基于体系架构的云计算安全研究进展

程宏兵 赵紫星 叶长河
(浙江工业大学计算机科学与技术学院 杭州 310023)

摘 要 云计算凭借其高效、可靠、廉价等优势,正引导着信息技术的又一次重大变革。考虑到云计算技术独有的特性和架构,安全问题一直是其发展和普及的瓶颈。针对云计算安全问题的研究也一直是该领域的重点和热点问题。将云计算体系划分为物理资源层、资源抽象层和服务提供层,并分层定义了体系中数据安全、虚拟机安全、多租户隔离、应用部署安全、数据处理技术、身份控制技术以及审计技术,介绍了相关标准,阐述了近年来的研究进展,指出了云计算体系架构安全领域的挑战与发展契机。

关键词 云安全,体系架构,研究进展
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.7.003

Survey of Cloud Computing Security Based on Infrastructure

CHENG Hong-bing ZHAO Zi-xing YE Chang-he
(College of Computer Science & Technology, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract Cloud computing is leading an information technology revolution with its advantages such as efficient, reliable, and low-cost. However, the security issue is always the obstruction which limits the development and popularization of cloud computing. Therefore, it is undisputed that the security research is a hot issue in the field of cloud computing. In this paper, we divided the cloud computing into resource layer, resource abstraction layer and service layer, and defined data security, virtual machine security, multi-tenant isolation, application deployment, data processing, identity control and audition. The paper reviewed the recent progresses in this area based on architecture division of cloud computing and provided references for further research in cloud computing.

Keywords Cloud security, Infrastructure, Research progress

1 引言

云计算是一种基于互联网的新型分布式计算模式,凭借其高效、可靠、廉价的特性,正成为大数据存储与处理、跨平台应用开发与部署等重大应用问题的优质解决方案。Gartner公司发布的2014新兴技术Hype cycle(发展规律周期)图(见图1)显示,云计算处于一个理论基本成熟但是产业应用尚未成熟的阶段。目前,制约云技术应用的因素有很多,如可用性、易用性、完整性、迁移复杂度、隐私、安全等。其中云数据隐私和安全的受关注程度最高[1]。因此,要使云计算技术获得社会各界的认可并将其普及,需要建立起人们对云计算的信任。而现阶段制约云计算发展和普及的瓶颈,正是云安全。

云计算作为新兴的技术,因大规模和开放性,其安全体系较传统网络信息系统面临更大的挑战,存在许多安全方面的挑战。如2009,2010,2012,2014和2015年Google、Microsoft、Amazon、阿里巴巴等公司的云计算服务均出现过重大故障,导致用户数据泄露、用户信息服务失败甚至出现拒绝服务等。因此,针对云计算安全的研究有着重要和深远的意义。

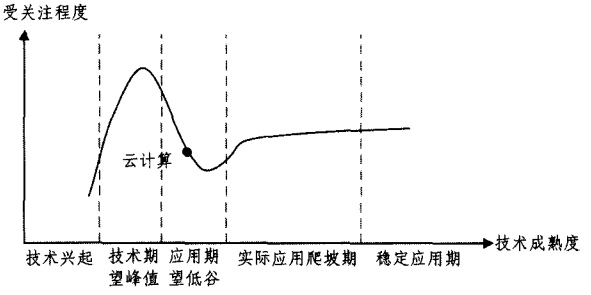

图1 2014 Gartner云计算发展规律周期图

2 云安全的定义及层次划分

2.1 云安全的定义

在云计算环境下,云安全包括了整个云计算体系的安全。传统意义上的信息安全主要保护存储在本地主机上数据的安全以及数据在传输过程中的安全,而在云环境下,云计算将各种计算资源抽象成资源池,用透明的方式提供给用户,用户按需索取使用,此过程中将会出现多租户共享资源、数据存储位置不确定等各种传统信息安全无法解决的问题。因此,云安

到稿日期:2015-06-22 返修日期:2015-09-12 本文受国家自然科学基金项目(61402413),浙江省自然科学基金(LY14F020019),中国博士后基金(2012M511732),江苏省六大人才高峰(11-JY-009),南京大学软件新技术重点实验室开放课题(KFKT2015B22)资助。
程宏兵(1979-),男,博士,副教授,CCF会员,主要研究方向为云计算安全、信息安全与密码学,E-mail:chenghb@zjut.edu.cn;赵紫星(1994-),男,硕士生,主要研究方向为云计算安全;叶长河(1993-),男,硕士生,主要研究方向为云计算安全。

全不仅包含了云环境下云平台自身的安全、存储在云基础设施中数据的安全，还包括部署在虚拟机上云应用的安全以及数据在用户端、云端以及云内部转移时的传输安全等。

2.2 云安全的层次划分

云计算安全体系架构十分复杂，覆盖面积广泛。云端和用户均被纳入其安全体系。由于云端的价值更大，因此云端常常是被攻击的重点。但这并不意味着客户端在云中就是安全的，传统的网站挂马等攻击手段依然影响着客户端的安全，同时新型的攻击手段层出不穷，例如文献[2]中针对缓存驱动的攻击就是一般安全手段无法解决的。本文讨论的云安全是在云提供服务时发生的，可以从云服务商的角度对云计算体系架构[3-10]进行层次划分并对不同层次的云安全研究进行分类。具体架构层次及目前的相应安全解决方案如图 2 所示。

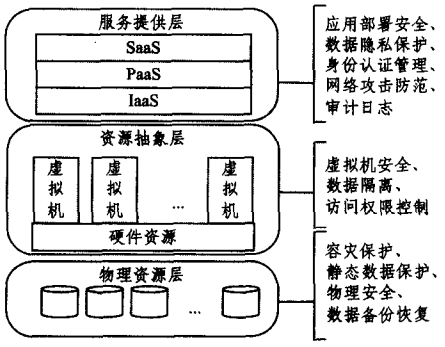

图 2 云安全层次划分及应对措施

架构中的最底层为物理资源层。云的硬件基础是大量的存储介质、计算芯片和传输介质等，这一层次的安全主要表现为容灾保护、静态数据保护和物理安全。

中间层为资源抽象层。为了使底层的硬件资源能够对租户透明，资源抽象层的主要目的是对物理资源进行抽象。这一层次的云安全主要表现为虚拟机的安全，包括多租户环境下的数据隔离、数据访问权限控制和虚拟机自身以及虚拟机之间的安全。

最上层为服务提供层。云计算的服务方式可分为 3 种：IaaS(基础设施即服务)，通过网络向用户提供存储空间、计算机等计算资源，用户可以在这些资源上部署和运行各种软件；PaaS(平台即服务)，为用户提供多环境支持的开发平台，用户可以在该平台上进行开发活动；SaaS(软件即服务)，用户向云服务商租用基于 Web 的软件，用以管理自身的一些活动。在这层中，云安全主要表现为基础设施安全、数据隐私保护、数据传输安全、身份认证管理、网络攻击防范和审计日志等。

3 云体系架构安全的研究进展

3.1 物理资源层

云计算的物理资源层是云提供服务的基础，数据最终都存储在物理设备中，对这些设备的维护及存储数据的备份、恢复技术就显得十分重要。为了提高系统整体的性能并便于维护，物理存储架构通常由控制节点和存储节点构成，其中存储节点负责存放数据，而控制节点负责文件索引、监控存储节点容量以及负载均衡等。典型地，Yahoo 云计算平台采用的分布式文档系统(Hadoop Distribute File System，HDFS)由控制节点 NameNode 和数据节点 DataNode 构成。

为了保证云端物理设备上数据的安全，必须从两方面对数据进行保护，即验证数据的正确性，避免被篡改、删除以及提供数据恢复能力[11]。一般地，数据恢复的方式可以分为 3 种：冗余恢复、副本恢复和备份恢复。冗余恢复是指数据传输中发生宕机时采用的纠错码恢复技术；副本恢复和备份恢复是根据需要处理的数据粒度来划分的。备份恢复是目前比较成熟的技术，它利用备份的数据达到“数据还原”的效果。在检测到数据发生损坏时，将依次采用冗余恢复、副本恢复和备份恢复。

冗余恢复需要增加数据的冗余度，可以直接通过复制数据到多个服务器或用纠删码实现，然而这会存在一定的局限性，例如多服务器数据备份机制虽然简单可靠，但其提高了存储成本，并且大量并发操作可能导致系统整体吞吐量下降；基于纠删码(如 RS 码)的冗余恢复解决方案能够较好地适应并发访问分布式存储系统的情形，但是针对系统故障修复的通信成本太高[12]。文献[13]提出的网络编码纠删码以及功能性数据修复方法通过将数据修复为正常状态而非精确的原始状态，在理论模型层面降低了数据修复的通信成本，然而对系统的全局性能如检索效率会产生不利的影响。文献[14]则主要研究了一种分散式的云存储安全架构，采用信息扩散法、分散存储管理等技术实现分层数据的安全存储和传输，该方法主要是通过定期检查数据片的受损情况来对受损数据进行修复。

副本恢复是在分布式存储环境中存储数据块的副本，通过数据块副本的复制来修复损坏的数据。图 3 示出一个副本恢复应用的流程[15,16]。

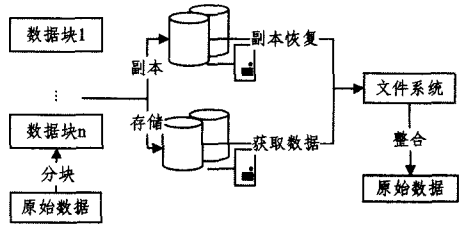

图 3 云存储中数据存储及副本恢复的流程

在该流程中，数据副本的生成和获取与数据的正常存储读取过程是同时进行的。用户数据在提交到云端后会被分割成小数据块，然后被存入不同的物理存储节点并同时进行备份。当用户需要读取数据时，文件系统将根据分块时建立的信息表组合各数据块。当故障发生时，文件系统将使用数据块副本快速进行数据的恢复。这一系列过程对云租户来说都是透明的。

在多租户的云计算数据恢复中，被租户正常删除的数据必须是不可恢复的，否则将会出现恶意恢复数据导致数据泄露的问题。因此针对不同文件系统的数据恢复方式，应当采取对应措施确保被删数据无法恢复[17]。

3.2 资源抽象层

3.2.1 虚拟机安全

资源抽象层对底层硬件进行了抽象，通过在一台物理设备上运行多台虚拟机的方式可以实现资源的共享使用，这是云计算的核心技术之一。多虚拟机同时运行的结构如图 4 所示。

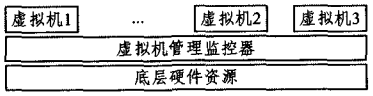

图 4　虚拟机结构

物理资源的有限性要求虚拟机得到合理分配，这是云提供服务的前提条件，优秀的分配算法可以使负载均衡并提高资源利用率，增强云系统的稳定性和高效性。文献[18]根据多目标演化算法提出了一种分配算法：从虚拟机结构图中可以发现抽象后的资源和物理资源之间存在着映射关系，虚拟机使用多资源对象，在优化目标上有多重影响因子，因此可以将虚拟机分配问题看成是多维装箱问题，可采用多目标演化算法来求解。该算法在性能上优于同类的优先匹配启发式算法和基于物理节点数量的单目标简单遗传算法。文献[19]分析了多层应用在不同虚拟机中运行时虚拟机分配遇到的问题，为多层应用设计一个应用资源控制器，该控制器采用反馈控制理论来动态计算虚拟机资源请求，并通过动态的系统识别自动改进资源分配与应用性能的计算模型，大大提高了资源分配效率和性能。文献[20]构造了针对应用服务层目标约束的虚拟机分配优化遗传算法，该算法通过分析应用的负载变化数据和系统日志建立性能模型，并设计虚拟机分配自适应管理框架。该框架相比传统启发式和单目标优化算法降低了应用的虚拟机资源请求违背率，减少了虚拟机的迁移次数。

传统虚拟机由于资源独占性而将安全关注点集中在虚拟机内部。然而在云环境下，即便虚拟软件本身可以提供隔离性保障，也无法保证共享物理资源的虚拟机间的安全，虚拟机一旦开始运行，就会产生诸如虚拟机间的隔离、漏洞、监视等安全问题。例如文献[21]中通过虚拟机之间存在的旁通道发动攻击，并得出预防的最佳措施是使物理资源独享，但这显然是不经济的。对虚拟机的入侵程度进行分析对整个云的安全都有很重要的意义，文献[22]分析了虚拟机的不同层次，提出并验证了一种根据不同的要求对入侵程度进行定义的方法。

在虚拟机的所有攻击中，最致命的是针对其内核的攻击。可采用在虚拟机内部安插写保护安全 hooks、内核内存区域监控等手段来保护虚拟机内核安全。文献[23]提出的安全框架将安全核心组件转移到具有特权的 Dom0 虚拟机上，提取被保护的虚拟机的系统调用、内存使用等情况进行分析决策，在保护用户虚拟机的同时避免恶意攻击安全框架本身而造成威胁。该框架良好的扩展性和性能使其具备了后续的研究价值。

虽然软件是保护虚拟机的常用手段，但是用软件来实现虚拟机的安全效果十分有限，因为安全软件自身大多运行在虚拟机中，对直接威胁虚拟机的攻击不能起到很好的防护，同时也不能保障自身运行的安全。为克服软件安全存在的弊端，引入硬件安全手段是一个行之有效的方法。更进一步，利用可信硬件虽然可以弥补安全软件的不足，但是由于云环境服务长时运行的特点，硬件安全手段必须能有效应对动态运行变化。刘川意等[24]构建了以安全芯片 TPM 为硬件基础的可信计算环境，提出了一种动态的用户运行环境可信性验证机制，该机制采集虚拟机在启动时、运行时的各类信息，并将其交由第三方进行审计，以确认用户的运行环境是否安全。其核心思想如图 5 所示。

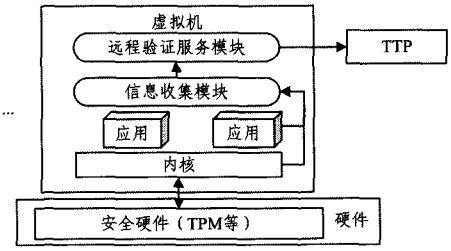

图 5　动态环境可信验证机制

机制启动时，由 TPM 作为可信根保证虚拟机环境安全启动，并将启动信息搜集上报；运行时则会周期性地采集运行信息并上报。远程验证服务模块将信息通过安全的手段发给第三方进行审计。审计方法通常是对载入的内核模块、执行过的程序等信息进行模式匹配以发现异常。

文献[25]设计了一种基于 UEFI 的虚拟机动态安全框架 VirtinSpector，由于 UEFI 程序是以固件形式刷入 UEFI ROM 中并跟随系统启动后被硬件锁定的，因此可以保证 UEFI 的安全。在这个硬件安全前提下，由底层硬件逐级保证上层安全，同时 UEFI 固件安全硬件、安全模块、调度模块、管理模块等与虚拟机之间定时相互验证并度量系统安全性。在运行时，对于虚拟机的特殊动作，需要通过管理模块和其他模块之间的验证才能执行，以动态地保证安全。VirtinSpector 安全框架如图 6 所示。

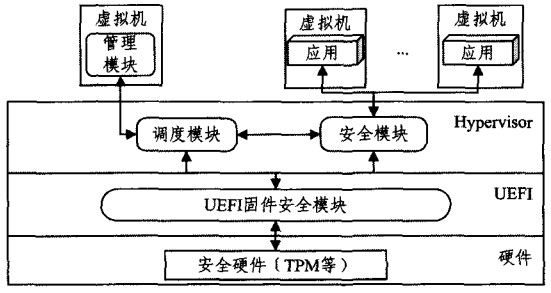

图 6　VirtinSpector 框架

该框架在实践中对虚拟机内、外部攻击做出了良好的反应，并且对系统的资源占用处在一个可接受的范围。不过该框架在解析识别特定操作、监控时效上有缺陷，度量对象的安全状态结果只有安全可信与不可信两种，不能得出精确的定量结论。

综上，云计算中虚拟机的软、硬件安全手段各有优点，表 1 对两种手段进行了对比。实际应用中，通常结合两种安全手段综合实现云虚拟机的安全。

表 1　虚拟机安全手段对比

	软件安全	硬件安全
灵活性	灵活。通过人为配置动态加载安全策略，并可依据安全状况进行相应调整。	固定。属于底层安全手段，无法在运行时进行监控。安全模块在嵌入后不易更改。
安全能力	一般。软件本身运行在虚拟机中，无法保证自身运行安全，同时对攻击虚拟机的行为保护能力有限。	强。基于安全硬件可以构建安全可控的计算环境，且无法被篡改和攻击。
实施复杂度	容易。通过软件安装并取得相应权限即可生效。	复杂。需要软件与硬件的配合，并需要考虑兼容问题。

3.2.2　多租户问题

在资源抽象层还有一个重要的安全点，即租户的隔离问题。云计算的一个重要应用领域是通过互联网提供软件服

务。不同的租户通过租赁的方式即可搭建各自的软件平台。这里涉及到多租户的问题。多租户使用的是部署在同一运行环境下的多台虚拟机，他们共享相同的系统或程序组件。多租户之间的逻辑隔离、访问控制依赖于虚拟机安全，如果不能保证多租户之间的有效隔离，将会导致严重的安全问题。

云计算环境的虚拟和多租户使传统安全手段存在缺乏设备之间统一管理、设备价格高昂、配置工作量巨大、安全需求多样化等问题，而现有数据中心本身存在灵活性不足、抗攻击能力弱等问题[26]。产生这些问题的根本原因是庞大的数据量造成计算节点数量众多、复杂度高，难以管理。因此可以从数据中心的拓扑结构、管理手段等方面提高数据中心的容错性和安全性[27]。

云计算环境中，合理选择云服务提供商是实现多租户技术的前提。一般地，用户更倾向于将数据计算外包给可靠的、知名的云服务商，为了实现云服务商的能力排序，通常需要一个度量框架。文献[28]设计了信任管理系统来度量云服务商的服务能力并帮助用户进行选择，为不同的租户分配资源。另外，可以使用类似的可信第三方 TTP(Trusted Third Party)概念来管理租户和云供应商之间的数据安全。文献[29]提出的基于 TTP 的多租户资源分配算法通过 TTP 提供的数字证书服务，保证云与端之间的原子性、不可否认性、可靠性和正确性，同时也由 TTP 根据一定的算法来为端匹配云资源。

云环境中资源分配后的最突出的问题是访问控制。云计算面临的访问控制问题主要是细粒度的访问控制和密文的访问控制，与常见访问控制手段使密文只对正确用户可见不同，密文访问控制的目的是使得只有正确的对象才可以解密阅读数据。文献[30]从访问控制模型、基于属性的密文访问控制和外包数据的访问控制 3 方面介绍了访问控制的相关技术。

此外，防火墙作为必不可少的安全组件，无论是在访问控制还是安全审计中都起到十分重要的作用。不过云服务商提供资源的最终目的是盈利，而用户希望得到高性价比的服务。如何设计云防火墙使得对用户资源获取效率的影响最小以及调整费用的计算[31]，是迫切需要解决的问题。

云计算中多租户带来的问题是从技术到体制多方面的，包括基础设施安全、数据存储传输安全、应用安全、云服务商管理层面的安全等[32,33]，要切实解决多租户下的安全问题，需要系统、综合地进行研究。

3.3 服务提供层

要确保云计算服务提供层安全，需要建立一条完整的安全保护链。首先要在云端之间建立信任，确保它们之间是可以安全通信的；其次要对传输的数据进行安全保护；最后需要对据存储、用户操作等进行审计。

3.3.1 应用部署

云计算的部署方式通常有公有云、私有云、社区云、混合云 4 种，这 4 种部署方式根据开放的程度，所面临的安全问题各不相同。公有云具有快速、弹性、易扩展的优点，而私有云具有安全性高的特点，混合云结合了两者的优点，因而是当下较为普遍的部署方式。

混合云的安全问题主要包括秘钥管理问题、加密算法选择问题和跨云认证的信任策略 3 个方面。对于秘钥管理问题，可以在私有云内设置秘钥管理系统，或通过在公有云购买虚拟机部署秘钥管理系统，由私有云使用者管理密钥、加解密算法及其过程。在加密算法的选择上，考虑到对称加密算法(如 DES、AES)快、普及的优点，以及非对称算法(如 RSA)安全，但运算量大，无法应用于大数据量的特点，使用混合加密算法是最佳的选择。混合加密算法的思想是数据使用对称加密算法，密钥使用非对称加密算法，同时密钥由密钥管理系统管理，密文由其他设施分开存储，经测试，这样的组合方式可以提高云系统安全性。

在主动防御方面，目前已经大量使用的“云杀毒”技术是通过构建云应用和云服务，将端作为“探针”，搜集上报危险内容，由云负责将应对方法下发到客户端，这种技术可以有效保护云内用户的安全。实际上该技术也存在一定的问题，例如端在上传问题文件 hash 值时很容易受到路径欺骗、通信欺骗和断网攻击。采用类似思想设计的针对恶意代码的系统在传统防范恶意代码的特征码匹配技术捉襟见肘时，可以使客户端对恶意代码起到良好的免疫效果。恶意代码为了实现其目的大都会使用系统调用，这就为监控其攻击行为留下了痕迹。文献[34]提出并实现了一种云主动防御系统，该系统主要通过对程序的系统调用情况进行监控，对恶意代码行为建模，通过分析程序行为实现对异常操作的拦截。该系统结合了云安全的概念，通过在云端建立的恶意代码行为分析系统收集客户端上报的恶意代码行为，证实为恶意代码后建立行为算法代码库并分发给客户端，使得客户端可以参照该算法代码库迅速对恶意代码取得免疫效果。该系统设计如图 7 所示。

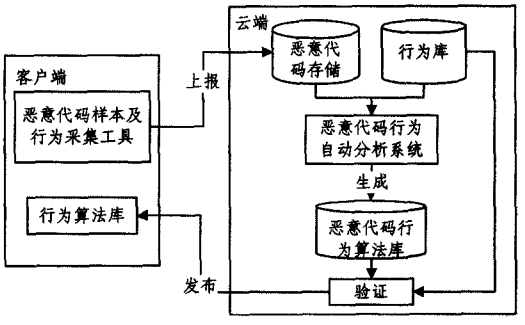

图 7 恶意代码云主动防御系统

使用该系统思想设计的软件具有较强的可实施性，但是由于该防御系统的针对性较强，因此缺点也十分明显。因为是通过监控系统调用来识别恶意代码的，如果恶意代码并未进行系统调用，该防御系统便无法对代码进行静态的查杀；另外，如果恶意代码剥夺了防御系统监控的能力，那么该防御系统将会失去保护能力。

3.3.2 数据处理

传统的数据安全保障一般可以通过加密实现，而单纯的加密对云数据安全则难以奏效。因为在 PaaS 服务和 SaaS 服务阶段对数据的加密和处理无法同时进行，而不加密的云数据的安全就无法得到保障。另外，在云中，单纯使用 RSA 算法会由于计算量过大而造成一些效率上的问题。一些针对 RSA 算法进行改进的研究[35]提升了 RSA 算法的性能，但这是以牺牲一部分安全性为前提的。例如，文献[36]对客户端辅助 RSA 算法(CA-RSA)进行攻击并成功破解了密钥。

“同态加密技术”作为一种能减小频繁的加解密对效率的影响同时也可提高数据安全性的技术，可以在不知道解密函

数的情况下直接对加密数据进行计算，但该算法的设计有一定的难度。文献[37]中就用同态加密技术实现了动态的多副本数据持有性的证明和对多副本数据的修改等多种操作。文献[38]设计的同态加密算法在实现同态加减时效率较高，但是在执行密文检索、乘除时效率较低。对于加密数据的数据挖掘也是一个重要的研究方向。文献[39]为了同时达到数据保密、可查询搜索、隐藏数据访问模式而提出的 K-近邻密文分级协议具有一定的创新性。文献[40]则在关注加密搜索时对安全进行了进一步强化。相对于同态加密技术，文献[41]提出了支持查询的数据加密算法，该算法只需要用户输入查询关键字即可对密文进行不解密搜索；但其缺点在于查询关键字有格式规定，且只支持布尔型查询。文献[42]对查询关键字做了格式放宽，但是也只支持布尔型查询[43]。某些情况下，如果因为云服务商的自私，对于用户的操作请求，云没有“全力”去实现，这对用户来说是不可接受的。“可验证”便成为用户的一个要求。结合上述对加密数据的处理技术，文献[44]提出的策略可以对加密的数据进行可验证的模糊关键字搜索。

无证书公钥加密技术可以解决秘钥、证书的托管问题，但是在效率和抗部分解密攻击上有所不足。文献[45]提出的无证书加密技术中，由云提供给数据上传者公钥用于加密敏感信息，只有经过云端和数据拥有者的共同解密才能完整解密数据，而两者均不能独自完全解密数据。数据关系隐藏法的出现可以做到尽量对数据少加密。该方法的主要思想就是将明文数据分片存储，隐藏它们之间的关系。不过该方法会造成一定程度的数据丢失；此外，其把数据保护工作交由租户端完成，会增加租户端的计算负担。利用数据关系隐藏法，文献[46]将数据进行分片后存储到不同的云服务商，并仅对其中的敏感信息进行加密以提高系统效率。考虑到租户的计算负担，实际上可以将数据关系隐藏的任务交由第三方来处理，则改进后的模型的工作流程如图 8 所示。

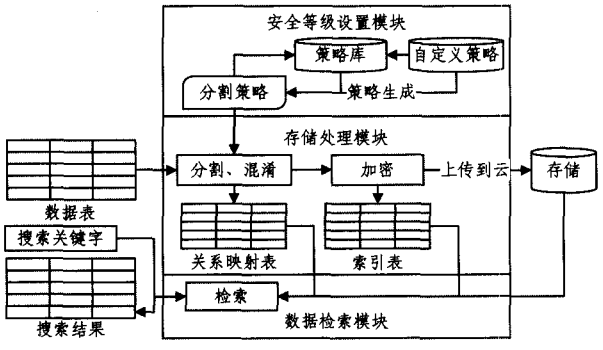

图 8　数据处理可信第三方模型

在该模型中，由安全等级设置模块确定分割策略；第三方的数据存储处理模块根据策略对数据进行混淆关系计算；数据搜索模块搜索数据并完成数据的重组。该模型依照自定义的策略仅对敏感类信息进行加密，这样可以在数据安全的前提下提高系统的运行效率；同时将分片数据存储在不同的服务商，以防止云服务商的高概率猜测攻击而泄漏租户隐私。

文献[47]将数据的切片思想细化到了位的程度，在数据上传前将字节中的某几位进行移位，然后分别存储在不同的文件中。操作过程如下：

1)读数据过程。从文件中读入 2 个字节的数据。

2)拆分、移位过程。分别分离两个数据的高 4 位和低 4 位，并将高 4 位与低 4 位数据调换顺序。将原来的高 4 位变为低 4 位；原来的低 4 位变为高 4 位。

3)重组过程。将第一个数据的高 4 位和第二个数据的低 4 位相加，重组成一个新的数据；将第一个数据的低 4 位和第二个数据的高 4 位相加，重组成一个新的数据。

4)写数据过程。把得到的新的数据分别写入文件 1 和文件 2 中。

5)判断是否到文件尾，如果未到文件尾，重复 1)－5)的过程；如果已经到达文件尾，则结束。

合并数据时的操作是上述过程的逆过程。文献中对该方法进行了详细的评估，发现其比传统加密算法的效率要高 25～35 倍。

3.3.3　身份控制

云计算提供给用户应用软件、数据、操作系统等可由用户自主控制的资源，而这些资源不仅仅属于单一用户，因此要对用户的访问进行控制，防止被劫持的用户恶意或者无意地对云安全进行有威胁的操作。访问控制模型的研究由来已久，比较热门的访问控制模型有基于任务的访问控制模型(TBAC)、基于属性模型的云计算访问控制(ABAC)、基于 UCON 模型的云计算访问控制、基于 BLP 的模型，以及在这些基础上进行扩展应用的云计算环境下的 RBAC[48] 和基于 XML 的 RBAC 分布式访问控制架构[49]等。

云计算用户具有不同的、动态变化的安全管理域和安全边界，传统的身份认证访问控制技术无法应对如此动态、大量的多租户访问控制需求。用户的动态性决定了固定的控制技术不可行，因此需要设计动态的访问控制手段。基于此，文献[50,51]均提出了基于行为的访问控制模型。文献[51]中除利用 BLP 模型保证数据的保密性和利用 Biba 模型保证数据的完整性外，还在权限和行为上进行访问控制。然而该模型会大大降低云资源的可用性。文献[52]设计的基于用户行为信任的控制模型可以在一定程度上缓解这个问题。通过动态监测用户的访问行为，评估出行为信任度，并依据信任度为其分配服务等级与访问权限。模型的工作过程如图 9 所示。

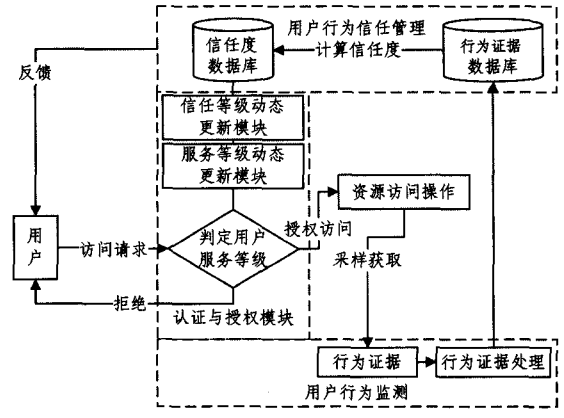

图 9　动态访问控制模型架构

该模型的核心为 3 大模块：用户行为监测中心、用户行为信任管理中心和认证与授权中心。其中用户行为监测负责监控和获取用户行为，为用户行为信任管理中心动态评估用户信任度提供参数，用户行为信任度将是认证与授权中心实时

设定用户权限的依据。设计该模型的关键在于建立一套从数据采集到分析授权的完整可用的信任评估及授权体系。在综合考虑了基于角色、任务、行为和信任等访问控制方法后，文献[53]提出的 AMAC 访问控制模型集合了角色、上下文、行为等访问控制要素的优点，为用户授予资源的动态访问控制权限提供了一种理想的方式。此外，静态的访问控制技术凭借在可操作性方面的优势，仍将是身份控制技术的重要部分。

“基于属性”的概念近年来备受关注，基于属性的加密签名技术可以通过使加密文件由多个同属性接受对象解密而提高系统访问效率、增强访问控制灵活性等[54,55]。基于属性的签名技术的主要思想是，用户加密所用的属性集与用户解密所用的属性集相交结果超过门限值就可以解密。文献[56]在此基础上引入了净化技术，提出了基于属性的可净化签名方案。净化就是对数据进行二次处理，隐藏掉其中部分信息。如图 10 所示，该方案包括 5 个参与方：数据提供者(签名者)，数据净化者，可信授权中心，云存储服务器和云端用户。

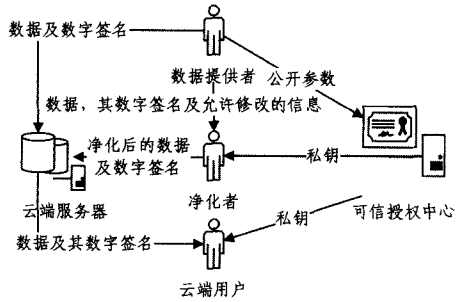

图 10　可净化系统模型

系统中，可信授权中心负责公钥秘钥的管理，数据提供者将数据以及签名上传，并允许净化者对敏感信息进行净化签名。云端用户下载数据时通过公钥与属性完成对数据的验证。研究方案对具体算法进行了详细的设计，以保证用户匿名性和敏感数据的隐藏，同时减少了与数据提供者的交互，从而更加适应云环境。密文策略基于属性加密，通过属性标明用户身份，同时密文与访问结构直接关联。

基于属性的加密由于属性常常属于多个实体，将会导致属性在撤销时牵连到其他拥有该属性的实体。这一问题在密文策略的基于属性加密中更为严峻。文献[57,58]提出了类似的方案，较好地解决了属性牵连问题，基本思想是：为同属性的用户建立属性组，组内分配共享的组秘钥。组内某个用户撤销属性时使用加密广播的方式发布新组秘钥，同时更新基于旧的秘钥加密的数据，以保证退出组的用户无法访问新数据，新加入以及留下的组内用户可以继续访问所有数据。系统中，唯一的可信机构为系统产生公钥和私钥参数，并根据用户的属性为其授予不同的访问权限。数据拥有者采用密文策略将属性加密后的数据传到服务器，服务器存储数据文件，负责管理用户对密文的访问，为每一个属性组生成组密钥。当一个属性撤销时，云服务器重新生成该属性组的密钥，并用该密钥去更新与该属性相关的密文组件。这样在保证“轻客户端”的前提下实现了访问控制。相关研究[59]显示，采用基于身份的加密技术设计的数据访问控制服务在安全性方面可以获得提高，同时也易于扩展。

从上述研究成果可以发现，近年来对访问控制的研究热点在于对传统访问控制模型的改进，使其更适合云计算的环境，针对云计算特征的访问控制技术评价需要从多个方面进行。为此参照相关成果并设定了 11 个性能指标：授权(模型对用户授权)、特权分配(为完成任务而赋予的特权)、职责分离度(满足职责分离原则程度)、易描述性(模型形式化描述)、控制粒度(对数据的控制粒度划分)、云属性参与度(云环境属性的关联程度)、约束能力(对模型各个环节的约束限制能力)、适应性(对云环境的适应性)、兼容性(模型兼容性)、扩展性(模型扩展性)、维护性(模型易维护性)。相关典型的访问控制技术性能比较如表 2 所列。

表 2　云计算中访问控制模型的性能对比

	RBAC	TBAC	ABAC	T-RBAC	基于信任的访问控制机制	UCON
授权	灵活		一般	灵活	灵活	灵活
特权分配	最小	最小		最小	一般	
职责分离度	一般	高		高		
易描述性	优		优	优	良	优
控制粒度			细	细	细	细
云属性参与度		一般	高	高	高	一般
约束能力	一般			强		
适应性		一般	强	强	强	强
兼容性			强	强	一般	强
扩展性			强	强	强	强
维护性	易					

3.4　审计技术

当数据以外包的形式存储在云平台中时，用户一般会重点关注两个问题：数据是否确实存储成功并能被安全和有效控制，以及是否除了授权用户外任何人不能修改数据。在实际云安全操作中，针对租户数据安全问题，最重要的是通过安全审计对操作数据的行为进行监控与记录，与其他安全手段一起保障云数据的安全。对云数据的审计显然不能将数据下载下来，同时云计算具有的商业特性使得租户并不希望数据被外人审计。因此，审计是云安全实施过程中的双刃剑。

云存储审计过程通过对数据的完整性和可用性进行检查，验证数据是否安全[60-64]。目前针对云计算审计的方法主要有特征匹配法、状态转移法、神经网络技术法、基于代理法、基于数据挖掘法，但它们普遍存在准确率不高、速度慢、自更新能力差等缺点。这些方法的解决思路是：取回少量的数据，以某种证明协议或分析手段判断云数据是否完整、安全。采用数据持有性证明算法可以对数据的状态进行验证，该算法在数据持有者和云服务提供商间制定协议，并将数据的状态反馈给数据持有者。粗略来讲，目前相关方案主要分 3 类。

1)“哨兵方案”：在文件中随机融入若干无法与文件内容区分的“哨兵”，协议执行时要求云服务提供商返回哨兵的位置。

2)哈希运算方案：对文件分块计算哈希值，协议执行时要求云服务提供商返回某组的哈希值。

3)同态标签方案：对文件分块计算同态标签，协议执行时要求云服务商提供若干文件块的同态标签。

依赖可信第三方进行审计是目前较为高效的手段，文献[65]利用可信第三方设计了动态的数据完整性审计框架，并对其进行了多向扩展。其数据完整性审计的模式归纳为图 11 所示。

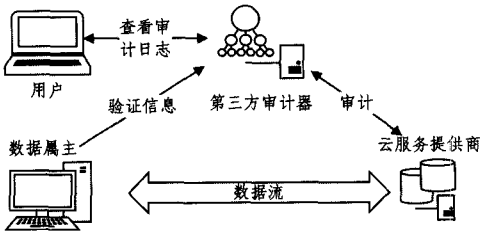

图 11　数据完整性审计模型

模型中，用户可能是数据的唯一持有人，也可能是部分数据的持有人。第三方审计器的作用是代替用户进行审计，依靠第三方审计的优点是第三方可以具备比用户更强大的审计能力，可以达到审计的目标。

云安全审计通过对云环境下各个部分的运行状况进行审查，来发现系统漏洞、恶意攻击、非法操作等。安全审计一般包括审计信息采集、信息传输、信息持久存储、信息处理几个部分[66]。采集的信息可以是系统日志、网络流量、操作系统信息等异构信息，因此还需要进行数据清洗。对信息进行持久化存储的好处是方便进行实时和事后审计，并为安全处理动作提供证据。目前成熟的安全审计系统的设计思想如图 12 所示。

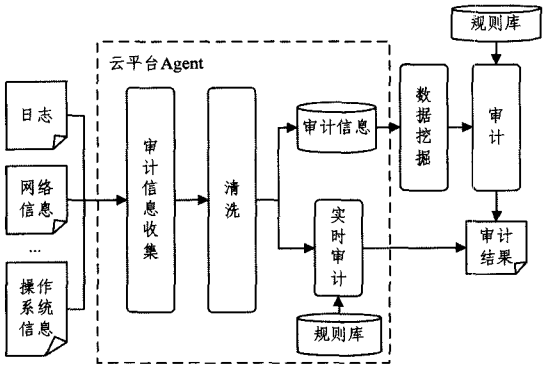

图 12　安全审计系统模型

该系统模型中，通过代理等手段获取到各类审计信息，经过清洗后存储，由审计中心进行安全审计，并告知系统管理员或用户系统出现的问题。然而云服务商通常不愿意将系统日志等重要数据交由外部进行审计，而服务商对内部进行审计的结果并不一定会做到公正、公开的处理。因此需要设法尽量少采集数据或者采集云服务商愿意提供的数据进行审计，这一思路是可行的，例如虚拟机旁路攻击时其他用户内存的变化[67]、SQL 攻击时造成的日志文件大小急剧增加、DDoS 攻击时新增的 IP 地址来源异常[68]等特征是云服务商可以提供的。但是由于此类数据的准确性终究不如日志等信息，即便识别出攻击，在攻击定位和处理方面仍有提升空间，目前通常作为一种辅助审计的手段。

结束语　云计算安全问题的根本是租户的安全应用环境和服务提供商的诚信、责任和约束等问题，并最终归因于云计算体系架构和相关安全模型、技术和方案的有效实现问题。建立有效、全面的云计算安全体系架构是云计算走向实际应用的关键。本文针对云计算服务体系数据、计算外包和大规模分布式架构的特点，将云计算服务划分为物理资源层、资源抽象层和服务提供层，依据该划分定义了数据安全、虚拟机安全、多租户隔离、应用部署安全、数据处理技术、身份控制技术以及审计技术，分层介绍了所包含的云安全关键问题，综述了云安全问题近几年研究的最新技术和进展，指出了云计算体系架构安全领域的重大挑战与发展契机。

参 考 文 献

[1] Phaphoom N, Wang Xiao-feng, Samuel S, et al. A survey study on major technical barriers affecting the decision to adopt cloud services[J]. The Journal of Systems and Software, 2015, 103: 167-181

[2] Lai Yeu-pong, Wu Wei-feng. The defense in-depth approach to the protection for browsing users against drive-by cache attacks [J]. Security and Communication Networks, 2015, 8(7): 1422-1430

[3] Feng Deng-guo, Zhang Min, Zhang Yan, et al. Study on Cloud Computing Security[J]. Journal of Software, 2011, 22(1): 71-83 (in Chinese)
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

[4] Xiao Zhi-feng, Xiao Y. Security and Privacy in Cloud Computing [J]. IEEE Communications Surveys and Tutorials, 2012, 15(2): 843-859

[5] Ali M, Khan S U, Vasilakos A V. Security in Cloud Computing: Opportunities and Challenges[J]. Information Sciences, 2015, 305: 357-383

[6] Fernandes D A B, Soares L F B, Gomes J V, et al. Security Issues in Cloud Environments: a Survey[J]. International Journal of Information Security, 2014, 13(2): 113-170

[7] Albakri S H, Shanmugam B, Samy G N, et al. Security Risk Assessment Framework for Cloud Computing environments[J]. Security and Communication Networks, 2014, 7(11): 2114-2124

[8] Spillner J, Müller J, Schill A. Creating optimal cloud storage systems[J]. Future Generation Computer Systems, 2013, 29(4): 1062-1072

[9] Youssef A E, Alageel M. A Framework for Secure Cloud Computing[J]. International Journal of Computer Science Issues, 2012, 9(3): 487-500

[10] Roy A, Sarkar S, Ganesan R, et al. Secure the Cloud: From the Perspective of a Service-Oriented Organization[J]. ACM Computing Surveys, 2015, 47(3): 326-328

[11] Chen Lan-xiang, Xu Li. Research on Provable Data Possession and Recovery Technology in Cloud Storage[J]. Journal of Computer Research and Development, 2012, 49(z1): 19-25 (in Chinese)
陈兰香，许力. 云存储服务中可证明数据持有及恢复技术研究[J]. 计算机研究与发展，2012，49(z1)：19-25

[12] Dimakis A G, Godfrey P B, Wainwright M J, et al. Network Coding for Distributed Storage Systems[J]. IEEE Transactions on Information Theory, 2010, 56(9): 4539-4551

[13] Wu Y. A Construction of Systematic MDS Codes With Minimum Repair Bandwidth[J]. IEEE Transactions on Informatio Theory, 2011, 57(6): 3738-3741

[14] Bian Gen-qing, Gao Song, Shao Bi-lin. Security Structure of Cloud Storage based on Dispersal[J]. Journal of Xian Jiaotong University, 2011, 45(4): 41-45(in Chinese)
边根庆，高松，邵必林. 面向分散式存储的云存储安全框架[J]. 西安交通大学学报，2011，45(4)：41-45

[15] Xiang F, Liu C Y, Fang B X, et al. Novel "Rich Cloud" Based Data Disaster Recovery Strategy[J]. Journal on Communications, 2013(6): 92-101(in Chinese)
项菲，刘川意，方滨兴，等. 新的基于云计算环境的数据容灾策略

[J]. 通信学报,2013(6):92-101

[16] Fabian B, Ermakova T, Junghanns P. Collaborative and Secure Sharing of Healthcare Data in Multi-clouds[J]. Information Systems,2015,48:132-150

[17] Li Hui, Sun Wen-hai, Li Feng-hua, et al. Secure and Privacy-Preserving Data Storage Service in Public Cloud[J]. Journal of Computer Research and Development, 2014, 51(7): 1397-1409 (in Chinese)
李晖,孙文海,李凤华,等. 公共云存储服务数据安全及隐私保护技术综述[J]. 计算机研究与发展,2014,51(7):1397-1409

[18] Ai Hao-jun, Gong Su-wen, Yuan Yuan-ming. Research of Cloud Computing Virtual Machine Allocated Strategy on Multi-object Evolutionary Algorithm[J]. Computer Science, 2014, 41(6): 48-53(in Chinese)
艾浩军,龚素文,袁远明. 基于多目标演化算法的云计算虚拟机分配策略研究[J]. 计算机科学,2014,41(6):48-53

[19] Wen Yu, Meng Dan, Zhan Jian-Feng. Adaptive Virtualized Resource Management for Application's SLO Guarantees[J]. Journal of Software, 2013(2): 358-377(in Chinese)
文雨,孟丹,詹剑锋. 面向应用服务级目标的虚拟化资源管理[J]. 软件学报,2013(2):358-377

[20] Li Qiang, Hao Qin-fen, Xiao Li-ming, et al. Adaptive Management and Multi-Objective Optimization for Virtual Machine Placement in Cloud Computing[J]. Chinese Journal of Computers, 2011, 34(12): 2253-2264(in Chinese)
李强,郝沁汾,肖利民,等. 云计算中虚拟机放置的自适应管理与多目标优化[J]. 计算机学报,2011,34(12):2253-2264

[21] Ristenpart T, Tromer E, Shacham H, et al. Hey, you, 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. New York: ACM Press, 2009:199-212

[22] Arshad J, Townend P, Xu J. A novel intrusion severity analysis approach for Clouds[J]. Future Gen Computer Systems, 2013, 29(1):416-428

[23] Lai Ying-xu, Hu Shao-long, Yang Zhen. Research of Security technology based on Virtualization[J]. Journal of University of Science and Technology of China, 2011, 41(10): 907-914(in Chinese)
赖英旭,胡少龙,杨震. 基于虚拟机的安全技术研究[J]. 中国科学技术大学学报,2011,41(10):907-914

[24] Liu Chuan-yi, Lin Jie, Tang Bo. Dynamic Trustworthiness Verification Mechanism for Trusted Cloud Execution Environment [J]. Journal of Software, 2014, 25(3): 662-914(in Chinese)
刘川意,林杰,唐博. 面向云计算模式运行环境可信性动态验证机制[J]. 软件学报,2014,25(3):662-674

[25] Yan Fei, Shi Xiang, Li Zhi-hua, et al. VirtinSpector: A UEFI Based Dynamic Secure Measurement Framework for Virtual Machine[J]. Journal of Sichuang University (Engineering Science Edition), 2014, 46(1): 22-28(in Chinese)
严飞,石翔,李志华,等. VirtinSpector:一种基于UEFI的虚拟机动态安全度量框架设计与实现[J]. 四川大学学报(工程科学版),2014,46(1):22-28

[26] Bari M F, Boutaba R, Esteves R, et al. Data Center Network Virtualization: A Survey[J]. Communications Surveys & Tutorials, IEEE, 2013, 15(2): 909-928

[27] Luo Jun-zhou, Jin Jia-hui, Song Ai-bo, et al. Cloud Computing: Architecture and Key Technologies[J]. Journal on Communications, 2011, 32(7): 3-21(in Chinese)
罗军舟,金嘉晖,宋爱波,等. 云计算:体系架构与关键技术[J]. 通信学报,2011,32(7):3-21

[28] Habib S M, Ries S, Mühlhäuser M, et al. Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source[J]. Security Comm. Networks, 2014, 7(11): 2185-2200

[29] Wang Pei-xue, Zhou Hua-qiang. Research on Cloud Security Model Based on Trusted Third Party on Multi-tenant Environment[J]. Computer Science, 2014, 41(6A): 363-365, 382(in Chinese)
王佩雪,周华强. 多租户环境下基于可信第三方的云安全模型研究[J]. 计算机科学,2014,41(6A):363-365,382

[30] Feng Chao-sheng, Qin Zhi-guang, Yuan Ding, et al. Key Techniques of Access Control for Cloud Computing[J]. Acta Electronica Sinica, 2015, 43(2): 312-319(in Chinese)
冯朝胜,秦志光,袁丁,等. 云计算环境下访问控制关键技术[J]. 电子学报,2015,43(2):312-319

[31] Liu M, Dou W, Yu S, et al. A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(3): 621-631

[32] Liu Guo-ping, Liu Jian-feng, Tan Guo-quan. Research on Security Technology of Multi-Tenanted SaaS Service[J]. Telecommunications Science, 2011(SI): 11-15(in Chinese)
刘国萍,刘建峰,谭国权. 多租户 SaaS 服务安全技术研究[J]. 电信科学,2011(S1):11-15

[33] Ju Jie-hui, Wu Ji-yi, Zhang Jian-lin, et al. Study on Multi-Tenancy and Security Technology in SaaS Applications[J]. Telecommunications Science, 2010, 26(10): 41-46(in Chinese)
琚洁慧,吴吉义,章剑林,等. SaaS 应用中的多租户与安全技术研究[J]. 电信科学,2010,26(10):41-46

[34] Zou Hang, Chen Zhuang, Li Xue-ping. Design and Implementation of Security Cloud Active Defence System Against Malicious Code[J]. Journal of Chongqing University of Technology(Natural Science), 2014, 28(5): 84-92(in Chinese)
邹航,陈庄,李雪平. 恶意代码云主动防御系统设计与实现[J]. 重庆理工大学学报(自然科学),2014,28(5):84-92

[35] Dan B, Shacham H. Fast Variants of RSA[J]. CryptoBytes, 2002, 5: 1-9

[36] Li Yun-fei, Liu Qing, Li Tong, et al. Cryptanalysis against an Improved RSA Algorithm[J]. Journal of Applied Science, 2013, 31(6): 655-660(in Chinese)
李云飞,柳青,李彤,等. 对一种改进 RSA 算法的密码分析[J]. 应用科学学报,2013,31(6):655-660

[37] Mukundan R, Madria S, Linderman M. Efficient integrity verification of replicated data in cloud using homomorphic encryption [J]. Distributed and Parallel Databases, 2014, 32(4): 507-534

[38] Huang Ru-wei, Gui Xiao-lin, Yu Si, et al. Privacy-Preserving Computable Encryption Scheme of Cloud Computing[J]. Chinese Journal of Computers, 2011, 34(12): 2391-2402(in Chinese)
黄汝维,桂小林,余思,等. 云环境中支持隐私保护的可计算加密方法[J]. 计算机学报,2011,34(12):2391-2402

[39] Samanthula B K, Elmehdwi Y, Wei Jiang. k-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data[J]. IEEE Transactions on Knowledge And Data Engineering, 2015, 27(5): 1261-1273

[40] Yu Jia-di, Lu P, Zhu Y, et al. Toward Secure Multikey word Top- k Retrieval over Encrypted Cloud Data[J]. Dependable and Secure Computing, 2013, 10(4): 239-250

[41] Song D X, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]// IEEE Sym on Security and Privacy. 2000: 44-55

[42] Li J, Wang Q, Wang C. Fuzzy keyword search over encrypted data in cloud computing[J]. Infocom, 2009(2): 1-5

[43] Feng Chao-sheng, Qin Zhi-guang, Yuan Ding. Techniques of Secure Storage for Cloud Data[J]. Chinese Journal of Computers, 2015, 38(1): 150-163(in Chinese)
冯朝胜,秦志光,袁丁. 云数据安全存储技术[J]. 计算机学报, 2015, 38(1): 150-163

[44] Wang Jian-feng, Ma H, Tang Q, et al. Efficient Verifiable Fuzzy Keyword Search over Encrypted Data in Cloud Computing[J]. Computer Science and Information Systems, 2013, 10(2): 499-505

[45] Seo S H, Nabeel M, Ding Xiao-yu, et al. An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(9): 2107-2119

[46] Hudic A, Islam S, Kieseberg P, et al. Data Confidentiality using Fragmentation in Cloud Computing[J]. International Journal of Pervasive Computing & Communications, 2013, 9(1): 37-51

[47] Sun Xin-wei, Zhang Wei, Xu Tao. High-performance Data Privacy Protection for Cloud[J]. Computer Science, 2014, 41(5): 137-142(in Chinese)
孙辛未,张伟,徐涛. 面向云存储的高性能数据隐私保护方法[J]. 计算机科学, 2014, 41(5): 137-142

[48] Yang Liu, Tang Zhuo, Li Ren-fa, et al. Roles query algorithm in cloud computing environment based on user require[J]. Journal on Communications, 2011, 32(7): 169-175(in Chinese)
杨柳,唐卓,李仁发,等. 云计算环境中基于用户访问需求的角色查找算法[J]. 通信学报, 2011, 32(7): 169-175

[49] Almutairi A, Sarfraz M, Basalamah S, et al. A Distributed Access Control Architecture for Cloud Computing[J]. IEEE Software, 2012, 29(2): 36-44

[50] Antonio M, Javie G, Antonio M. A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications[J]. Computer Journal, 2012, 55(8): 979-994

[51] Lin Guo-yuan, He Shan, Huang Hao, et al. Access control security model based on behavior in cloud computing environment[J]. Journal on Communications, 2012(3): 59-66(in Chinese)
林果园,贺珊,黄皓,等. 基于行为的云计算访问控制安全模型[J]. 通信学报, 2012(3): 59-66

[52] Liu Wu, Duan Hai-xin, Zhang Hong, et al. TRBAC: Trust Based Access Control Model[J]. Journal of Computer Research and Development, 2011, 48(8): 1414-1420(in Chinese)
刘武,段海新,张洪,等. TRBAC:基于信任的访问控制模型[J]. 计算机研究与发展, 2011, 48(8): 1414-1420

[53] Xiong Jin-bo, Yao Zhi-qiang, Ma Jian-feng, et al. Action Based Multilevel Access Control for Structure Document[J]. Journal of Computer Research and Development, 2013, 50(7): 1399-1408(in Chinese)
熊金波,姚志强,马建峰,等. 基于行为的结构化文档多级访问控制[J]. 计算机研究与发展, 2013, 50(7): 1399-1408

[54] Hur J. Improving Security and Efficiency in Attribute-Based Data Sharing[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(10): 2271-2282

[55] Li M, Yu Shu-cheng, Zheng Y, et al. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1): 131-143

[56] Liu Xi-meng, Ma Jian-feng, Xiong Jin-bo, et al. Attribute Based Sanitizable Signature Scheme in Cloud Computing[J]. Journal of Electronics & Information Technology, 2014, 36(7): 1749-1754 (in Chinese)
刘西蒙,马建峰,熊金波,等. 云计算环境下基于属性的可净化签名方案[J]. 电子与信息学报, 2014, 36(7): 1749-1754

[57] Chen Yan-li, Song Ling-ling, Yang Geng. Efficient Access Control Scheme Combining CP-ABE and SD in Cloud Computing [J]. Computer Science, 2014, 41(9): 152-157, 168(in Chinese)
陈燕俐,宋玲玲,杨庚. 基于 CP-ABE 和 SD 的高效云计算访问控制方案[J]. 计算机科学, 2014, 41(9): 152-157, 168

[58] Liu Xue-feng, Zhang Yu-qing, Wang Bo-yang, et al. Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191

[59] Dong X, Yu J D, Zhu Y M, et al. SECO: Secure and Scalable Data Collaboration Services in Cloud Computing[J]. Computers and Security, 2015, 50: 91-105

[60] Tan Shuang, Jia Yan, Han Wei-hong. Research and Development of Provable Data Integrity in Cloud Storage[J]. Chinese Journal of Computers, 2015, 38(1): 164-177(in Chinese)
谭霜,贾焰,韩伟红. 云存储中的数据完整性证明研究及进展[J]. 计算机学报, 2015, 38(1): 164-177

[61] Chang Chin-chen, Sun Chin-yu, Cheng Ting-fang. A Dependable Storage Service System in Cloud Environment [J]. Security and Communication Networks, 2015, 8(4): 574-588

[62] Lei X Y, Liao X F, Huang T W, et al. Achieving Security, Robust Cheating Resistance, and High-efficiency for Outsourcing Large Matrix Multiplication Computation to a Malicious Cloud [J]. Information Science, 2014, 280: 205-217

[63] Wang B Y, Li H, Liu X F, et al. Efficient Public Verification on the Integrity of Multi-Owner Data in the Cloud[J]. Journal of Communications and Networks, 2014, 16(6): 592-599

[64] An Bao-yu, Gong Zhe, Xiao Da, et al. Data possession audit with an implicit trusted third-party for cloud storage[J]. Journal of Harbin Engineering University, 2012, 33(8): 1039-1045(in Chinese)
安宝宇,宫哲,肖达,等. 具有隐式可信第三方的云存储数据持有性审计[J]. 哈尔滨工程大学学报, 2012, 33(8): 1039-1045

[65] Yang K, Jia X H. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing[J]. IEEE Transactions on Parallel and Distributed, 2013, 24(9): 1717-1726

[66] Wang Q, Wang C, Li J, et al. Enabling Public Verifiability and Data Dynamics for Storage Security. [J]. Lecture Notes in Computer Science, 2009, 22(5): 355-370

[67] Milan R M. Researchers find a new way to attack the cloud[EB/OL]. (2011). http://www.computerworld.com/article/2528070/cloud-computing/researchers-find-a-new-way-to-attack-the-cloud.html

[68] Zhang Yong-zheng, Xiao Jun, Yun Xiao-chun, et al. DDoS Attacks Detection and Control Mechanisms[J]. Journal of Software, 2012, 23(8): 2058-2072(in Chinese)
张永铮,肖军,云晓春,等. DDoS 攻击检测和控制方法[J]. 软件学报, 2012, 23(8): 2058-2072