文章编号:1671-9352(2014)09-0083-07 DOI:10.6040/j.issn.1671-9352.2.2014.262

云计算中的数据隐私保护研究

蔡红云,田俊峰
(河北大学数学与计算机学院,河北 保定 071002)

摘要: 云计算是当前IT领域正在发生的深刻变革,它在提高使用效率和降低使用成本的同时,带来了极大的安全挑战,其中隐私保护问题首当其冲。分析了云计算中隐私风险产生原因,指出了云计算中隐私保护应解决的关键问题,回顾并总结了当前国内、外在云隐私保护领域的主流技术及研究现状,探讨了云隐私保护领域仍然存在的问题并对未来研究方向进行了展望。

关键词: 云计算; 隐私风险; 隐私保护
中图分类号: TP393 **文献标志码:** A

Research of data privacy protection for cloud computing

CAI Hong-yun, TIAN Jun-feng
(College of Mathematics and Computer, Hebei University, Baoding 071002, Hebei, China)

Abstract: Cloud computing is a fundamental change happening in the field of information technology. It can improve the efficiency and reduce the cost, while it also brings great challenges in the field of data security. Among these challenges, how to protect data privacy for cloud consumers has been a key problem. In this paper, the reasons that could cause privacy risk were analyzed, and the key issues of privacy protection for cloud computing were proposed, then the mainstream technologies and present situation were reviewed and summarized, final the problems which existed in the present were discussed and prospects for some future research directions were analyzed.

Key words: cloud computing; privacy risk; privacy protection

0 引言

云计算的产生借鉴了传统分布式计算的思想,将大量计算资源、存储资源与软件资源链接在一起,形成巨大规模的共享虚拟资源池,体现了“网络就是计算机”的思想[1]。作为一种新兴的计算模式,云计算已成为当前产业界、学术界、政府等各界均十分关注的焦点。在云计算框架中,所有的资源以服务的形式交付给用户,用户对云资源就如同用水、电一样按需购买。根据云平台基础设施的部署方式,当前的云计算平台可分为:私有云(private cloud)、公有云(public cloud)及混合云(hybrid cloud)。私有云是指企业自己搭建的云平台架构,企业拥有基础架构的自主权,面向内部用户或外部客户提供云服务,因此云用户能够控制用户数据的访问并且只授权给用户所信任的团体;公有云是指由专业云服务商搭建云平台基础架构,直接向外部云用户提供相应的云服务,云用户并不拥有云计算及存储资源,而是将存储和计算外包给云服务提供商,如Amazon EC2、阿里云等。混合云是指私有云和公有云的结合,由两个或更多云端系统组成云端基础设施。

收稿日期:2014-06-24; 网络出版时间:2014-08-27 11:54
网络出版地址:http://www.cnki.net/kcms/doi/10.6040/j.issn.1671.9352.2.2014.262.html
基金项目:国家自然科学基金资助项目(61170254);河北省自然科学青年基金资助项目(F2014201165)
作者简介:蔡红云(1980-),女,副教授,硕士,研究方向为网络安全与可信计算. E-mail:chy_hbu@126.com

在混合云中,用户关键数据存放在私有云,但当私有云工作负载过重时,为保证服务质量,也会将部分数据迁移到公有云上。

在公有云和混合云中,存储和计算的外包意味着数据的外包,数据属主将数据外包给一个不信任的云服务提供商,数据的隐私性和安全性问题成为云用户的安全忧虑[2],这个忧虑也是阻碍云计算技术普及的最大障碍。全球技术研究和咨询公司 Gartner 2009 年的调查结果显示,70% 以上受访企业的 CTO 认为不采用云计算的首要原因在于存在数据安全性与隐私性的忧虑。随后 Google、MediaMax 和 Salesforce.com 等云服务商泄漏或丢失用户数据的事实也进一步证实了人们的担心[3]。然而由于全球经济面临金融压力,企业和组织被迫降低运营成本,Gartner 在 2011 年针对 IT 机构和用户发布了 2012 年及未来重大预测,认为到 2016 年底,将会有超过 50% 的全球 1000 家公司将客户敏感数据存储在公共云或混合云中[4]。尽管近些年,云安全联盟(cloud security alliance,CSA)等业界代表已经发布了一系列基于传统 IT 技术的云安全加强措施,并不断扩大研究的覆盖范围,然而 2013 年 6 月美国国家安全局(NSA)窃取数据的秘密文件的曝光又重新引起了人们对存储在云中数据安全的担忧。Gartner 在最近的调查统计中也指出安全和隐私问题仍然是妨碍许多企业采用云服务的最关键因素。

1 云计算中的隐私风险

隐私是指自然人自身所享有的与公众利益无关并不愿他人知悉的私人信息,最早是由美国法学家沃伦(Samuel D. Warren)和布兰德斯(Louis D. Brandeis)于 1890 年在《哈佛法律评论》发表的“论隐私权”文中提出的,后来逐渐得到全世界各国的普遍认同。云计算环境中用户的隐私数据即秘密数据,是不想被他人获知的信息。从隐私所有者的角度,可将隐私数据分为个人隐私数据和共同隐私数据,个人隐私数据包括可用来识别或定位个人的信息(如电话号码、地址、信用卡号、认证信息等)和敏感的信息(如个人的健康状况、财务信息、历史访问记录、公司的重要文件等);共同隐私不仅包含个人的隐私,还包含所有公共属性共同表现出但不愿被暴露的信息,如公司员工的平均薪资、薪资分布等。云中隐私数据存在泄漏和被跟踪的隐私风险,原因有以下几点:

1) 数据的外包存储

在云计算中,用户租用云服务商的计算或存储资源,即将数据外包存放在云端。外包了数据意味着用户不再对数据和环境拥有完全的控制权,尽管可以借助数据加密技术在一定程度上保障静态存储的机密性,然而在动态运行时,解密后的数据可能存在于内存、网络或磁盘缓存等介质中,在用户数据自上传到销毁的整个生命周期中,隐私性可能受到多方面的威胁,隐私风险不可忽视。

2) 虚拟化与多租户

虚拟化技术是实现云计算资源池化和按需服务的基础,而多租户作为云计算中的一种软件架构技术被广泛使用,多个租户的虚拟机可被部署到同一台主机上,即共享同一堆栈的软、硬件资源。尽管通过虚拟机能够有效隔离用户的资源,然而目前的虚拟化平台并不是完美的,仍然存在安全漏洞,如 Xen 虚拟化平台存在被旁路攻击的危险[5],攻击者可通过操纵自己的虚拟机对放置于同一台主机上的其他虚拟机进行旁路攻击,致使对方隐私数据被泄漏。

3) 大数据

云计算的出现带动了大数据应用的发展,对数据整合、分析与挖掘所产生的效果前所未有,社会和个人均因大数据的使用而获益,然而不容忽视的问题是隐私风险的存在。大数据背景下由于各种挖掘和整合技术的使用,导致个人的兴趣爱好、行为模式、社会习惯等隐私信息暴露。多项实际案例说明,即使无害的数据被大量收集后,也会暴露个人隐私[6]。大数据如同一把双刃剑,在带来便利的同时隐藏着风险。

2 云计算中数据隐私保护的关键问题及研究现状

云计算中的隐私数据存在泄漏和被跟踪的隐私风险[7]。云隐私保护是指采取相应的措施防止个人信息的跟踪、暴露以及存储在云中敏感信息的泄漏,涉及对云中数据的共享、搜索、计算、完整性验证、删除等各

种操作以及数据自上传到销毁的整个生命周期。目前，国内外学者对云计算中数据隐私保护的研究热点主要集中在以下领域。

2.1　隐私保护框架

在隐私保护框架方面，Pearson[8] 建议隐私应该从一开始就被考虑并且在云服务的每个阶段都应该考虑到。Kamara 等人[9] 提出了一种安全云存储框架，由数据发生器、数据证实者、令牌发生器及证书发生器共同合作完成云用户数据的加密存储服务。只有从数据属主获取令牌和证书才能访问存放在云端的加密数据。该方案在提供隐私保护的同时增加了通信开销及数据属主方的实现难度。文献 [10] 认为可通过缩小云提供商的权限来解决数据隐私保护问题，提出的 MyCloud 限制云供应商的能力，只让其执行如虚拟机分配、回收等正常的云资源管理操作。

考虑到云用户数据的敏感程度或安全级别需求的不同，所采取的隐私保护机制也应不同。文献 [11] 将用户数据按照敏感程度分类为私有敏感数据和公共非敏感数据，私有敏感数据被存放在私有云中，只允许机构内用户通过认证机制来访问。然而这种方案不具有通用性，因其在提供数据隐私保护的同时也极大地降低了云计算的优势。文献 [12] 提出了由隐私分析、量化模型、数据分类和数据保护过程 4 部分组成的云数据保护系统(cloud data protection system，CDPS) ，根据不同类型数据的隐私需求不同，将用户数据进行隐私等级划分，不同隐私等级的数据采用不同的加密机制。该方案考虑了隐私需求，但文中没有涉及隐私需求描述及隐私分析的具体方法。文献 [13] 进一步考虑了云服务商的可信程度，敏感数据的加密处理是基于一个安全和隔离的加密处理器，将软件应用的实现组件也划分为需要受保护的部分和不需要受保护的部分，定义软件隐私结构及隐私标签，加密处理器上的进程读取软件隐私标签，通过验证软件包的数字签名确保其授权和完整性。文献 [14] 对数据进行合理分割及部署，然后按数据的安全级别需求，联合采用数据染色和不同强度的数据加密技术进行染色或加密。文献 [15] 基于策略代数讨论了云服务商能力和云用户隐私需求间的关系及二者自动协商过程。

在隐私保护框架研究中，合理的方案是基于数据保护的安全级别采取不同隐私保护机制并且应满足用户对隐私保护需求的可控性。因此，数据安全级别划分、隐私需求的通用描述、可信删除、隐私反馈等都是值得进一步研究的问题。

2.2　基于数据加密技术的隐私保护

基于加密技术的隐私保护方案一直是云内容隐私保护采用的主流技术。用户在上传敏感数据之前首先将数据加密，这样攻击者即使获取了数据也无法获知其内容，保证了数据在云端存储的安全，保护了用户数据的隐私性。然而，在大多数情况下，对云端中的数据不仅局限于存储，还涉及对数据的共享、搜索、计算、完整性验证等处理。密钥的泄漏、搜索和计算过程中对密文的解密等均会带来潜在的数据隐私风险。

针对加密数据计算过程中因解密带来的隐私泄漏问题，当前的研究集中在可计算加密技术(对密文直接操作) 和明文隔离策略。Gentry 提出了全同态加密 FHE[16] ，可对存放在云提供商不同服务器上的加密数据直接进行计算，云服务商无法获知输入数据、处理功能、结果以及任何中间结果数据，因此隐私被保留，FHE 已成为云计算中实施隐私保留的一个强有力工具，然而当前对同态加密机制的研究还处于理论阶段，所提出的同态加密算法不能对密文进行任意运算，并且计算开销较大，在实际应用中的效率不高，研究者正试图对算法进行改进以降低算法的复杂度。Sadeghi 等人[17] 对基于全同态和可证实加密的纯加密方法进行了讨论，提出将可信硬件令牌和安全函数评价相结合的策略，能够对加密格式的数据进行任意操作，计算不会有任何信息泄漏并且是可验证的。这项工作的关键是如何最小化计算延迟提高效率。硬件令牌能够阻止物理攻击，一旦令牌在可信假设下，用户数据即可在令牌下执行，从而与不可信的云服务商相分离。然而文献中令牌仅在数据预处理阶段考虑，接下来的在线阶段，云端仅执行对称加密算法，没有考虑与令牌的进一步交互。文献 [18] 提出了云计算环境中隐私保留的可扩展和高效的公开审计方案，通过同态认证确保 TPA 在审计过程中无法获知数据内容，从而使得云用户能够在需要的时候对外存数据进行数据完整性的验证。Naehring 等人[19] 也提出了一些同态加密机制，相比于 FHE 而言该机制更快速和简洁，但这些方法仅支持部分同态操作。文献 [20] 针对现有全同态加密体制在非适应性选择密文攻击下的安全性进行了研究。Pearson[21-22] 等人提出了基于混淆技术的隐私管理者，隐私管理者能够对存放在云端的敏感数据进行混淆操作，仅需将用户隐私数据的加密形式存到云上，然后在加密数据上直接执行相应操作。这种方法要求云服务商

必须支持对隐私保护的额外服务。

在查询隐私保护方面,文献[23]提出了基于通配符的密文查询策略,云服务商无需对查询文件进行解密,在密文上直接完成云用户的查询请求,防止云服务商因解密可能带来的隐私风险。文献[24]对加密云数据上的多关键字排序搜索进行了研究,考虑了针对索引及查询关键词频率的相关攻击带来的隐私泄露。文献[25]采用多叉树结构构建数据索引,设计密钥推导算法EKDA实现密钥的管理和分发,构建关键字检索算法DLSEK实现对数据共享和密文检索的支持。文献[26]通过设计无证书认证的PKES(支持关键词检索的公钥加密),构建了一种支持隐私保护的高效密文排序查询方法(RQED),实现强隐私保护的密文查询,提高了密文查询的时空效率。如何提高查询效率、支持灵活的查询语句以及保留数据明文中的查询结果,仍是目前基于密文的查询隐私保护研究中的重点。

针对云存储平台上密文共享中的隐私保护,当前的研究主要集中在密钥安全分发和具有隐私感知的密文访问控制方面。文献[27]提出在可信第三方云TTP建立一个全局授权注册系统GARS,提供密钥分发工作。Yu等人[28]讨论了基于文件属性的访问控制策略,在不泄漏数据内容的前提下将与访问控制相关的复杂计算工作交给不可信的云服务器完成,从而达到访问控制的目的。文献[29]将基于密文属性的加密算法CP-ABE引入云存储中,访问授权由数据拥有者制定,云用户的私钥则和其自身的属性相关,在服务商不可信的云存储环境中,不让服务提供商参与数据加密密钥的产生和管理,增加了访问权限管理的安全。洪澄等人[30]在属性基加密的基础上设计出一种基于秘密共享方案的云端重加密方法,在不损失安全性的前提下将一部分重加密代价转移到云端,降低权限管理的复杂度,实现密文访问控制。文献[31]提出了一种云计算环境中基于角色的访问控制模型CARBAC,将角色细化为用户角色和管理角色,通过权限查找算法为相应用户确定最小角色集。文献[32]提出了云计算环境中数字内容版权全生命周期保护和用户隐私保护的框架,采用属性基加密和加法同态加密算法分发内容加密密钥,而且允许用户匿名获取内容和授权,同时防止云服务提供商获得用户使用内容的记录。基于属性的加密机制能有效地保护用户隐私并且保证数据的机密性,但目前来看,为更好的将属性加密方式应用在云存储平台上应进一步降低其时间复杂度。

2.3 基于数据隔离或可信计算平台的隐私保护

陈海波等人[33]采用隔离的思想,利用虚拟机监控器为虚拟机中的指定程序提供一个私密运行空间,所有的解密操作及解密后的明文只能在私密运行空间中进行及存在,在这个运行空间中运行的程序,其内存是不能被操作系统或其他程序访问的。这种内存的隔离性保证了数据在内存中的高度隐私性。文献[34]考虑到仅有私密运行空间还不足以保证用户数据的安全,提出了用户数据全生命周期的隐私性管理以及强制性数据销毁协议,为存储在云端的用户数据提供了控制机制,明文形式的用户数据只存在于私密运行空间中,而密钥则位于虚拟机监控器的内存空间。在用户指定的时间点,内存中的数据以及用户密钥均将会被强制销毁。文献[35]引入可信计算平台(trusted platform module,TPM)作为安全入口,使用可信的软件和硬件组件来提供安全机制,产生数据外存加密使用的对称密钥,使数据属主能够验证云及其计算的完整性。然而,这些解决方法都要求云提供商物理控制下的硬件可信,同时都要面对运行时间证词的挑战。

2.4 云数据组合隐私风险研究

云数据组合隐私保护指云用户不希望存放在云端的一系列数据属性的组合同时被暴露,以防止他人通过推断加以恶意利用,可通过保护数据间关系而不是数据值的方式防止隐私泄露。张坤[36]针对敏感关联关系的保护提出了一种基于信息隐藏的敏感数据组合的隐私保护机制,同时针对数据分布变化可能导致的隐私泄漏提出了对应的均衡化机制,基于伪造数据实现对各种导致隐私泄漏的数据分布的调整,防止数据分布带来的数据组合隐私泄漏。

随着大数据时代的到来,组合隐私风险将更加突出,然而当前该方面的研究还较少。

2.5 云用户身份隐私保护研究

在云计算架构中,一切皆服务,云用户在访问云服务时需提供身份认证信息,而身份认证信息中往往包含大量的敏感信息,因此云用户在享用云计算带来的便利及高效的同时也存在身份隐私泄漏的风险。文献[37-38]从云用户身份属性信息的泄漏带来的隐私安全问题方面进行了研究,提出了云计算中的隐私保留的数字身份管理机制,使用查询表、词典和本体映射的组合技术,能够对身份属性名字的不同变种进行定位,使CSP在不知用户身份属性隐私的情形下完成对用户的认证服务。文献[39]提出了一种基于属性加密的匿

名特权控制机制 AnonyControl,包含用户身份信息的属性由不同的属性授权方单独控制,实现了对云数据的匿名访问及细粒度的特权控制。文献[40]提出了一种面向服务的认证方法,云用户身份信息被抽取及分类形成层次树结构,通过模糊算法进行身份信息树及访问服务间的映射,根据信息安全等级,动态开启相应的服务访问控制并提供细粒度面向服务的身份认证,保证敏感信息的最少泄露,最大限度地保护个人隐私。文献[41]针对云计算下的可信模型进行研究,采用零知识可靠证明协议,在保留云服务用户身份隐私同时证明其身份的有效性。

3　研究趋势

安全和隐私一直是云计算领域中的热点及关键问题,尽管近些年国内外学者已在云计算中的数据隐私保护方面进行了卓有成效的研究,但整体而言云计算中隐私保护的研究仍然处于起步阶段,已有的隐私保护研究侧重于可计算加密算法本身、密文访问控制及虚拟机隔离等方面,这些隐私保护机制不能完全避免隐私风险的存在,仍有一些关键的问题需要进行深入细致的研究。

(1) 隐私需求与服务等级协议(SLA)

云用户(消费者)在使用云计算平台前应考虑它的安全和隐私,了解云服务商提供的公共云计算环境,确保云计算方案满足机构安全和隐私需求[42]。然而消费者对服务的隐私需求是不同的,不同地方的隐私法也存在很大差异,所以从云服务商的角度满足所有消费者的期望是不可能的,只能通过协商过程在用户隐私需求和云服务质量方面保持平衡。随着越来越多的消费者将任务托付给云服务商,消费者和服务商之间的服务等级协议(service level agreement,SLA)成为了一个重要方面。目前 SLA 缺少隐私保护相关的条款[43],存在云服务商利用特权无意或者恶意泄露用户隐私的隐患,因此结合云体系特征进行隐私需求建模与验证、隐私需求的一致性检测、隐私需求描述和 SLA 的规范、SLA 实施执行的监测等问题都是亟待解决的关键问题。

(2) 隐私反馈

隐私反馈是指通过相应的反馈机制告知云用户其行为的隐私风险。在云计算中,使用云服务的用户应能感知其隐私数据的使用和操作[8],云平台应向云用户证明自己具备某种程度的数据隐私保护能力,即提供一定的隐私反馈机制。基于隐私保护的目的,云用户在隐私需求阶段描述出需感知的隐私操作类型及操作内容,当执行相应类型操作时,系统创建对应的隐私审计记录并反馈给云用户。通过隐私反馈机制,用户获知应用在其数据上不同的隐私操作,了解潜在可能损害隐私数据机密性的风险。因此在设计具有隐私感知的云服务时,隐私反馈机制是应该考虑和仔细设计的一个重要部分。如何设计隐私记录的结构以及利用可信第三方对隐私记录进行可信审计等都是隐私反馈机制需要考虑的关键问题,然而当前隐私反馈的相关研究还较少。

(3) 隐私风险评估

云计算中的隐私风险问题是不言而喻的,云用户在享用云服务资源的同时,面临一定的隐私泄漏风险,而云服务的便捷和可问责性与隐私保护问题之间存在一定的冲突。如: 出于身份隐私保护的目的采用匿名访问会使对恶意用户的追踪更复杂,而从可问责性角度来说,重放、轨迹分析等操作完全不揭露隐私信息是不可能的。因此当机构或个人将数据、应用或服务迁移到云端时需要对风险进行合理评估,能够度量所使用的云服务是否安全或者能够支持的隐私保护程度,从而根据应用的具体需要进行合理选择及部署。尽管风险评估并不是一个新的话题,但云计算中的隐私风险评估仍然是一个重要挑战,要求对云服务提供商及租户进行信任等级评估,对云服务商的行为进行可信度量,文献[44-46]已对云计算中风险分析和风险评价开展了相关研究。

(4) 基于可信云平台的隐私保护

可信云平台是近来云计算领域中的一个发展方向[47],其目的是增强虚拟化环境的可信性。在云计算环境中建立可信计算基(trusted computing base,TCB)以保护用户、基础设施提供商以及服务提供商的隐私数据,进行完整性度量以及执行云计算参与各方的身份证明和软件可信性证明,构造基于可信基的可信云计算平台。可信云平台中的隐私保护涉及云中数据处理的全生命周期。由于可信云平台尚处于起步阶段,当前

的研究主要围绕可信云平台环境的构造。

4 结束语

云计算是当前发展十分迅速的一种新兴产业。作为制约云计算技术发展及普及的关键问题,云计算中的数据隐私保护越来越受到各界的关注。分析云中数据隐私风险的产生原因,归纳云隐私保护的关键问题及研究现状,对云隐私保护中的相关问题进行展望。总体而言,云隐私保护技术正处于发展阶段,围绕隐私需求、可计算加密技术、云用户身份及行为隐私保护、隐私风险评估等方面仍有大量关键问题需要深入研究。然而,云隐私保护不仅仅是技术问题,它还涉及隐私法、标准化、监管等诸多方面。因此,云计算中数据隐私保护问题的解决将依赖于学术界、产业界及政府部门的共同努力。

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.
FENG Dengguo, ZHANG Min, ZHANG Yan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83.

[2] ALMULLA S A, CHAN Y Y. Cloud computing security management [C]//Proceedings of the 2nd International Conference on Engineering System Management and Applications (ICESMA 2010). Piscataway: IEEE, 2010: 1-7.

[3] HUANG Ruwei, GUI Xiaolin, YU Si, et al. Study of privacy-preserving framework for cloud storage [J]. Computer Science and Information Systems, 2011, 8(3): 801-819.

[4] 中国公共云发展现状[EB/OL]. [2013-12-01]. http://wenku.baidu.com/view/21e97f4c33687e21af45a9b7.html.
The development status of Chinese public cloud [EB/OL]. [2013-12-01]. http://wenku.baidu.com/view/21e97f4c33687-e21af45a9b7.html.

[5] 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: Springer Press, 2009: 199-212.

[6] VIKTOR M S, KENNETH C. Big data: a revolution that will transform how we live, work and think [M]. Boston: Houghton Mifflin Harcourt, 2013.

[7] HASSAN T, JAMES B D, GAIL J A. Security and privacy challenges in cloud computing environments [J]. IEEE Security & Privacy, 2010, 8(6): 24-31.

[8] PEARSON S. Taking account of privacy when designing cloud computing services [C]. Proceedings of the Workshop on Software Engineering Challenges of Cloud Computing. Washington: IEEE Computer Society, 2009: 44-52.

[9] KAMARA S, LAUTER K. Cryptographic cloud storage [J]. Lecture Notes in Computer Science, 2010, 6054: 136-149.

[10] LI Min, ZANG Wanyu, BAI Kun, et al. MyCloud-supporting user-configured privacy protection in cloud computing [C]// Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC 2013). [S. l.]: [s. n.], 2013: 59-68.

[11] RAY C, GANGULY U. An approach for data privacy in hybrid cloud environment [C]//Proceedings of the 2nd International Conference on Computer and Communication Technology (ICCCT 2011). Piscataway: IEEE, 2011: 316-320.

[12] CHUANG I H, LI S H, HUANG K C, et al. An effective privacy protection scheme for cloud computing [C]//Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT 2011). Piscataway: IEEE, 2011: 260-265.

[13] ITANI W, KAYSSI A, CHEHAB A. Privacy as a service: privacy-aware data storage and processing in cloud computing architectures [C]//Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC '09). Los Alamitos: IEEE Computer Society, 2009: 711-716.

[14] 徐小龙,周静岚,杨庚. 一种基于数据分割与分级的云存储数据隐私保护机制[J]. 计算机科学,2013,40(2):98-102.
XU Xiaolong, ZHOU Jinglan, YANG Geng. Data privacy protection mechanism for cloud storage based on data partition and classification [J]. Computer Science, 2013, 40(2): 98-102.

[15] LIN Dan, SQUICCIARINI A. Data protection models for service provisioning in the cloud [C]//Proceedings of the 15th ACM Symposium on Access Control Models and Technologies (SACMAT 2010). New York: ACM Press, 2010: 183-192.

[16] GENTRY C. Fully homomorphic encryption using ideal lattices [C]//Proceedings of 2009 ACM Symposium on Theory of Computing (STOC '09). New York: ACM Press, 2009: 169-178.

[17] SADEGHI A R, SCHNEIDER T, WINANDY M. Token-based cloud computing secure outsourcing of data and arbitrary computations with lower latency [J]. Lecture Notes in Computer Science, 2010, 6101: 417-429.

[18] WANG Cong, WANG Qian, REN Kui, et al. Privacy-preserving public auditing for data storage security in cloud computing [C] // Proceedings of 2010 IEEE INFOCOM. New York: IEEE, 2010: 1-9.

[19] NAEHRIG M, LAUTER K, VAIKUNTANATHAN V. Can homomorphic encryption be practical? [C] //Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. New York: ACM Press, 2011: 113-124.

[20] 光焱,祝跃飞,顾纯祥,等. 一种针对全同态加密体制的密钥恢复攻击 [J]. 电子与信息学报,2013, 35(12): 2999-3004.
GUANG Yan, ZHU Yuefei, GU Chunxiang, et al. A key recovery attack on fully homomorphism encryption scheme [J]. Journal of Electronics & Information Technology, 2013, 35(12): 2999-3004.

[21] PEARSON S, SHEN Y, MOWBRAY M. A privacy manager for cloud computing [J]. Cloud Computing, 2009, 5931: 90-106.

[22] MOWBRAY M, PEARSON S. A client-based privacy manager for cloud computing [C] //Proceedings of the 4th International ICST Conference on Communication System Software and Middle-ware. [S. l.]: [s. n.], 2009: 1-8.

[23] LI Jin, WANG Qian, WANG Cong, et al. Fuzzy keyword search over encrypted data in cloud computing [C] //Proceedings IEEE INFOCOM. New York: IEEE, 2010: 1-5.

[24] CAO Ning, WANG Cong, LI Ming, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 222-233.

[25] 黄汝维,桂小林,余思,等. 支持隐私保护的云存储框架设计 [J]. 西安交通大学学报,2011, 45(10): 1-6, 12.
HUANG Ruwei, GUI Xiaolin, YU Si, et al. Design of cloud storage framework with privacy-preserving [J]. Journal of Xi'an Jiaotong University, 2011, 45(10): 1-6, 12.

[26] 程芳权,彭智勇,宋伟,等. 云环境下一种隐私保护的高效密文排序查询方法 [J]. 计算机学报,2012, 35(11): 2215-2227.
CHENG Fangquan, PENG Zhiyong, SONG Wei, et al. An efficient privacy-preserving rank query over encrypted data in cloud computing [J]. Chinese Journal of Computers, 2012, 35(11): 2215-2227.

[27] CHEN Chih-Yung, TU Jih-Fu. A novel cloud computing algorithm of security and privacy [J]. Mathematical Problems in Engineering, 2013: 871430.1-871430.6.

[28] YU Shucheng, WANG Cong, REN Kui, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing [C] //Proceedings of 2010 IEEE INFOCOM. New York: IEEE, 2010: 1-9.

[29] 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): 146-152.
SUN Guozi, DONG Yu, LI Yun. CP-ABE based data access control for cloud storage [J]. Journal on Communications, 2011, 32(7): 146-152.

[30] 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.
HONG Cheng, ZHANG Min, FENG Dengguo. Achieving efficient dynamic cryptographic access control in cloud storage [J]. Journal on Communications, 2011, 32(7): 125-132.

[31] 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.
YANG Liu, TANG Zhuo, LI Renfa, et al. Roles query algorithm in cloud computing environment based on user require [J]. Journal on Communications, 2011, 32(7): 169-175.

[32] 黄勤龙,马兆丰,傅镜艺,等. 云计算环境中支持隐私保护的数字版权保护方案 [J]. 通信学报,2014, 35(2): 95-103.
HUANG Qinlong, MA Zhaofeng, FU Jingyi, et al. Privacy-preserving digital rights management scheme in cloud computing [J]. Journal on Communications, 2014, 35(2): 95-103.

[33] 陈海波. 云计算平台可信性增强技术的研究 [D]. 上海: 复旦大学,2008.
CHEN Haibo. Improving the dependability of cloud computing systems [D]. Shanghai: Fudan University, 2008.

[34] 张逢喆,陈进,陈海波,等. 云计算中的数据隐私性保护与自我销毁 [J]. 计算机研究与发展,2011, 48(7): 1155-1167.
ZHANG Fengzhe, CHEN Jin, CHEN Haibo, et al. Lifetime privacy and self-Destruction of data in the cloud [J]. Journal of Computer Research and Development, 2011, 48(7): 1155-1167.

[35] PATEL A, DANSENA P. TPM as a middleware for enterprise data security [J]. International Journal of Computer Science and Mobile Computing, 2013, 2(7): 327-332.

[36] 张坤. 面向多租户应用的云数据隐私保护机制研究 [D]. 济南: 山东大学,2012.
ZHANG Kun. Research on cloud data privacy preservation mechanism for multi-tenancy applications [D]. Jinan: Shandong University, 2012.

(下转第 96 页)

[17] PhishTank. 基于社区的反钓鱼攻击服务 [EB/OL]. [2014-04-15]. http://www.phishtank.com/phish_search.php?valid=y&active=y.
PhishTank. Community service based on the anti phishing attacks [EB/OL]. [2014-04-15]. http://www.phishtank.com/phish_search.php?Valid=y&active=y.

[18] 丁南燕. 世界各国网址大全 [EB/OL]. [2014-04-15]. http://www.world68.com/.
DING Nanyan. The world web site [EB/OL]. [2014-04-15]. http://www.world68.com/.

(编辑:许力琴)

(上接第89页)

[37] BERTINO E, PACI F, FERRINI R, et al. Privacy-preserving digital identity management for cloud computing [C]. IEEE Computer Society Data Engineering Bulletin, 2009, 32(1): 1-4.

[38] HWANG M, KWAK J. Improved user-centric ID management model for privacy protection in cloud computing [J]. International Journal of Computer and Network Security, 2010, 2(8): 45-49.

[39] JUNG Taeho, LI Xiangyang, WAN Zhiguo, et al. Privacy preserving cloud data access with multi-authorities [C]//Proceedings of 2013 IEEE INFOCOM. New York: IEEE, 2013: 2625-2633.

[40] LI X H, HE J S, ZHANG T. A service-oriented identity authentication privacy protection method in cloud computing [J]. International Journal of Grid and Distributed Computing, 2013, 6(1): 77-86.

[41] TALAL H N, QUAN Z S, ABDULLAH A. Identifying fake feedback for effective trust management in cloud environments [J]. Lecture Notes in Computer Science, 2013, 7759: 47-58.

[42] WAYNE J, TIMOTHY G. Guidelines on security and privacy in public cloud computing [EB/OL]. [2014-07-10]. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[43] PATEL P, AJITH R, AMIT S. Service level agreement in cloud computing [EB/OL]. [2014-07-10]. http://knoesis.wright.edu/library/download/OOPSLA_cloud_wsla_v3.pdf.

[44] Rabia Latif, Haider Abbasside Assar. Cloud computing risk assessment: a systematic literature review [J]. Lecture Notes in Electrical Engineering, 2014, 276: 285-295.

[45] THEOHARIDOU M, PAPANIKOLAOU N, PEARSON S, et al. Privacy risk, security, accountability in the cloud [C]//Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013). Los Alamitos: IEEE Computer Society, 2013: 177-184.

[46] MARIANTHI T, NIKOLAOS T, DIMITRIS G. In cloud we trust: risk-assessment-as-a-service [J]. Trust Management VII IFIP Advances in Information and Communication Technology, 2013, 401: 100-110.

[47] 赵波,严飞,张立强,等. 可信云计算环境的构建 [J]. 中国计算机学会通讯, 2012, 8(7): 28-34.
ZHAO Bo, YAN Fei, ZHANG Liqiang, et al. Construction of trusted cloud computing environment [J]. Communications of the CCF, 2012, 8(7): 28-34.

(编辑:许力琴)