软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(1):71−83 [doi: 10.3724/SP.J.1001.2011.03958]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

云计算安全研究*

冯登国, 张 敏+, 张 妍, 徐 震

(信息安全国家重点实验室 中国科学院 软件研究所,北京 100190)

Study on Cloud Computing Security

FENG Deng-Guo, ZHANG Min+, ZHANG Yan, XU Zhen

(State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: mzhang@is.iscas.ac.cn

Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. *Journal of Software*, 2011,22(1): 71−83. http://www.jos.org.cn/1000-9825/3958.htm

Abstract: Cloud Computing is the fundamental change happening in the field of Information Technology. It is a representation of a movement towards the intensive, large scale specialization. On the other hand, it brings about not only convenience and efficiency problems, but also great challenges in the field of data security and privacy protection. Currently, security has been regarded as one of the greatest problems in the development of Cloud Computing. This paper describes the great requirements in Cloud Computing, security key technology, standard and regulation etc., and provides a Cloud Computing security framework. This paper argues that the changes in the above aspects will result in a technical revolution in the field of information security.
Key words: cloud computing; cloud security framework; cloud security standard; cloud security service

摘 要: 云计算代表 IT 领域向集约化、规模化与专业化道路发展的趋势,是 IT 领域正在发生的深刻变革.但它在提高使用效率的同时,为实现用户信息资产安全与隐私保护带来极大的冲击与挑战.当前,安全成为云计算领域亟待突破的重要问题,其重要性与紧迫性已不容忽视.分析了云计算对信息安全领域中技术、标准、监管等各方面带来的挑战;提出云计算安全参考框架及该框架下的主要研究内容;指出云计算的普及与应用是近年来信息安全领域的重大挑战与发展契机,将引发信息安全领域又一次重要的技术变革.
关键词: 云计算;云安全技术框架;云安全标准;云安全服务
中图法分类号: TP309 **文献标识码**: A

云计算是当前信息技术领域的热门话题之一,是产业界、学术界、政府等各界均十分关注的焦点.它体现了“网络就是计算机”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 IT 资源池,为远程计算机用户提供“召之即来,挥之即去”且似乎“能力无限”的 IT 服务.云计算以其便利、经济、高可扩展性等优势吸引了越来越多的企业的目光,将其从 IT 基础设施管理与维护的沉重压力中解放出来,更专注于自身的核心业务发展.在 IT 产业界,云计算被普遍认为是继互联网经济繁荣以来的又一个重要 IT 产业增长

* 基金项目: 国家高技术研究发展计划(863)(2007AA120404); 中国科学院知识创新工程项目(YYYJ-1013)
收稿时间: 2010-08-26; 定稿时间: 2010-11-03
CNKI 网络优先出版: 2010-11-26 16:37, http://www.cnki.net/kcms/detail/11.2560.TP.20101126.1637.002.html

点,具有巨大的市场增长前景.根据 IDC 咨询公司的预测,未来 5 年内,IT 云服务上的支出将增长 3 倍,到 2012 年将达到 420 亿美元,占 IT 支出增长总量中的 25%.此外,由于云计算的发展理念符合当前低碳经济与绿色计算的总体趋势,并极有可能发展成为未来网络空间的神经系统,它也为世界各国政府所大力倡导与推动.云计算代表了 IT 领域迅速向集约化、规模化与专业化道路发展的趋势,有人形象地将云计算比喻成为当前信息领域正在发生的工业化革命.

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.Gartner2009 年的调查结果显示,70%以上受访企业的 CTO 认为近期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.而近来,Amazon,Google 等云计算发起者不断爆出各种安全事故更加剧了人们的担忧.例如,2009 年 3 月,Google 发生大批用户文件外泄事件,2009 年 2 月和 7 月,亚马逊的“简单存储服务(simple storage service,简称 S3)”两次中断导致依赖于网络单一存储服务的网站被迫瘫痪等等.因此,要让企业和组织大规模应用云计算技术与平台,放心地将自己的数据交付于云服务提供商管理,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.

目前,云计算安全问题已得到越来越多的关注.著名的信息安全国际会议 RSA2010 将云计算安全列为焦点问题,CCS 从 2009 年起专门设置了一个关于云计算安全的研讨会.许多企业组织、研究团体及标准化组织都启动了相关研究,安全厂商也在关注各类安全云计算产品.本文通过分析当前云计算所面临的安全问题以及云计算对信息安全领域带来的影响,提出未来云计算安全技术框架及重要的科研方向,以期为我国未来云计算安全的科研、产业发展做出有益的探索.

1 云计算发展趋势

IT 资源服务化是云计算最重要的外部特征.目前,Amazon,Google,IBM,Microsoft,Sun 等国际大型 IT 公司已纷纷建立并对外提供各种云计算服务.根据美国国家标准与技术研究院(NIST)的定义,当前云计算服务可分为 3 个层次,分别是:(1) 基础设施即服务(IaaS),如 Amazon 的弹性计算云(elastic compute cloud,简称 EC2)、IBM 的蓝云(blue cloud)[1]以及 Sun 的云基础设施平台(IAAS)[2]等;(2) 平台即服务(PaaS),如 Google 的 Google App Engine[3]与微软的 Azure 平台等;(3) 软件即服务(SaaS),如 Salesforce 公司的客户关系管理服务等.

当前,各类云服务之间已开始呈现出整合趋势,越来越多的云应用服务商选择购买云基础设施服务而不是自己独立建设.例如:在云存储服务领域,成立于美国乔治亚州的 Jungle Disk 公司基于 Amazon S3 的云计算资源,通过友好的软件界面,为用户提供在线存储和备份服务;在数据库领域,Oracle 公司利用 Amazon 的基础设施提供 Oracle 数据库软件服务以及数据库备份服务;而 FanthomDB 为用户提供基于 MySQL 的在线关系数据库系统服务,允许用户选择底层使用 EC2 或 Rackspace 基础设施服务,等等.可以预见,随着云计算标准的出台,以及各国的法律、隐私政策与监管政策差异等问题的协调解决,类似的案例会越来越多.对比其他领域(如制造业领域)的全球化经验可知,云计算将推动 IT 领域的产业细分:云服务商通过购买服务的方式减少对非核心业务的投入,从而强化自己核心领域的竞争优势.最终,各种类型的云服务商之间形成强强联合、协作共生关系,推动信息技术领域加速实现全球化,并最终形成真正意义上的全球性的“云”.

未来云计算将形成一个以云基础设施为核心、涵盖云基础软件与平台服务与云应用服务等多个层次的巨型全球化 IT 服务化网络,如图 1 所示.如果以人体作为比喻,那么处于核心层的云基础设施平台将是未来信息世界的神经中枢,其数量虽然有限但规模庞大,具有互联网级的强大分析处理能力;云基础软件与平台服务层提供基础性、通用性服务,例如,云操作系统、云数据管理、云搜索、云开发平台等,是这个巨人的骨骼与内脏;而外层云应用服务则包括与人们日常工作与生活相关的大量各类应用,例如,电子邮件服务、云地图服务、云电子商务服务、云文档服务等等,这些丰富的应用构成这个巨型网络的血肉发肤.各个层次的服务之间既彼此独立又相互依存,形成一个动态稳定结构.越靠近体系核心的服务,其在整个体系中的权重也就越大.因此,未来谁掌握了云计算的核心技术主动权以及核心云服务的控制权,谁就将在信息技术领域全球化竞争格局中处于优势地位.

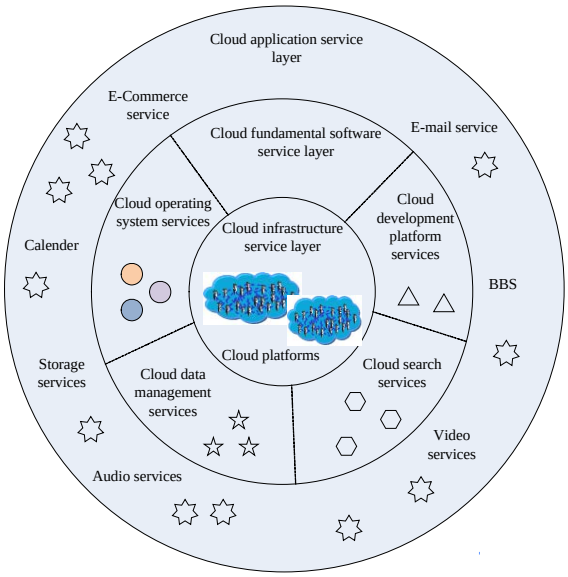

Fig.1 Hierarchical distribution of future cloud computing services

图 1 未来云计算服务分布层次图

由于云计算代表未来信息技术领域的核心竞争力,当前世界各国政府都十分重视本国云计算的发展,力争在未来信息技术的制高点占据一席之地.例如,2009 年 9 月,美国总统奥巴马宣布将执行云计算政策,希望借助应用虚拟化来压缩美国政府的经济支出;韩国政府计划向云计算领域投资 6 146 亿韩元(约合人民币 36 亿元),使韩国云计算市场的规模扩大为目前的 4 倍;日本内务部和通信监管机构计划建立大规模云计算基础设施,以支持所有政府运作所需的资讯科技系统,提高政府运营效率并降低成本.在我国,继无锡之后,北京、上海等城市启动了云计算发展计划,电信、能源交通、电力等多个行业领域也在启动行业内部云计算中心建设.

2 云计算安全挑战

目前,关于云计算与安全之间的关系一直存在两种对立的说法.持有乐观看法的人认为,采用云计算会增强安全性.通过部署集中的云计算中心,可以组织安全专家以及专业化安全服务队伍实现整个系统的安全管理,避免了现在由个人维护安全,由于不专业导致安全漏洞频出而被黑客利用的情况.然而,更接近现实的一种观点是,集中管理的云计算中心将成为黑客攻击的重点目标.由于系统的巨大规模以及前所未有的开放性与复杂性,其安全性面临着比以往更为严峻的考验.对于普通用户来说,其安全风险不是减少而是增大了.

2.1 云计算将推动信息安全领域又一次重大革新

信息安全领域的发展历程已多次证明,信息技术的重大变革将直接影响信息安全领域的发展进程.例如,在计算机出现之前,信息安全学科以实现通信保密为主要目的,主要研究内容是密码学.自进入计算机时代,信息安全研究目标扩展到计算机系统安全.信息安全学术界形成了以安全模型分析与验证为理论基础、以信息安全产品为主要构件、以安全域建设为主要目标的安全防护体系思想;不仅涌现出安全操作系统、安全数据库管理系统、防火墙为代表的信息安全产品,同时形成了相关的信息安全产品测评标准,以及基于安全标准的测评认证制度与市场准入制度,实现了信息安全产品的特殊监管.当信息技术快速步入网络时代,跨地域、跨管理域的协作不可避免,多个系统之间存在频繁交互或大规模数据流动,专一、严格的信息控制策略变得不合时宜,信息安全领域随即进入了以立体防御、深度防御为核心思想的信息安全保障的时代.形成了以预警、攻击防护、响应、恢复为主要特征的全生命周期安全管理,出现了大规模网络攻击与防护、互联网安全监管等各项新的研究内容.安全管理也由信息安全产品测评发展到大规模信息系统的整体风险评估与等级保护等,如图 2 所示.

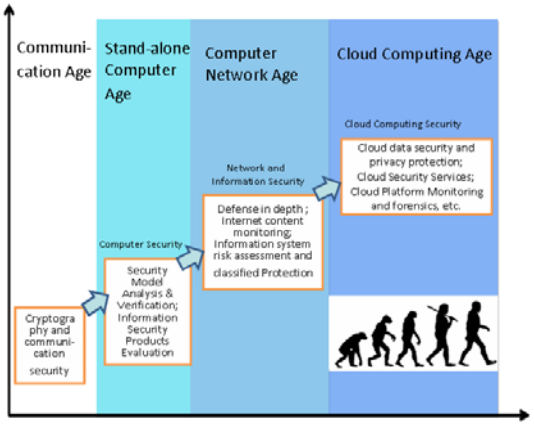

Fig.2 Evolution of information security technology

图 2 信息安全技术发展阶段图

云计算以动态的服务计算为主要技术特征,以灵活的“服务合约”为核心商业特征,是信息技术领域正在发生的重大变革.这种变革为信息安全领域带来了巨大的冲击:

(1) 在云平台中运行的各类云应用没有固定不变的基础设施,没有固定不变的安全边界,难以实现用户数据安全与隐私保护;

(2) 云服务所涉及的资源由多个管理者所有,存在利益冲突,无法统一规划部署安全防护措施;

(3) 云平台中数据与计算高度集中,安全措施必须满足海量信息处理需求.

由于当前信息安全领域仍缺乏针对此类问题的充分研究,尚难为安全的云服务提供必要的理论技术与产品支撑,因此,未来在信息安全学术界与产业界共同关注及推动下,信息安全领域将围绕云服务的“安全服务品质协议”的制定、交付验证、第三方检验等,逐渐发展形成一种新型的技术体系与管理体系与之相适应,标志着信息安全领域一个新的时代的到来.

从目前来看,实现云计算安全至少应解决关键技术、标准与法规建设以及国家监督管理制度等多个层次的挑战.下面分别予以简要阐述.

2.2 挑战1:建立以数据安全和隐私保护为主要目标的云安全技术框架

当前,云计算平台的各个层次,如主机系统层、网络层以及 Web 应用层等都存在相应安全威胁,但这类通用安全问题在信息安全领域已得到较为充分的研究,并具有比较成熟的产品.研究云计算安全需要重点分析与解决云计算的服务计算模式、动态虚拟化管理方式以及多租户共享运营模式等对数据安全与隐私保护带来的挑战:

(1) 云计算服务计算模式所引发的安全问题.当用户或企业将所属的数据外包给云计算服务商,或者委托其运行所属的应用时,云计算服务商就获得了该数据或应用的优先访问权.事实证明,由于存在内部人员失职、黑客攻击及系统故障导致安全机制失效等多种风险,云服务商没有充足的证据让用户确信其数据被正确地使用.例如,用户数据没有被盗卖给其竞争对手、用户使用习惯隐私没有被记录或分析、用户数据被正确存储在其指定的国家或区域,且不需要的数据已被彻底删除等等;

(2) 云计算的动态虚拟化管理方式引发的安全问题.在典型的云计算服务平台中,资源以虚拟、租用的模式提供给用户,这些虚拟资源根据实际运行所需与物理资源相绑定.由于在云计算中是多租户共享资源,多个虚拟资源很可能会被绑定到相同的物理资源上.如果云平台中的虚拟化软件中存在安全漏洞,那么用户的数据就可能被其他用户访问.例如,2009 年 5 月,网络上曾经曝光 VMware 虚拟化软件的 Mac 版本中存在一个严重的安全漏洞.别有用心的人可以利用该漏洞通过 Windows 虚拟机在 Mac 主机上执行恶意代码.因此,如果云计算平台无法实现用户数据与其他企业用户数据的有效隔离,用户不知道自己的邻居是谁、有何企图,那么云服务商就无

法说服用户相信自己的数据是安全的;

(3) 云计算中多层服务模式引发的安全问题.前面已经提及,云计算发展的趋势之一是 IT 服务专业化,即云服务商在对外提供服务的同时,自身也需要购买其他云服务商所提供的服务.因而用户所享用的云服务间接涉及到多个服务提供商,多层转包无疑极大地提高了问题的复杂性,进一步增加了安全风险.

由于缺乏安全关键技术支持,当前的云平台服务商多数选择采用商业手段回避上述问题.但长远来看,用户数据安全与隐私保护需求属于云计算产业发展无法回避的核心问题.其实,上述问题并不缺乏技术基础,如数据外包与服务外包安全、可信计算环境、虚拟机安全、秘密同态计算等各项技术多年来一直为学术界所关注.关键在于实现上述技术在云计算环境下的实用化,形成支撑未来云计算安全的关键技术体系,并最终为云用户提供具有安全保障的云服务.

2.3 挑战2:建立以安全目标验证、安全服务等级测评为核心的云计算安全标准及其测评体系

建立安全指导标准及其测评技术体系是实现云计算安全的另一个重要支柱.云计算安全标准是度量云用户安全目标与云服务商安全服务能力的尺度,也是安全服务提供商构建安全服务的重要参考.基于标准的“安全服务品质协议”,可以依据科学的测评方法检测与评估,在出现安全事故时快速实现责任认定,避免产生责任推诿.建立云计算安全标准及其测评体系的挑战在于以下几点:

- 首先,云计算安全标准应支持更广义的安全目标.云计算安全标准不仅应支持用户描述其数据安全保护目标、指定其所属资产安全保护的范围和程度,更重要的是,应支持用户、尤其是企业用户的安全管理需求,如分析查看日志信息、搜集信息,了解数据使用情况以及展开违法操作调查等.而这些信息的搜集可能会牵涉到云计算服务商的数据中心或涉及到其他用户的数据,带来一定安全隐患.当前,云计算商业运作模式仍不十分成熟,用户与云计算服务商之间的责任与权限界定得并不清晰,用户与云计算服务商就管理范围与权限上可能存在冲突,因此,需要以标准形式将其确定下来,明确指出信息搜集的程度、范围、手段等,防止影响其他用户的权益.不仅如此,上述安全目标还应是可测量、可验证的,便于在相关规范中规定上述安全目标的标准化测量验证方法;
- 其次,云计算安全标准应支持对灵活、复杂的云服务过程的安全评估.传统意义上对服务商能力的安全风险评估方式是,通过全面识别和分析系统架构下威胁和弱点及其对资产的潜在影响来确定其抵抗安全风险的能力和水平,但在云计算环境下,云服务提供商可能租用其他服务商提供的基础设施服务或购买多个服务商的软件服务,根据系统状况动态选用.因此,标准应针对云计算中动态性与多方参与的特点,提供相应的云服务安全能力的计算和评估方法.同时,标准应支持云服务的安全水平等级化,便于用户直观理解与选择;
- 此外,云计算安全标准应规定云服务安全目标验证的方法和程序.由于用户自身缺乏举证能力,因此,验证的核心是服务商提供正确执行的证据,如可信审计记录等.云计算安全标准应明确定义证据提取方法以及证据交付方法.

2.4 挑战3:建立可控的云计算安全监管体系

科学技术是把双刃剑,云计算在为人们带来巨大好处的同时也带来巨大的破坏性能力.而网络空间又是继领土权、领空权、领海权、太空权之后的第五维国家主权,是任何主权国家必须自主掌控的重要资源.因此,应在发展云计算产业的同时大力发展云计算监控技术体系,牢牢掌握技术主动权,防止其被竞争对手控制与利用.与互联网监控管理体系相比,实现云计算监控管理必须解决以下几个问题:

(1) 实现基于云计算的安全攻击的快速识别、预警与防护.如果黑客攻入了云客户的主机,使其成为自己向云服务提供商发动 DDoS 攻击的一颗棋子,那么按照云计算对计算资源根据实际使用付费的方式,这一受控客户将在并不知情的情况下为黑客发起的资源连线偿付巨额费用.不仅如此,与以往 DDoS 攻击相比,基于云的攻击更容易组织,破坏性更大.而一旦攻击的对象是大型云服务提供商,势必影响大批用户,所造成的损失就更加难以估量.因此,需要及时识别与阻断这类攻击,防止重大的灾害性安全事件的发生;

(2) 实现云计算内容监控.云的高度动态性增加了网络内容监管的难度.首先,云计算所具有的动态性特征使得建立或关闭一个网站服务较之以往更加容易,成本代价更低.因此,各种含有黄色内容或反动内容的网站将很容易以打游击的模式在网络上迁移,使得追踪管理难度加大,对内容监管更加困难.如果允许其检查,必然涉及到其他用户的隐私问题;其次,云服务提供商往往具有国际性的特点,数据存储平台也常跨越国界,将网络数据存储到云上可能会超出本地政府的监管范围,或者同属多地区或多国的管辖范围,而这些不同地域的监管法律和规则之间很有可能存在着严重的冲突,当出现安全问题时,难以给出公允的裁决;

(3) 识别并防止基于云计算的密码类犯罪活动.云计算的出现使得组织实施密码破译更加容易,原来只有资金雄厚的大型组织才能实施的密码破解任务,在云计算平台的支持下,普通用户也可以轻松实现,严重威胁了各类密码产品的安全.在云计算环境下,如何防止单个用户或者多个合谋用户购得足够规模的计算能力来破解安全算法,也是云计算安全监管中有待解决的问题之一.

3 云计算安全现状

3.1 各国政府对云计算安全的关注

云计算在美国和欧洲等国得到政府的大力支持和推广,云计算安全和风险问题也得到各国政府的广泛重视.2010 年 11 月,美国政府 CIO 委员会发布关于政府机构采用云计算的政府文件,阐述了云计算带来的挑战以及针对云计算的安全防护,要求政府及各机构评估云计算相关的安全风险并与自己的安全需求进行比对分析.同时指出,由政府授权机构对云计算服务商进行统一的风险评估和授权认定,可加速云计算的评估和采用,并能降低风险评估的费用.

2010 年 3 月,参加欧洲议会讨论的欧洲各国网络法律专家和领导人呼吁制定一个关于数据保护的全球协议,以解决云计算的数据安全弱点.欧洲网络和信息安全局(ENISA)表示,将推动管理部门要求云计算提供商通知客户有关安全攻击状况.

日本政府也启动了官民合作项目,组织信息技术企业与有关部门对于云计算的实际应用开展计算安全性测试,以提高日本使用云计算的安全水平,向中小企业普及云计算,并确保企业和个人数据的安全性.

在我国,2010 年 5 月,工信部副部长娄勤俭在第 2 届中国云计算大会上表示,我国应加强云计算信息安全研究,解决共性技术问题,保证云计算产业健康、可持续地发展.

3.2 国内外云计算安全标准组织及其进展

国外已经有越来越多的标准组织开始着手制定云计算及安全标准,以求增强互操作性和安全性,减少重复投资或重新发明,如 ITU-TSG17 研究组[4]、结构化信息标准促进组织[5]与分布式管理任务组[6]等都启动了云计算标准工作.此外,专门成立的组织,如云计算安全联盟[7]也在云计算安全标准化方面取得了一定进展.下面我们对这些标准组织及其目前的研究进展展开加以介绍.

3.2.1 云安全联盟

云安全联盟 CSA(Cloud Security Alliance)是在 2009 年的 RSA 大会上宣布成立的一个非盈利性组织,宗旨是“促进云计算安全技术的最佳实践应用,并提供云计算的使用培训,帮助保护其他形式的计算”.自成立后,CSA 迅速获得了业界的广泛认可,其企业成员涵盖了国际领先的电信运营商、IT 和网络设备厂商、网络安全厂商、云计算提供商等.

云计算安全联盟确定了云计算安全的 15 个焦点领域,对每个领域给出了具体建议,并从中选取较为重要的若干领域着手标准的制定,在制定过程中,广泛咨询 IT 人员的反馈意见,获取关于需求方案说明书的建议.云计算安全联盟确定的 15 个云计算安全焦点领域分别是:信息生命周期管理、政府和企业风险管理、法规和审计、普通立法、eDiscovery、加密和密钥管理、认证和访问管理、虚拟化、应用安全、便携性和互用性、数据中心、操作管理事故响应、通知和修复、传统安全影响(商业连续性、灾难恢复、物理安全)、体系结构.

目前,云计算安全联盟已完成《云计算面临的严重威胁》、《云控制矩阵》、《关键领域的云计算安全指

南》[7]等研究报告,并发布了云计算安全定义.这些报告从技术、操作、数据等多方面强调了云计算安全的重要性、保证安全性应当考虑的问题以及相应的解决方案,对形成云计算安全行业规范具有重要影响.

3.2.2 其他相关标准组织动态

2009 年底,国际标准化组织/国际电工委员会、第一联合技术委员会(ISO/IEC,JTC1)正式通过成立分布应用平台服务分技术委员会(SC38)的决议,并明确规定 SC38 下设云计算研究组.

国际电信联盟 ITU-TSG17 研究组会议于 2010 年 5 月在瑞士的日内瓦召开,决定成立云计算专项工作组,旨在达成一个“全球性生态系统”,确保各个系统之间安全地交换信息.工作组将评估当前的各项标准,将来会推出新的标准.云计算安全是其中重要的研究课题,计划推出的标准包括《电信领域云计算安全指南》.

结构化信息标准促进组织(OASIS)将云计算看作是 SOA 和网络管理模型的自然扩展.在标准化工作方面,OASIS 致力于在现有标准的基础上建立云计算模型、配置文件和扩展相关的标准.现有标准包括安全、访问和身份策略标准,如 OASIS SAML,XACML,SPML,WSSecurityPolicy 等;内容、格式控制和数据导入/导出标准,如 OASIS ODF,DITA,CMIS 等;注册、储存和目录标准,如 OASIS ebXML,UDDI;以及 SOA 方法和模型、网络管理、服务质量和互操作性标准,如 OASIS SCA,SDO,SOA-RM 和 BPEL 等.

近期,分布式管理任务组(Distributed Management Task Force,简称 DMTF)[6]也已启动了云标准孵化器过程.参与成员将关注通过开发云资源管理协议、数据包格式以及安全机制来促进云计算平台间标准化的交互,致力于开发一个云资源管理的信息规范集合.该组织的核心任务是扩展开放虚拟化格式(OVF)标准,使云计算环境中工作负载的部署及管理更为便捷.

3.3 国内外云计算安全技术现状

在 IT 产业界,各类云计算安全产品与方案不断涌现.例如,Sun 公司发布开源的云计算安全工具可为 Amazon 的 EC2,S3 以及虚拟私有云平台提供安全保护.工具包括 OpenSolaris VPC 网关软件,能够帮助客户迅速和容易地创建一个通向 Amazon 虚拟私有云的多条安全的通信通道;为 Amazon EC2 设计的安全增强的 VMIs,包括非可执行堆栈,加密交换和默认情况下启用审核等;云安全盒(cloud safety box),使用类 Amazon S3 接口,自动地对内容进行压缩、加密和拆分,简化云中加密内容的管理等.微软为云计算平台 Azure 筹备代号为 Sydney 的安全计划,帮助企业用户在服务器和 Azure 云之间交换数据,以解决虚拟化、多租户环境中的安全性.EMC,Intel, Vmware 等公司联合宣布了一个“可信云体系架构”的合作项目,并提出了一个概念证明系统.该项目采用 Intel 的可信执行技术(trusted execution technology)、Vmware 的虚拟隔离技术、RSA 的 enVision 安全信息与事件管理平台等技术相结合,构建从下至上值得信赖的多租户服务器集群.开源云计算平台 Hadoop 也推出安全版本,引入 kerberos 安全认证技术,对共享商业敏感数据的用户加以认证与访问控制,阻止非法用户对 Hadoop clusters 的非授权访问.

4 云计算安全技术框架建议

解决云计算安全问题的当务之急是,针对威胁,建立综合性的云计算安全框架,并积极开展其中各个云安全的关键技术研究.在本节中,我们抛砖引玉,提出一个参考性的云安全框架建议,如图 3 所示.由于云计算安全监管技术与管理的特殊性,不属于本文讨论范围,这里不再赘述.该框架包括云计算安全服务体系与云计算安全标准及其测评体系两大部分,为实现云用户安全目标提供技术支撑.

4.1 云用户安全目标

云用户的首要安全目标是数据安全与隐私保护服务.主要防止云服务商恶意泄露或出卖用户隐私信息,或者对用户数据进行搜集和分析,挖掘出用户隐私数据.例如,分析用户潜在而有效的盈利模式,或者通过两个公司之间的信息交流推断他们之间可能有的合作等.数据安全与隐私保护涉及用户数据生命周期中创建、存储、使用、共享、归档、销毁等各个阶段,同时涉及到所有参与服务的各层次云服务提供商.

云用户的另一个重要需求是安全管理.即在不泄漏其他用户隐私且不涉及云服务商商业机密的前提下,允

许用户获取所需安全配置信息以及运行状态信息,并在某种程度上允许用户部署实施专用安全管理软件.

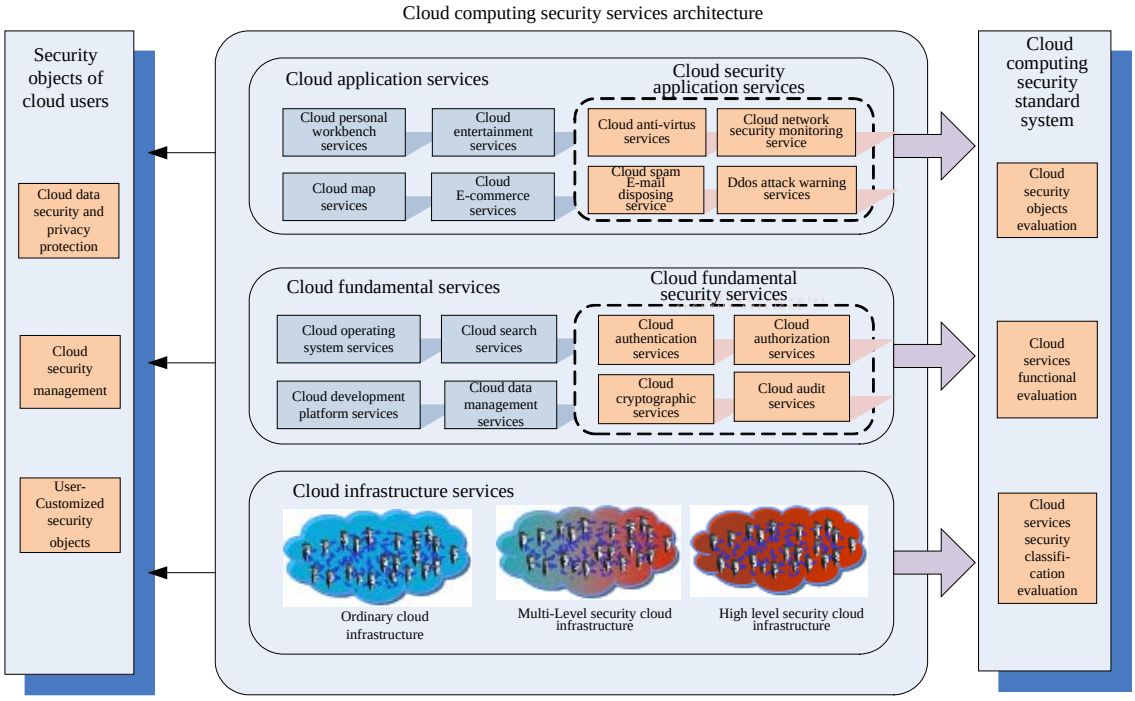

Fig.3 Cloud computing security framework

图 3 云计算安全技术框架

4.2 云计算安全服务体系

云计算安全服务体系由一系列云安全服务构成,是实现云用户安全目标的重要技术手段.根据其所属层次的不同,云安全服务可以进一步分为可信云基础设施服务、云安全基础服务以及云安全应用服务 3 类.

4.2.1 安全云基础设施服务

云基础设施服务为上层云应用提供安全的数据存储、计算等 IT 资源服务,是整个云计算体系安全的基石.这里,安全性包含两个层面的含义:其一是抵挡来自外部黑客的安全攻击的能力;其二是证明自己无法破坏用户数据与应用的能力.一方面,云平台应分析传统计算平台面临的安全问题,采取全面严密的安全措施.例如,在物理层考虑厂房安全,在存储层考虑完整性和文件/日志管理、数据加密、备份、灾难恢复等,在网络层应当考虑拒绝服务攻击、DNS 安全、网络可达性、数据传输机密性等,系统层则应涵盖虚拟机安全、补丁管理、系统用户身份管理等安全问题,数据层包括数据库安全、数据的隐私性与访问控制、数据备份与清洁等,而应用层应考虑程序完整性检验与漏洞管理等.另一方面,云平台应向用户证明自己具备某种程度的数据隐私保护能力.例如,存储服务中证明用户数据以密态形式保存,计算服务中证明用户代码运行在受保护的内存中,等等.由于用户安全需求方面存在着差异,云平台应具备提供不同安全等级的云基础设施服务的能力.

4.2.2 云安全基础服务

云安全基础服务属于云基础软件服务层,为各类云应用提供共性信息安全服务,是支撑云应用满足用户安全目标的重要手段.其中比较典型的几类云安全服务包括:

(1) 云用户身份管理服务.主要涉及身份的供应、注销以及身份认证过程.在云环境下,实现身份联合和单点登录可以支持云中合作企业之间更加方便地共享用户身份信息和认证服务,并减少重复认证带来的运行开销.但云身份联合管理过程应在保证用户数字身份隐私性的前提下进行.由于数字身份信息可能在多个组织间共享,其生命周期各个阶段的安全性管理更具有挑战性,而基于联合身份的认证过程在云计算环境下也具有更高

的安全需求;

(2) 云访问控制服务.云访问控制服务的实现依赖于如何妥善地将传统的访问控制模型(如基于角色的访问控制、基于属性的访问控制模型以及强制/自主访问控制模型等)和各种授权策略语言标准(如 XACML, SAML 等)扩展后移植入云环境.此外,鉴于云中各企业组织提供的资源服务兼容性和可组合性的日益提高,组合授权问题也是云访问控制服务安全框架需要考虑的重要问题;

(3) 云审计服务.由于用户缺乏安全管理与举证能力,要明确安全事故责任就要求服务商提供必要的支持.因此,由第三方实施的审计就显得尤为重要.云审计服务必须提供满足审计事件列表的所有证据以及证据的可信度说明.当然,若要该证据不会披露其他用户的信息,则需要特殊设计的数据取证方法.此外,云审计服务也是保证云服务商满足各种合规性要求的重要方式;

(4) 云密码服务.由于云用户中普遍存在数据加、解密运算需求,云密码服务的出现也是十分自然的.除最典型的加、解密算法服务外,密码运算中密钥管理与分发、证书管理及分发等都可以基础类云安全服务的形式存在.云密码服务不仅为用户简化了密码模块的设计与实施,也使得密码技术的使用更集中、规范,也更易于管理.

4.2.3 云安全应用服务

云安全应用服务与用户的需求紧密结合,种类繁多.典型的例子,如 DDOS 攻击防护云服务、Botnet 检测与监控云服务、云网页过滤与杀毒应用、内容安全云服务、安全事件监控与预警云服务、云垃圾邮件过滤及防治等.传统网络安全技术在防御能力、响应速度、系统规模等方面存在限制,难以满足日益复杂的安全需求,而云计算优势可以极大地弥补上述不足:云计算提供的超大规模计算能力与海量存储能力,能在安全事件采集、关联分析、病毒防范等方面实现性能的大幅提升,可用于构建超大规模安全事件信息处理平台,提升全网安全态势把握能力.此外,还可以通过海量终端的分布式处理能力进行安全事件采集,上传到云安全中心分析,极大地提高了安全事件搜集与及时地进行相应处理的能力.

4.3 云计算安全支撑服务体系

云计算安全标准及其测评体系为云计算安全服务体系提供了重要的技术与管理支撑,其核心至少应覆盖以下几方面内容:

(1) 云服务安全目标的定义、度量及其测评方法规范.帮助云用户清晰地表达其安全需求,并量化其所属资产各安全属性指标.清晰而无二义的安全目标是解决服务安全质量争议的基础.这些安全指标具有可测量性,可通过指定测评机构或者第三方实验室测试评估.规范还应指定相应的测评方法,通过具体操作步骤检验服务提供商对用户安全目标的满足程度.由于在云计算中存在多级服务委托关系,相关测评方法仍有待探索实现;

(2) 云安全服务功能及其符合性测试方法规范.该规范定义基础性的云安全服务,如云身份管理、云访问控制、云审计以及云密码服务等的主要功能与性能指标,便于使用者在选择时对比分析.该规范将起到与当前 CC 标准中的保护轮廓(PP)与安全目标(ST)类似的作用.而判断某个服务商是否满足其所声称的安全功能标准需要通过安全测评,需要与之相配合的符合性测试方法与规范;

(3) 云服务安全等级划分及测评规范.该规范通过云服务的安全等级划分与评定,帮助用户全面了解服务的可信程度,更加准确地选择自己所需的服务.尤其是底层的云基础设施服务以及云基础软件服务,其安全等级评定的意义尤为突出.同样,验证服务是否达到某安全等级需要相应的测评方法和标准化程序.

5 云计算安全关键技术研究

5.1 可信访问控制

由于无法信赖服务商忠实实施用户定义的访问控制策略,所以在云计算模式下,研究者关心的是如何通过非传统访问控制类手段实施数据对象的访问控制.其中得到关注最多的是基于密码学方法实现访问控制,包括:基于层次密钥生成与分配策略实施访问控制的方法[8,9];利用基于属性的加密算法(如密钥规则的基于属性加密方案(KP-ABE)[10],或密文规则的基于属性加密方案(CP-ABE)[11]),基于代理重加密[12]的方法;以及在用户密钥

或密文中嵌入访问控制树的方法[13−16]等.基于密码类方案面临的一个重要问题是权限撤销,一个基本方案[17]是为密钥设置失效时间,每隔一定时间,用户从认证中心更新私钥;文献[18]对其加以改进,引入了一个在线的半可信第三方维护授权列表,文献[19]提出基于用户的唯一 ID 属性及非门结构,实现对特定用户进行权限撤销.但目前看,上述方法在带有时间或约束的授权、权限受限委托等方面仍存在许多有待解决的问题.

5.2 密文检索与处理

数据变成密文时丧失了许多其他特性,导致大多数数据分析方法失效.密文检索有两种典型的方法:基于安全索引的方法[20,21]通过为密文关键词建立安全索引,检索索引查询关键词是否存在;基于密文扫描的方法[22]对密文中每个单词进行比对,确认关键词是否存在,以及统计其出现的次数.由于某些场景(如发送加密邮件)需要支持非属主用户的检索,Boneh 等人提出支持其他用户公开检索的方案[23].

密文处理研究主要集中在秘密同态加密算法设计上.早在 20 世纪 80 年代,就有人提出多种加法同态或乘法同态算法.但是由于被证明安全性存在缺陷,后续工作基本处于停顿状态.而近期,IBM 研究员 Gentry 利用“理想格(ideal lattice)”的数学对象构造隐私同态(privacy homomorphism)算法[24],或称全同态加密,使人们可以充分地操作加密状态的数据,在理论上取得了一定突破,使相关研究重新得到研究者的关注,但目前与实用化仍有很长的距离.

5.3 数据存在与可使用性证明

由于大规模数据所导致的巨大通信代价,用户不可能将数据下载后再验证其正确性.因此,云用户需在取回很少数据的情况下,通过某种知识证明协议或概率分析手段,以高置信概率判断远端数据是否完整.典型的工作包括:面向用户单独验证的数据可检索性证明(POR)[25]方法、公开可验证的数据持有证明(PDP)方法[26,27].NEC 实验室提出的 PDI(provable data integrity)[28]方法改进并提高了 POR 方法的处理速度以及验证对象规模,且能够支持公开验证.其他典型的验证技术包括:Yun 等人提出的基于新的树形结构 MAC Tree 的方案[29];Schwarz 等人提出的基于代数签名的方法[30];Wang 等人提出的基于 BLS 同态签名和 RS 纠错码的方法[31]等.

5.4 数据隐私保护

云中数据隐私保护涉及数据生命周期的每一个阶段.Roy 等人将集中信息流控制(DIFC)和差分隐私保护技术融入云中的数据生成与计算阶段,提出了一种隐私保护系统 airavat[32],防止 map reduce 计算过程中非授权的隐私数据泄露出去,并支持对计算结果的自动除密.在数据存储和使用阶段,Mowbray 等人提出了一种基于客户端的隐私管理工具[33],提供以用户为中心的信任模型,帮助用户控制自己的敏感信息在云端的存储和使用.

Munts-Mulero 等人讨论了现有的隐私处理技术,包括 *K* 匿名、图匿名以及数据预处理等,作用于大规模待发布数据时所面临的问题和现有的一些解决方案[34].Rankova 等人则在文献[35]中提出一种匿名数据搜索引擎,可以使得交互双方搜索对方的数据,获取自己所需要的部分,同时保证搜索询问的内容不被对方所知,搜索时与请求不相关的内容不会被获取.

5.5 虚拟安全技术

虚拟技术是实现云计算的关键核心技术,使用虚拟技术的云计算平台上的云架构提供者必须向其客户提供安全性和隔离保证.Santhanam 等人提出了基于虚拟机技术实现的 grid 环境下的隔离执行机[36].Raj 等人提出了通过缓存层次可感知的核心分配,以及给予缓存划分的页染色的两种资源管理方法实现性能与安全隔离[37].这些方法在隔离影响一个 VM 的缓存接口时是有效的,并整合到一个样例云架构的资源管理(RM)框架中.Wei 等人在文献[38]中关注了虚拟机映像文件的安全问题,每一个映像文件对应一个客户应用,它们必须具有高完整性,且需要可以安全共享的机制.所提出的映像文件管理系统实现了映像文件的访问控制、来源追踪、过滤和扫描等,可以检测和修复安全性违背问题.

5.6 云资源访问控制

在云计算环境中,各个云应用属于不同的安全管理域,每个安全域都管理着本地的资源和用户.当用户跨域

访问资源时,需在域边界设置认证服务,对访问共享资源的用户进行统一的身份认证管理.在跨多个域的资源访问中,各域有自己的访问控制策略,在进行资源共享和保护时必须对共享资源制定一个公共的、双方都认同的访问控制策略,因此,需要支持策略的合成.这个问题最早由 Mclean 在强制访问控制框架下提出,他提出了一个强制访问控制策略的合成框架,将两个安全格合成一个新的格结构.策略合成的同时还要保证新策略的安全性,新的合成策略必须不能违背各个域原来的访问控制策略.为此,Gong 提出了自治原则和安全原则[39,40].Bonatti 提出了一个访问控制策略合成代数,基于集合论使用合成运算符来合成安全策略[41].Wijesekera 等人提出了基于授权状态变化的策略合成代数框架[42].Agarwal 构造了语义 Web 服务的策略合成方案[43].Shafiq 提出了一个多信任域 RBAC 策略合成策略,侧重于解决合成的策略与各域原有策略的一致性问题[44].

5.7 可信云计算

将可信计算技术融入云计算环境,以可信赖方式提供云服务已成为云安全研究领域的一大热点.Santos 等人在文献[45]中提出了一种可信云计算平台 TCCP,基于此平台,IaaS 服务商可以向其用户提供一个密闭的箱式执行环境,保证客户虚拟机运行的机密性.另外,它允许用户在启动虚拟机前检验 Iaas 服务商的服务是否安全.Sadeghi 等人[46]认为,可信计算技术提供了可信的软件和硬件以及证明自身行为可信的机制,可以被用来解决外包数据的机密性和完整性问题.同时设计了一种可信软件令牌,将其与一个安全功能验证模块相互绑定,以求在不泄露任何信息的前提条件下,对外包的敏感(加密)数据执行各种功能操作.

6 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,需要 IT 领域与信息安全领域的研究者共同探索解决之道.同时,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.

References:

[1] IBM Blue Cloud Solution (in Chinese). http://www-900.ibm.com/ibm/ideasfromibm/cn/cloud/solutions/index.shtml

[2] Sun Cloud Architecture Introduction White Paper (in Chinese). http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf

[3] Barroso LA, Dean J, Holzle U. Web search for a planet: The Google cluster architecture. IEEE Micro, 2003,23(2):22−28.

[4] International Telegraph Union (ITU) (in Chinese). http://www.itu.int/en/pages/default.aspx

[5] Organization for the Advancement of Structured Information Standards (OASIS) (in Chinese). http://www.oasis-open.org/

[6] Distributed Management Task Force (DMTF) (in Chinese). http://www.dmtf.org/home

[7] Cloud Security Alliance (in Chinese). http://www.cloudsecurityalliance.org

[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. In: Guttan J, ed, Proc. of the 19th IEEE Computer Security Foundations Workshop—CSFW 2006. Venice: IEEE Computer Society Press, 2006. 5−7.

[9] Damiani E, De S, Vimercati C, Foresti S, Jajodia S, Paraboschi S, Samarati P. An experimental evaluation of multi-key strategies for data outsourcing. In: Venter HS, Eloff MM, Labuschagne L, Eloff JHP, Solms RV, eds. New Approaches for Security, Privacy and Trust in Complex Environments, Proc. of the IFIP TC-11 22nd Int'l Information Security Conf. Sandton: Springer-Verlag, 2007. 385−396.

[10] Goyal V, Pandey A, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Juels A, Wright RN, Vimercati SDC, eds. Proc. of the 13th ACM Conf. on Computer and Communications Security, CCS 2006. Alexandria: ACM Press, 2006. 89−98.

[11] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Shands D, ed. Proc. of the 2007 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2007. 321−334. [doi: 10.1109/SP.2007.11]

[12] Chang YC, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data. In: Ioannidis J, Keromytis AD, Yung M, eds. LNCS 3531. New York: Springer-Verlag, 2005. 442−455.

[13] Malek B, Miri A. Combining attribute-based and access systems. In: Muzio JC, Brent RP, eds. Proc. IEEE CSE 2009, 12th IEEE Int'l Conf. on Computational Science and Engineering. IEEE Computer Society, 2009. 305−312.

[14] Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Ning P, Vimercati SDC, Syverson PF, eds. Proc. of the 2007 ACM Conf. on Computer and Communications Security, CCS 2007. Alexandria: ACM Press, 2007. 195−203.

[15] Yu S, Ren K, Lou W, Li J. Defending against key abuse attacks in KP-ABE enabled broadcast systems. In: Bao F, ed. Proc. of the 5th Int'l Conf. on Security and Privacy in Communication Networks. Singapore: Springer-Verlag, http://www.linkpdf.com/ebook-viewer.php?url=http://www.ualr.edu/sxyu1/file/SecureComm09_AFKP_ABE.pdf

[16] Hong C, Zhang M, Feng DG. AB-ACCS: A cryptographic access control scheme for cloud storage. Journal of Computer Research and Development, 2010,47(Supplementary issue I):259−265 (in Chinese with English abstract).

[17] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. SIAM Journal on Computing, 2003,32(3):586−615.

[18] Ibraimi L, Petkovic M, Nikova S, Hartel P, Jonker W. Ciphertext-Policy attribute-based threshold decryption with flexible delegation and revocation of user attributes. Technical Report, Centre for Telematics and Information Technology, University of Twente, 2009.

[19] Roy S, Chuah M. Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs. Technical Report, 2009.

[20] Goh EJ. Secure indexes. Technical Report, Stanford University, 2003. http://eprint.iacr.org/2003/216/

[21] Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J. Controlling data in the cloud: Outsourcing computation without outsourcing control. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 85–90. [doi: 10.1145/1655008.1655020]

[22] Song D, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Titsworth FM, ed. Proc. of the IEEE Computer Society Symp. on Research in Security and Privacy. Piscataway: IEEE, 2000. 44−55.

[23] Boneh D, Crescenzo G, Ostrovsky R, Persiano G. Public key encryption with keyword search. In: Cachin C, Camenisch J, eds. LNCS 3027. Heidelberg: Springer-Verlag, 2004. 506−522.

[24] Gentry C. Fully homomorphic encryption using ideal lattices. In: Mitzenmacher M, ed. Proc. of the 2009 ACM Int'l Symp. on Theory of Computing. New York: Association for Computing Machinery, 2009. 169−178.

[25] Juels A, Kaliski B. Pors: Proofs of retrievability for large files. In: Ning P, Vimercati SDC, Syverson PF, eds. Proc. of the 2007 ACM Conf. on Computer and Communications Security, CCS 2007. Alexandria: ACM Press, 2007. 584−597.

[26] Ateniese G, Burns R, Curtmola R. Provable data possession at untrusted stores. In: Ning P, Vimercati SDC, Syverson PF, eds. Proc. of the 2007 ACM Conf. on Computer and Communications Security, CCS 2007. Alexandria: ACM Press, 2007. 598−609.

[27] Di Pietro R, Mancini LV, Ateniese G. Scalable and efficient provable data possession. In: Levi A, ed. Proc. of the 4th Int'l Conf. on Security and Privacy in Communication Netowrks. Turkey: ACM DL, 2008. http://eprint.iacr.org/2008/114.pdf [doi: 10.1145/1460877.1460889]

[28] Zeng K. Publicly verifiable remote data integrity. In: Chen LQ, Ryan MD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 2008. 419−434.

[29] Yun A, Shi C, Kim Y. On protecting integrity and confidentiality of cryptographic file system for outsourced storage. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 67−76.

[30] Schwarz T, Ethan SJ, Miller L. Store, forget, and check: Using algebraic signatures to check remotely administered storage. In: Proc. of the 26th IEEE Int'l Conf. on Distributed Computing Systems. IEEE Press, 2006. 12−12. [doi: 10.1109/ICDCS.2006.80]

[31] Wang Q, Wang C, Li J, Ren K, Lou W. Enabling public verifiability and data dynamics for storage security in cloud computing. In: Backes M, Ning P, eds. LNCS 5789. Heidelberg: Springer-Verlag, 2009. 355−370.

[32] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E. Airavat: Security and privacy for MapReduce. In: Castro M, eds. Proc. of the 7th Usenix Symp. on Networked Systems Design and Implementation. San Jose: USENIX Association, 2010. 297−312.

[33] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 43−54. [doi: 10.1145/1655008.1655015]

[34] Muntés-Mulero V, Nin J. Privacy and anonymization for very large datasets. In: Chen P, ed. Proc of the ACM 18th Int'l Conf. on Information and Knowledge Management, CIKM 2009. New York: Association for Computing Machinery, 2009. 2117−2118. [doi: 10.1145/1645953.1646333]

[35] Raykova M, Vo B, Bellovin SM, Malkin T. Secure anonymous database search. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 115−126. [doi: 10.1145/1655008.1655025]

[36] Elangop S, Dusseauaetal A. Deploying virtual machines as sandboxes for the grid. In: Karp B, ed. USENIX Association Proc. of the 2nd Workshop on Real, Large Distributed Systems. San Francisco, 2005. 7−12.

[37] Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 77−84. [doi: 10.1145/1655008.1655019]

[38] Wei J, Zhang X, Ammons G, Bala V, Ning P. Managing security of virtual machine images in a cloud environment. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 91−96. [doi: 10.1145/1655008.1655021]

[39] Gong L, Qian XL. The complexity and composability of secure interoperation. In: Proc. of the '94 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 1994. 190−200.

[40] Gong L, Qian XL. Computational issues in secure interoperation. IEEE Trans. on Software and Engineering, 1996,22(1):43−52. [doi: 10.1109/32.481533]

[41] Bonatti P, Vimercati SC, Samarati P. An algebra for composing access control policies. ACM Trans. on Information and System Security, 2002,5(1):1−35. [doi: 10.1145/504909.504910]

[42] Wijesekera D, Jajodia S. A propositional policy algebra for access control. ACM Trans. on Information and System Security, 2003, 6(2):286−325. [doi: 10.1145/762476.762481]

[43] Agarwal S, Sprick B. Access control for semantic Web services. In: Proc. of the IEEE Int'l Conf. on Web Services. 2004. 770−773.

[44] Shafiq B, Joshi JBD, Bertino E, GhafoorA. Secure interoperation in a multidomain environment employing RBAC policies. IEEE Trans. on Knowledge and Data Engineering, 2005,17(11):1557−1577. [doi: 10.1109/TKDE.2005.185]

[45] Santos N, Gummadi KP, Rodrigues R. Towards trusted cloud computing. In: Sahu S, ed, USENIX Association Proc. of the Workshop on Hot Topics in Cloud Computing 2009. San Diego, 2009. http://www.usenix.org/events/hotcloud09/tech/full_papers/santos.pdf

[46] Sadeghi AR, Schneider T, Winandy M. Token-Based cloud computing: Secure outsourcing of data and arbitrary computations with lower latency. In: Proc. of the 3rd Int'l Conf. on Trust and Trustworthy Computing. Berlin: Springer-Verlag, 2010. 417−429.

附中文参考文献:

[1] IBM.蓝云解决方案. http://www-900.ibm.com/ibm/ideasfromibm/cn/cloud/solutions/index.shtml

[2] SUN 云计算架构介绍白皮书. http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf

[4] 国际电信联盟组织 ITU. http://www.itu.int/en/pages/default.aspx

[5] 结构化信息标准促进组织. http://www.oasis-open.org/

[6] 分布式管理任务组 DMTF. http://www.dmtf.org/home

[7] 云安全联盟标准组织. http://www.cloudsecurityalliance.org/

[16] 洪澄,张敏,冯登国.AB-ACCS:一种云存储密文访问控制方法.计算机研究与发展,2010,47(增刊 I):259−265.

冯登国(1965－),男,陕西靖边人,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为信息安全理论与技术.

张妍(1983－),女,博士生,CCF 学生会员,主要研究领域为访问控制理论与技术.

张敏(1975－),女,博士,副研究员,CCF 会员,主要研究领域为数据安全,隐私保护理论与技术.

徐震(1976－),男,博士,副研究员,主要研究领域为系统安全,应用安全.