安全控制,而用户负责操作系统安全、应用安全和数据安全。SaaS 云提供整个服务,提供商不仅负责物理、环境和虚拟化安全,还必须负责操作系统、应用和数据的安全控制。

按需防护的安全框架是高效的。给所有服务使用强安全策略降低了云服务的速度。根据用户使用的服务类型、用户指定的安全要求以及接入网络特点等区别使用不同的安全保护措施,有助于提高云服务的整体速度。

按需防护的安全框架的另一个特点是简单。用户输入层的 3 个参数都可以设置默认值,用户选择某个服务,系统便可自动判断安全等级、服务类型和接入网络的风险等级,进而提供相应的安全防护。用户也可以更改安全等级。

结束语 云计算是当前发展十分迅速的新兴产业,具有广阔的发展前景,但同时其所面临的安全技术挑战也是前所未有的。本文综合分析了云计算的安全目标、各类安全风险及防范对策,提出了按需防护的安全框架,该框架的用户输入层共有 3 个参数:安全等级、服务类型和接入网络的风险等级。每个云服务都有本身的默认安全等级,用户可以根据实际情况进行修改,也可以不修改。服务是用户申请使用的云服务的类型,系统可以自动获取。接入网络的风险等级可以由系统根据终端位置和 IP 自动判断。所以,在实际使用过程中,用户只需要设置 0－1 个参数,操作非常便利。云计算安全并不仅仅是技术问题,它还涉及标准化、监管模式、法律法规等诸多方面。因此,仅从技术角度出发探索解决云计算安全问题是不够的,需要信息安全学术界、产业界以及政府相关部门的共同努力才能实现[19]。

参 考 文 献

[1] 俞能海,郝卓,徐甲甲,等. 云安全研究进展综述[J]. 电子学报,2013,41(5):371-381
[2] Chen Z G, Liu L P, Liu A F. Trust-sensitive Web service composition strategy based on black and white board[J]. Journal on Communications, 2010, 31(6): 25-35
[3] 邓谦. 基于 Hadoop 的云计算安全机制研究[D]. 南京:南京邮电大学,2013
[4] 杨凯. 银联数据异地灾难备份架构设计探讨[J]. 中国金融电脑,2005,9(9):51-54
[5] Damiani E, Vimercati D C, Paraboschi S. A reputation based approach for choosing reliable resources in peer-to-peer net-works [C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. 2002: 18-22
[6] Jurca R, Faltingsi B. Eliciting truthful feed-back for binary reputation mechanisms [C]// Proceedings of the 2004 IEEE/WIC/ACM International Conference on Web Intelligence. 2004: 214-220
[7] 陈志刚,刘莉平,刘安丰. 基于黑白板的信任敏感服务组合策略[J]. 通信学报,2010,31(6):25-35
[8] 潘静,徐锋,吕建. 面向可信服务选取的基于声誉的推荐者发现方法[J]. 软件学报,2010,21(2):388-400
[9] 胡春华,刘济波,刘建勋. 云计算环境下基于信任深化及集合的服务选择[J]. 通信学报,2011,32(7):71-79
[10] 于洋洋,虞慧群,范贵生. 一种云存储数据完整性验证方法[J]. 华东理工大学学报,2013,39(4):211-216
[11] 颜湘涛,李益发. 基于消息认证函数的云端数据完整性检测方案[J]. 电子与信息学报,2013,35(2):310-313
[12] 安玉,蒋天发,吴有林. 一种基于量子保密通信及信息隐藏协议方案[J]. 武汉大学学报,2012,45(3):394-398
[13] 李顺东,王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报,2013,41(4):798-803
[14] Pan J, Xu F, Lv J. Reputation-based recommender discovery approach for service selection[J]. Chinese Journal of Software, 2010, 21(2): 388-400
[15] Ryan M D. Cloud computing security: The scientific challenge, and a survey of solutions[J]. The Journal of Systems and Software, 2013, 86(5): 2263-2268
[16] Van-Hau P, Dacier M. Honeypot Trace Forensics: The Observation Viewpoint Matters[J]. Future Generation Computer System, 2011, 27(5): 539-546
[17] Shpantzer G. Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age[J]. SANS Analyst Program, 2013, 40(6): 1-15
[18] Liu H. A new form of DOS attack in a cloud and its avoidance mechanism[C]// Proceedings of the 2010 ACM Work-shop on Cloud Computing Security Workshop. New York, USA: ACM Press, 2010
[19] 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
[20] CSA. Security guidance for critical areas of focus in cloud computing v3.0[OL]. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
[21] Thomas C. OW2 and the Open Cloud Industry Ecosystem[OL]. www.ciecloud.org/2013