云安全研究进展综述

俞能海,郝 卓,徐甲甲,张卫明,张 驰
(中国科学技术大学信息科学与技术学院,安徽合肥 230027)

摘 要: 随着云计算在学术界和工业界的兴起,云计算也不可避免的带来了一些安全问题.本文对云计算的安全需求进行了总结,指出云计算不仅在机密性、数据完整性、访问控制和身份认证等传统安全性上存在需求,而且在可信性、配置安全性、虚拟机安全性等方面具有新的安全需求.我们对云计算的两个典型产品 Amazon Web Services 和 Windows Azure 的安全状况进行了总结,并阐述了针对云计算的拒绝服务攻击和旁通道攻击.基于云计算的安全需求和面临的攻击,对现有安全机制进行了优缺点分析,系统的总结了现有的安全机制.

关键词: 云计算; 机密性; 数据完整性; 访问控制; 公开认证; 可信性; 虚拟机安全性
中图分类号: TP391.41 **文献标识码:** A **文章编号:** 0372-2112 (2013)02-0371-011
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.02.026

Review of Cloud Computing Security

YU Neng-hai, HAO Zhuo, XU Jia-jia, ZHANG Wei-ming, ZHANG Chi
(*School of Science and Technology, University of Science and Technology of China, Hefei, Anhui* 230027, *China*)

Abstract: With the development of cloud computing in the academia and industry, it is inevitable that many security problems arise. This paper summarizes the security requirements of cloud computing, which not only cover the traditional security requirements like confidentiality, data integrity, access control and identity authentication, but also introduce new security requirements in the credibility, configuration and virtual machinery. We make conclusions about the security situations on two typical cloud computing products: Amazon Web Services and Windows Azure and elaborate two attack mechanisms against cloud computing: Denial of service attack and Side channel attack. Based on the security requirements and attacks against cloud computing, we systematically summarize the current security protection mechanisms and further make a comparison among them.

Key words: cloud computing, confidentiality, data integrity, access control , public verifiability, credibility, security of virtual machine

1 引言

云计算[1~4]因其宽带互联、资源池共享、弹性配置、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.云计算提供商以自己强大的经济和技术实力,在法律法规的约束下保障云计算的高度可靠性.

在云计算中,用户对放置在云服务器中的数据和计算失去控制,对于数据是否受到保护、计算任务是否被正确执行都不能确定.因此需要设计相应的安全机制保护用户数据的机密性、完整性、可用性,并需要使云服务器的执行具有可信性,或者能够通过问责的方法在发生攻击时迅速判断出问题所在.在公用云中,大量用户都可以在云中租赁资源,并且可以租赁基础设施向其他用户提供服务,这些用户之间不可避免的要进行通信或数据共享等.因此在云的多用户之间需要设计安全的访问控制机制[5,6].因为云计算具有开放特性和资源共享特性,针对云计算的新型攻击方式已经出现,如基于共用物理机的旁通道攻击和基于共驻子网的拒绝服务攻击等.需要设计新的防御措施,以抵抗这些攻击.另外,很多研究[7~14]提出将安全服务放在云中进行,一方面能够增强安全服务的更新能力和处理能力,另一方面能够减少客户的计算代价.这种新型的安全产品称为"安全即服务"(Security as a Service).目前的研究主要针对

收稿日期:2012-04-16;修回日期:2012-10-17
基金项目:国家自然基金(No.61170234, No.60803155);中国科学院"面向感知中国的新一代信息技术研究"战略性先导科技专项子课题(No.XDA06030601)

移动手机作为客户端的情况,因为其计算和存储能力非常有限.目前已有的研究包括反病毒服务[7]、认证[8]、安全检测[11,12]和数字版权管理[13,14]等.

2 云计算的安全需求

2.1 机密性

为了保护数据的隐私,数据在云端应该以密文形式存放,但是加密的方式又带来了运算上的开销,因此要以尽可能小的计算开销带来可靠的数据机密性[17];为了保护用户行为信息的隐私,云服务器要保证用户匿名使用云资源[18]和安全记录数据起源[19].此外,在某些应用情况下,服务器需要在用户数据上面进行运算,而运算结果也以密文形式返回给用户,因此使服务器能够在密文上面直接进行操作是一个重要的需求方向.

在最理想的情况下,服务器在密文上的任何操作都能够直接对应到明文上的相应操作,这种加密方法称为完全同态加密[20~22].如果完全同态加密能够高效安全的实现,则不仅用户的隐私得到保护,而且效率也不会降低.在完全同态加密不能高效实现的情况下,利用同态函数的特性保护隐私,研究基于密文的操作,也是很重要的.在云计算中,信息检索是一个很常用的操作,因此支持搜索的加密是云安全的一个重要需求.已有的支持搜索的加密[25~27]只支持单关键字搜索,并且不支持搜索结果排序和模糊搜索.针对云计算特征,目前的研究主要包括模糊搜索[28]、支持排序的搜索[29]和多关键字搜索[30]等.如果操作不能在密文上进行,那么用户的任何操作都要把涉及到的数据密文发送回用户方解密之后再进行,将会严重降低效率.

2.2 数据完整性

在基于云的存储服务,例如 Amazon 简单存储服务 S3[31],Amazon 弹性块存储 EBS[32],以及 Nirvanix 云存储服务[33]中,需要保证数据存储的完整性.在基于云的数据流处理[34,35]中,主要考虑的是数据处理结果的完整性和恶意服务提供商的检测[36~38].

在数据存储中,因为用户无法完全相信云服务器会对自己的数据进行完整性保护,所以用户需要对其数据的完整性进行验证.远程数据完整性验证[39~41]是解决这一问题的好方法,其能够在不下载用户数据的情况下,仅仅根据数据标识和服务器对于挑战码的响应就可以对数据的完整性进行验证.

在数据流处理[33]中,完整性验证的需求主要来源于用户对云中数据处理服务提供商的不信任性.在这种情况下,确保数据处理结果的完整性是至关重要的.

2.3 访问控制

云计算中要阻止非法的用户对其他用户的资源和数据等的访问、细粒度的控制合法用户的访问权限,因此云服务器需要对用户的访问行为进行有效的验证.其访问控制需求主要包括以下两个方面:

(1)网络访问控制[5,6]:指云基础设施中主机之间彼此互相访问的控制;

(2)数据访问控制[42,43]:指云端存储的用户数据的访问控制.数据的访问控制中要保证对用户撤销操作[104]、用户动态加入[44]和用户操作可审计[45]等要求的支持.

2.4 身份认证

现有的身份认证技术主要包括三类:(1)基于用户持有秘密的认证;(2)基于用户持有的硬件(例如智能卡、U 盾等)的认证;(3)基于用户生物特征(例如指纹)的认证.目前口令认证[46]和 X.509 证书认证[47]是云计算产品中应用比较广泛的身份认证方法.此外,层次化的基于身份认证[48,49]能够在多个云之间实现层次化的身份管理.多因子身份认证[50,51]能够从多重特征上对客户进行认证,因此能够提供增强的安全性.

2.5 可信性

为了增强云计算和云存储等服务的可信性,可以从两个方面入手.一方面是提供云计算的问责功能,通过记录操作信息实现对恶意操作的追踪和问责,如[52]提出基于云环境下信任模糊综合评价和云信任管理机制,[53]提出基于服务调用和反馈信息云服务的可信模型;另一方面是构建可信的云计算平台,通过可信计算、安全启动、云端网关[54]等技术手段达到云计算的可信性.

2.6 防火墙配置安全性

在基础设施云,例如 Amazon 弹性计算云[55]中,云中的虚拟机需要进行通信,这些通信分为虚拟机之间的通信和虚拟机与外部的通信.通信的控制可以通过防火墙来实现,因此防火墙的配置安全性[56]非常重要.如果防火墙配置出现问题,那么攻击者很可能利用一个未被正确配置的端口对虚拟机进行攻击.因此,在云计算中,需要设计对虚拟机防火墙配置安全性进行审查的算法.

2.7 虚拟机安全性

虚拟机技术在构建云服务架构[58,59]、大规模用户请求[60]及网络资源配置效率等被广泛使用,但与此同时,虚拟机也面临着两方面的安全性,一方面是虚拟机监督程序的安全性[61],另一方面是虚拟机镜像的安全性[62].在以虚拟化为支撑技术的基础设施云中,虚拟机监督程序是每台物理机上的最高权限软件,因此其安全的重要性毋庸置疑.另外,在使用第三方发布的虚拟机镜像的情况下,虚拟机镜像中是否包含恶意软件、盗

版软件等,也是需要进行检测的.

3 工业界云安全概况

目前工业界比较成功的云计算产品是 Amazon Web Services[15]和微软的 Windows Azure[16].前者属于基础设施云,旨在为用户提供方便访问的计算、存储和网络等资源.后者属于平台即服务云,旨在使客户基于 Azure 平台快速的发布应用程序.本章我们以这两个产品的安全白皮书为根据,介绍它们的安全现状.

3.1 Amazon Web Service 安全性介绍

Amazon[15]提供的云服务主要包括:弹性计算云 EC2 (Elastic Compute Cloud)[55],简单存储服务 S3(Simple Storage Service)[31],简单数据库服务 SimpleDB[64]等.以下参考 Amazon 安全白皮书[65],分别从这三个方面介绍所提供的安全保护.

在 EC2[55]中,安全保护包括宿主操作系统安全、来宾操作系统安全、防火墙和 API 保护.宿主操作系统安全基于堡垒主机和权限提升.来宾操作系统安全基于客户对虚拟实例的完全控制,利用基于 token 或 key 的认证来获取对非特权账户的访问.此外,要求客户对于每个用户建立带有日志的权限提升机制,并能够生成自己独一无二的密钥对.在防火墙方面,使用缺省拒绝模式,使得网络通信可以根据协议、服务端口和源 IP 地址进行限制.API 保护指所有 API 调用都需要 X.509 证书或客户的 Amazon 秘密接入密钥的签名,并且能够使用 SSL 进行加密.此外,在同一个物理主机上的不同实例通过使用 Xen 监督程序进行隔离,并提供对抗分布式拒绝服务攻击、中间人攻击和 IP 欺骗的保护.

在 S3[31]中,提供 bucket-level 和 object-level 两种访问控制,通过访问控制列表进行实施.此外,通过 SSL 加密来防止传输的数据被拦截,并允许用户在上传数据之前进行加密等.

在 SimpleDB[64]中,提供 domain-level 的访问控制,基于 AWS(Amazon Web Service)账户进行授权.一旦认证之后,订购者具有对系统中所有用户操作的完全访问权限.SimpleDB 服务也使用 SSL 加密进行访问.

3.2 Windows Azure 安全性介绍

Windows Azure[16]提供的是“平台即服务”类型的云计算.在 Windows Azure 的安全文档中,介绍了 Azure 平台所提供的安全性主要包括机密性、完整性、加密和问责.

在机密性方面,提供基于自签名数字证书的身份认证、最小权限客户软件、基于 SSL 的内部控制通信互认证、证书和私钥管理、控制程序硬件设备凭证、Windows Azure 存储访问控制机制等,并提供 VM (Virtual Machine)监督程序和客户 VM 之间的隔离、Fabric 控制器之间的隔离、分组过滤、VLAN (Virtual Local Area Network)隔离和客户访问等隔离机制.此外,通过.NET 密码服务,客户可以很容易的在存储数据或传输数据上实现加密、哈希和密钥管理功能.

在完整性方面,提供底层操作系统和客户应用程序的完整性、客户配置的完整性、基于密钥的存储访问控制和 Fabric 完整性控制等.在可用性方面,对数据提供三个节点的冗余存放、软硬件失效监测、方便的客户 OS (Operating System)迁移等.

此外,如果客户服务存在多个实例,则在 Azure 平台或客户服务软件更新时,将多个实例划分为不同的更新域,分阶段进行更新,以保证服务在更新期间是可用的.在问责方面,提供监控代理和监控数据分析服务,对监控和诊断日志信息进行收集,并记录在日志文件中.

4 云计算中的安全攻击

在多租客的云基础设施中,一台物理服务器上面通过运行多台虚拟机来同时为多个用户进行服务.理论上来说这些虚拟机之间是完全隔离并独立的,但由于共用相同的物理设备,这些虚拟机并不是完全独立的.针对虚拟机之间的物理依赖关系能够对其进行攻击,目前这些攻击主要包括拒绝服务攻击[66]和旁通道攻击[67,68].

4.1 拒绝服务攻击

Liu[66]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.

4.2 旁通道攻击

Ristenpart 等人[67]利用共享同一台物理机的虚拟机之间存在的旁通道进行攻击.旁通道攻击包括两个阶段:(1)判断两个虚拟机是否同在一台物理机上,(2)通过缓存级旁通道窃取数据.通过挖掘 Amazon EC2[55]的虚拟机安置方法,构建判断两台虚拟机是否在同一台物理机上的算法.通过暴力攻击或实例泛洪的方法使攻击者实例与目标实例被安置在同一台物理机上面.Okamura 和 Oyama[68]在 Xen 虚拟机监督程序下,提出了一种利用 CPU 负载进行虚拟机之间旁通道通信的方法.在理想环境下,该旁通道通信可达到 0.49bps 的带宽和较高的准确率.

5 云计算安全技术

5.1 同态加密及其应用

同态性是指如果 $c_1, c_2, \cdots, c_n$ 分别为 $m_1, m_2, \cdots,$

m_n 对应的密文,那么在 $c_1, c_2, \cdots, c_n$ 上执行操作 C 的结果经过解密之后,等同于在 $m_1, m_2, \cdots m_n$ 上执行 C 得到的结果. Gentry[20] 和 Dijk 等人[21]分别利用理想格和整数算术构建了具有完全同态性的加密算法. 在[22]中,Gentry 给出了同态加密在云计算加密数据存储中的两个应用:加密数据查询和私有数据查询. 但是这些算法目前还不实用. 在文献[71]中指出如果 Google 使用 Gentry 算法进行加密的关键字搜索,将会将计算时间增加到目前的一百万兆倍. 因此,设计高效的完全同态加密方案是一个有待解决的问题.

5.2 密文域搜索及其应用

支持搜索的加密[28~30,72]成为云存储安全当中的一个关键技术. 在使用支持搜索的加密的情况下,用户将数据加密后存储到服务器端,在搜索时提供加密过的关键字,服务器根据加密过的关键字和加密的数据进行搜索,得到结果后返回给用户. 传统的基于关键字的加密搜索[24~27]存在以下三个问题:(1)只支持精确匹配,对于输入的微小错误和格式的不一致性缺乏鲁棒性;(2)不支持返回结果排序;(3)不支持多关键字搜索. 针对这三个问题,

目前的研究[28~30]主要关注加密数据的模糊搜索、搜索结果的排序和多关键字搜索. Li 等人[28]针对传统的关键字加密搜索[24~27]只支持关键字精确匹配的问题,提出了一种加密数据的模糊搜索方案. Wang 等人[29]首次提出了支持搜索结果排序的加密数据搜索的定义,并基于保序对称加密[73]构建了一个高效的支持返回结果排序的加密数据搜索方案. Cao 等人[30]提出了一个支持多关键字搜索并能够对返回结果进行排序的加密搜索方案. 基本思想是:对安全的 k 最近邻算法[74]加以改进,在服务器无法访问数据明文的情况下,安全地根据文件包含的关键字个数进行排序. Li 等人[72]在半诚信模型[75]下,针对加密电子医疗记录的授权搜索问题,提出了一个授权关键字搜索方案. 通过改进并使用层次化谓词加密[76],能够实现多维的多关键字简单范围搜索. 通过代理服务器的使用,能够同时保护用户的查询隐私和数据索引隐私.

5.3 数据存储与处理完整性

在数据存储完整性方面,通过传统方法(如安全哈希函数、密钥消息验证码及数字签名等)进行数据完整性验证需要将海量的数据下载到客户端,从而带来大量的通信代价. 远程数据完整性验证协议[38~40,80~89]能够仅根据原始数据的一部分信息和数据的标识进行完整性验证,因此适用于云计算的数据完整性验证. Deswarte 和 Quisquater[79]首次提出非信任服务器上的远程数据完整性验证协议,他们构建了一个基于 Diffie-Hellman 密钥交换[88]的验证协议. Filho 和 Barreto[78]提出了基于 RSA 哈希函数的数据持有证明协议. Ateniese 等人[39]提出了两个可证明数据持有方案,以提供远程数据的完整性保护. Sebe 等人[79]提出了一种适用于关键基础设施的远程数据完整性验证协议. 他们的协议能够很容易的扩展到支持数据动态更新,但是不能支持公开可验证性. Wang 等人[82]提出了支持数据动态更新的远程数据完整性验证协议. 使用 Merkle 哈希树支持数据动态更新和使用 BLS 签名[94]支持公开可验证性的协议. Wang 等人[40]提出了一种支持公开可验证性和数据隐私性的协议. Zhu 等人[82]提出了交互式可证明数据持有协议(Interactive Provable Data Possession, IPDP),并为私有云构建了一个零知识 IPDP 协议. Zhu 等人的协议[82]能够支持数据动态更新、公开可验证性和数据隐私性. 他们也提出了一个高效的协作可证明数据持有协议,其适用于混合云. 在[40,81,82]中使用了第三方审计者,其具有比较特殊的技术专长和能力,是云存储系统的用户所不具备的. Hao 等人[41]通过使用 RSA 同态验证标识构建了一种远程数据完整性验证协议,其能够支持数据动态更新、公开可验证性和数据隐私性,并且不需要使用第三方审计者. 在多副本存储完整性验证方面,Curtmola 等人[80]提出了一种多副本 PDP 协议,但只有数据所有者才能对数据完整性进行验证. Hao 和 Yu[83]提出了一种基于 BLS 验证标识,适用于多副本存储的远程数据持有性验证协议,其能够支持公开可验证性和数据隐私性. Bowers 等人[93]在 PoR(Proof of Retrievability, PoR)的基础上,提出了一种提供高可用性和完整性的分布式密码系统,使得一系列服务器能够向用户证明文件存储的完整性和可取回性.

在数据流处理完整性验证方面,传统的分布式数据流处理假设所有的处理模块都是可信的,这在开放的多租客云基础设施中是无效的. 例如有些模块可能存在安全漏洞,被攻击者挖掘而进行攻击;甚至有些攻击者可以租赁云服务器设置恶意的处理模块. 在这种环境下,客户能够对数据流处理结果的完整性进行验证是非常重要的. Du 等人[36~38]针对多租客的云基础设施中可能存在共谋攻击. 他们构建了基于数据重放的解决方案,提出了基于节点自身信任分数和节点间信任分数的自适应多跳完整性证明协议.

5.4 访问控制

5.4.1 多租客云中的网络访问控制

Popa 等人[4]提出了多租客云中的网络访问控制问题,认为在云基础设施中,虚拟机监督程序控制了消息传输的两个端点,因此访问需要在虚拟机监督程序处强制实施访问控制策略. 其访问控制策略包括租客隔离、租客间通信、租客间公平共享服务和费率限制等.

Hao 等人[5]提出了将网络访问控制策略存储在一个中心服务器处,在转发元件(即增强型的二层交换机)中强制施行这些策略.客户网络的隔离通过使用虚拟局域网(Virtual Local Area Network,VLAN)来实现,当分组发往同一个 VLAN 时,不需经过策略检测就直接发送到目的地虚拟机;而当分组是发往不同的 VLAN 时,则根据安全策略进行转发判定.

5.4.2 云存储系统的数据访问控制

传统的数据访问控制基于服务器是可信的,由服务器实行访问控制策略.这在云存储环境下并不成立.Yu 等人[42]提出了基于加密的数据访问控制方案,使用户在加密数据和生成密钥的时候能够设定访问控制权限.Yu 等人提出的访问控制方案使用的密码技术主要包括密钥策略的基于属性加密(Key-Policy Attribute Based Encryption,KP-ABE)[96]、代理重加密[97]和懒惰重加密[98].KP-ABE[96]的原理是将访问控制策略嵌入到用户密钥中,用不同的属性标识数据,只有当数据的属性满足密钥当中嵌入的策略时,该密钥才能够解密该数据.代理重加密[97]起的作用是将发生用户撤销时客户的一部分计算任务转移到云服务器,而懒惰重加密[98]的使用进一步降低了服务器的开销.Wang 等人[43]通过结合层次化的基于身份密码[102]和密文策略的属性加密系统(Ciphertext-Policy Attribute Based Encryption,CP-ABE)[102],构建了一个层次化的属性加密模型.Green 等人[99]提出了一种新的基于属性加密的范例.在该范例中,用户向云提供一个单一的变换密钥,云就可以将任何一个满足该用户属性的密文变换为一个 El-Gamal 风格[100]的密文.Liu 等人[101]指出,在云计算环境下,为了提高可用性,用户数据往往被存放在多个服务器上,因此用户的重加密操作可能不会被所有服务器及时的接收执行.Liu 等人提出了一种云服务器基于内部时钟自动重加密数据的方案,该方案在基于属性加密[96,102]的基础上进行构建,可达到访问控制的正确性、数据的一致性和数据的机密性.

5.5 身份认证

在云计算身份认证方面,已有的方案包括[48~51]等.文献[48]和[49]中的方案是通过使用层次化的基于身份加密[105]构建的.Yan 等人[48]设计了一个联合身份管理系统,并在此基础上提出了基于层次化身份加密的互认证方案.Li 等人[49]使用基于身份的加密和签名,实现了一个比基于 SSL[67]的认证协议更高效的身份认证方案.Bertino 等人[50]提出了一个可互操作的多因子认证方案,适用于多域云计算环境.文献[48]和[49]的方案使用基于身份加密和签名方案,需要计算椭圆曲线上的双线性映射,而文献[50]的方案在认证过程中需要进行多次指数运算.相比之下,Hao 等人[51]提出的基于票据的可计数双因子认证方案在认证过程中仅仅使用哈希函数和异或运算,使得用户和服务器的计算代价大大降低.Hao 等人的方案在用户注册时向云服务器购买 t 个票据,之后用户每访问一次服务需要使用一张票据,通过票据和用户口令之间的绑定能够有效防止票据盗用攻击.Hao 等人的方案支持双向认证,并且智能卡的使用[107]能够方便的支持"随用随付费"设计.

5.6 问责

对云服务器的行为的问责机制,可显著提高云计算平台的可信度.Wang 和 Zhou[105]提出了一个云计算数据库问责方案,在每个用户和云服务器之间放置一个可信封装器,其能够截取用户对云服务器的请求和得到的响应,根据这些数据提取问责服务所需要的信息,发送给外在的问责服务.外在的问责服务根据给定的服务等级协议收集并管理证据.为了提高问责服务的可信性,Wang 和 Zhou[105]提出了一个分布式的协作监控机制,也就是将问责服务分布到多个数据状态服务上面,每个数据状态服务负责一部分数据,对于数据产生的更新异步式地向其他数据状态服务进行更新.这种分布式的协作监控机制既提高了服务的可信性,又保持了一致性.Haeberlen 等人[106]提出并实现了可问责虚拟机,其不仅能够在虚拟机中执行一个虚拟计算机系统,而且能够记录不可抵赖的信息,使得问责者对于软件行为的问责成为可能.可问责虚拟机的引入能够对未经修改的二进制镜像提供问责,而且不需要任何可信硬件.

5.7 可信云计算

为了保证在云基础设施中数据和计算的完整性提出了可信云计算的概念.可信云计算从引入可信的外在协调方开始,通过协调方对云端网络中的节点进行认证,维护可信节点,并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[107],其通过安装可信平台模块芯片并执行一个安全启动过程来进行安装,能够防止特权用户对客户的虚拟机进行监视或修改.Dai 等人[108]基于虚拟的动态信任根测量(Dynamic Root of Trust for Measurement),提出了一个云计算可信执行环境.

5.8 防火墙配置安全

在多租客的云基础设施中,软件服务提供商可以同时租用多个虚拟机,每个虚拟机上各有一个防火墙,通过防火墙对该虚拟机的通信进行过滤.Bleikertz 等人[56]指出计算机中防火墙的配置非常复杂,很容易出错[112],而如果防火墙配置出现问题,很可能导致数据或服务的暴露.

Bleikertz 等人[56]提出了一种利用可达性图对用户租用虚拟机防火墙配置进行审计的方案.在方案中,根据多个虚拟机之间以及虚拟机与外界之间可达性构建出的整体可达性图,Bleikertz 等人设计了两个算法,分别能够对任意的访问模式进行审计和验证可达性图是否包含某个可达性策略.对于给定的可达性策略集合,通过周期性的调用验证算法进行审计,就能够保证所有的可达性策略都被满足.

5.9 虚拟机监督程序安全性

在云基础设施中,虚拟机监督程序对于运行在物理机上的虚拟机进行监督,是物理机上具有最高权限的软件.因此,虚拟机监督程序的安全性非常重要.

Azab 等人[61]提出了 HyperSentry,通过安全硬件设计的方法来增强虚拟机监督程序的完整性.方法是在虚拟机监督程序中增加一个完整性度量代理,其与硬件中的基线板管理控制器进行通信,基线板管理控制器进一步通过一个智能平台管理接口与远端的验证方进行通信.HyperSentry 通过使用服务器上常见的带外信道(例如智能平台管理接口)来触发隐秘的完整性度量过程,并使用系统管理模式保护其基本代码和关键数据.所使用的完整性度量代理具有(1)与虚拟机监督程序相同的背景信息,(2)完全受保护的执行模式和(3)输出的证明.在 Xen 上的原型系统显示了 HyperSentry 是一个能够适用于真实世界系统的低代价实用解决方法.

5.10 虚拟机镜像安全

Wei 等人[62]提出了一个云端虚拟机镜像管理系统.在该系统中,有三类实体:发布者、使用者和管理者.发布者将镜像发布到镜像仓库中,使用者从镜像仓库中获得镜像并在云中进行使用,管理者对镜像仓库进行管理.在这三类实体中,发布者的风险主要在于有可能将自己的敏感信息泄露在镜像中,例如浏览历史等;使用者的风险在于对于所使用的镜像是未知的,因此可能用到的是脆弱的甚至包含恶意程序的镜像;管理者的风险在于所承载的镜像当中可能包含恶意或非法内容(例如盗版软件).针对这三方面风险,Wei 等人[62]设计了一系列安全机制,包括访问控制、镜像过滤器、镜像起源追踪机制和镜像维护服务等.这些安全机制能够高效的降低镜像发布者、使用者和管理者的风险.

Bugiel 等人[63]提出了针对亚马逊机器镜像(Amazon Machine Image,AMI)的攻击方法,能够从中获取到一些具有高敏感度的信息,例如口令、密钥和证书等.在对 1225 个亚马逊机器镜像进行分析之后,能够从其中获取到许多 Web 服务提供商的源代码库、管理员口令和证书等敏感信息.另外,从欧洲和美东地区的 1100 个公开的亚马逊机器镜像中,发现三分之一存在 SSH (Secure Shell)后门,这些后门使得镜像发布者可以登入使用该镜像创建的实例.Bugiel 等人还发现,通过镜像的 SSH 主机密钥对可以对使用该镜像创建的实例进行识别,由此可能会引发伪装攻击、中间人攻击和钓鱼攻击等.针对这些攻击,Bugiel 等人[63]提出了组织措施、工具辅助、常规扫描和云应用程序商店改进等应对措施.

5.11 抗拒绝服务攻击

针对 4.1 中讲到的拒绝服务攻击问题,Liu 等人[66]提出了一种检测和防御方法,其基本思想是通过监控代理和应用程序之间周期性的彼此探测以获取双向的可用带宽,当检测到可用带宽无法满足应用程序的需求时,将应用程序从当前的虚拟机迁移到其它子网.所提出的方案对设计更好的数据中心网络体系结构有一定借鉴意义.

5.12 抗旁通道攻击

Ristenpart 等人[67]讨论了一些旁通道攻击的防御措施,认为避免与敌人共享物理机是目前最理想的方法.为了避免攻击者轻易的与攻击目标共享一台物理机,云提供商可以为客户提供选择独占物理机的选项,而客户要为资源利用率的降低而多付钱.在文献[110]中,Aviram 等人设计了一个计时困难的云基础设施,通过提供商强制实行的确定性执行来消除内部计时信道.提供商强制实行的确定性执行使得输出仅依赖于显式的输入,而不依赖于任何内部计时.

6 安全即服务

6.1 反病毒服务

Oberheide 等人[7]提出了一个简捷易用的 *N*-版本反病毒服务,其主要特点是在用户计算机维护一个轻量级的杀毒软件客户端,而把反病毒引擎放在云端.Oberheide 等人[7]为移动设备设计云端反病毒服务,使得移动设备的功率消耗大大降低.

6.2 认证服务

Chow 等人[8]提出了一个认证移动用户的隐式认证框架,其认证服务在云中进行.其新奇之处在于使用用户行为数据作为辅助的认证手段,例如用户的地理位置信息和打电话的信息等.云中认证服务不仅降低了移动设备的计算和功耗开销,也使得新认证技术的集成变得方便.

6.3 安全检测服务

Portokalidis 等人[9]使得智能手机和云端副本之间保持同步,将所有的安全检测服务全部运行在云端的副本上面.Gilbert 等人[11]提出了基于云平台的智能手机应用程序自动安全检验框架.Martignoni 等人[12]提出了一种基于行为的恶意软件分析框架,在云端模拟客

户环境执行目标软件并进行分析.

6.4 数字版权管理服务

Wang 等人[13,14]提出了基于云平台的 SIM 卡数字版权管理系统,将数字版权管理系统的许可证服务和内容服务放到云中,以能够向用户提供优质的服务.

安全服务运行在云平台具有降低客户端消耗、提高安全服务质量等优点.因此,"安全即服务"成为未来安全保护软件的发展趋势.

7 结束语

目前工业界云计算产品已经使用的安全策略只能针对现有的安全攻击技术进行保护,而对云计算中新型的安全问题还没有加以考虑.另外,因为缺少密文域上的运算(例如高效的支持加密的搜索等),大部分用户内容在云端还是以明文方式存放.我们对现阶段对云安全的研究做以总结和归纳,在云安全的各个方面目前都有学者展开了研究,并且已经取得了不错的成果.云计算作为一个新兴的产业发展非常迅速,我们期待着其中的安全问题能够早日被完善解决并在实际产品中得以应用.

参考文献

[1] M Armbrust, A Fox, R Griffith, et al. A view of cloud computing[J]. Commun ACM, 2010, 53(4): 50 – 58.

[2] B Hayes. Cloud computing[J]. Commun ACM, 2008, 51(7): 9 – 11.

[3] 冯登国,张敏,张妍,徐震.云计算安全研究[J].软件学报,2011,22(1):71 – 83.
Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security[J]. Journal of Software, 2011, 22(1): 71 – 83. (in Chinese)

[4] L Popa, M Yu, et al. Cloud police: taking access control out of the network[A]. Hotnets'10. ACM 2010[C]. New York: ACM, 2010. 1 – 6.

[5] F Hao, TV Lakshman, S Mukherjee, and HY Song. Secure cloud computing with a virtualized network infrastructure[A]. The 2nd USENIX Conference on Hot Topics in Cloud Computing[C]. Boston, Massachusetts, 2010. 1 – 7.

[6] J Oberheide, E Cooke, F Jahanian. Cloudav: N-version antivirus in the network cloud[A]. Proceedings of the 17th Conference on Security Symposium[C]. Berkeley, CA, USA: USENIX Association, 2008. 91 – 106.

[7] J Oberheide, K Veeraraghavan, E Cooke, J Flinn, and F Jahanian. Virtualized in-cloud security services for mobiledevices[A]. Proceedings of the First Workshop on Virtualization in Mobile Computing[C]. New York, USA: ACM, 2008. 31 – 35.

[8] R Chow, M Jakobsson, R Masuoka, Jlina, Y Niu, E Shi, Z Song. Authentication in the clouds: a framework and its application to mobile users[A]. Proceedings of the 2010 ACM Workshop on Cloud computing Security Workshop[C]. New York, USA: ACM, 2010. 1 – 6.

[9] G Portokalidis, P Homburg, K Anagnostakis, H Bos Paranoid Android: versatile protection for smartphones[A]. In Proceedings of the 26th Annual Computer Security Applications Conference[C]. ACM, New York, NY, USA: ACM, 2010. 347 – 356.

[10] 吴吉义,傅建庆,平玲娣,谢琪.一种对等结构的云存储系统研究[J].电子学报,2011,38(5):1100 – 1107.
Wu Ji-yi, Fu Jian-qing, Ping Ling-di, Xie Qi. Study on the P2P cloud storage system[J]. Acta Electronica Sinica, 2011, 38(5): 1100 – 1107. (in Chinese)

[11] P Gilbert, B G Chun, L P Cox, and J Jung. Vision: Automated security validation of mobile apps at app markets[A]. The second International Workshop on Mobile Cloud Computing and Services[C]. ACM, 2011. 21 – 26.

[12] L Martignoni, R Paleari, D Bruschi. A Framework for behavior-based malware analysis in the cloud[A]. Fifth International Conference on Information Systems Security[C]. 2009. 178 – 192.

[13] C K Wang, P Zou, Z Liu, J M Wang. CS-DRM: A cloud-based SIM DRM scheme for mobile internet[J]. EURASIP J Wirel Commun Netw, 2011, 14(1): 22 – 30.

[14] P Zou, C K Wang, Z Liu, D L Bao. Phosphor: A cloud based DRM scheme with sim card[A]. 12th International Asia-Pacific[C]. 2010. 459 – 463.

[15] Amazon Web Services. [EB/OL]. http://aws.amazon.com/, 2012-10-07.

[16] Windows Azure. [EB/OL]. http://www.microsoft.com/windowsazure/, 2012-10-07.

[17] A Hudic, S Islam, P Kieseberg, and E RWeippl. Data Confidentiality using fragmentation in cloud computing[J]. Int J Communication Networks and Distributed Systems, 2012, 1(3/4): 1 – 10.

[18] D Slamanig. Efficient schemes for anonymous yet authorized and bounded use of cloud resources[J]. Lecture Notes in Computer Science, 2012: 73 – 91.

[19] M R Asghar, M Ion, G Russello, B Crispo. Securing data provenance in the cloud[J]. Lecture Notes in Computer Science, 2012: 145 – 160.

[20] Gentry. Fully Homomorphic Encryption using ideal lattices[A]. STOC '09[C]. New York, NY: ACM, 2009. 169 – 178.

[21] MV Dijk, C Gentry, S Halevi, V Vaikuntanathan. Fully Homomorphic encryption over the Integers[A]. In EuroCrypt' 10[C]. Springer 2010. 24 – 43.

[22] C Gentry. A fully Homomorphic Encryption Scheme[D]. Ph

D Thesis, Stanford University, 2009.
[23] SG Sutar, GA Patil. Privacy management in cloud by making use of Homomorphic functions[J]. International Journal of Computer Applications, 2012.37(2)13 – 16.
[24] D Song, D Wagner, A Perrig. Practical techniques for searches on encrypted data[A]. In Proc of IEEE Symposium on Security and Privacy[C]. 2000.
[25] R Curtmola, J A Garay, S Kamara, R Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions[A]. In Proc of ACM CCS'06[C]. 2006.
[26] D Boneh, G D Crescenzo, R Ostrovsky, G Persiano. Public key encryption with keyword search[A]. In Proc of EUROCRYP'04[C]. 2004.
[27] M Bellare, A Boldyreva, A O'Neill. Deterministic and efficiently searchable encryption[J]. In Proceedings of Crypto of LNCS: Springer-Verlag, 2007(4622).
[28] J Li , Q Wang, C Wang, N Cao, K Ren, W Lou. Fuzzy keyword search over encrypted data in cloud computing[A]. In IEEE INFOCOM'10, Mini-Conference[C]. NJ: IEEE Press, Piscataway, 2010.441 – 445.
[29] C Wang, N Cao, J Li, K Ren, W Lou. Secure ranked keyword search over encrypted cloud data[A]. In ICDCS 2010[C]. Washington, DC: IEEE Computer Society, 2010.253 – 262.
[30] N Cao, C Wang, M Li, K Ren, and W J Lou. Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data [A]. 31st International Conference on Distributed Computing Systems(ICDCS)[C]. 2011.393 – 402.
[31] Amazon. Amazon Simple Storage Service[EB/OL]. http://aws.amazon.com/s3/, 2012-10-07.
[32] Amazon. Amazon Elastic Block Storage[EB/OL]. http://aws.amazon.com/ebs/, 2012-10-07.
[33] Nirvanix Cloud. Why Nirvanix[EB/OL]. http://www.nirvanix.com/company/why-nirvanix.aspx, 2011-10-12/2012-10-09.
[34] Kleiminger M . Stream processing in the cloud[D]. London: Imperial College, 2010.
[35] Kleiminger M, Kalyvianaki E, et al. Balancing load in stream processing with the cloud[A]. IEEE 27th International Conference on Data Engineering Workshops[C]. Germany: IEEE Press, 2011.16 – 21.
[36] Du J, Wei W, et al. RunTest: assuring integrity of dataflow processing in cloud computing infrastructures[A]. In Proc 5th ACM Symposium on Information, Computer and Communications Security[C]. New York: ACM Press, 2010.293 – 304.
[37] Du J, Gu X, et al. On verifying stateful dataflow processing services in large-scale cloud systems[A]. Proceedings of the 17th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2010.672 – 674.
[38] Du J, Shah N et al. Adaptive data-driven service integrity attestation for multi-tenant cloud systems[A]. IEEE 19th International Workshop on Quality of Service[C]. New York: IEEE Press, 2011.1 – 9.
[39] Ateniese G, Burns R, et al. Provable data possession at untrusted stores[A]. Proceedings of the 14th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2007.598 – 609.
[40] Wang C, Wang Q et al. Privacy-preserving public auditing for data storage security in cloud computing[A]. InfoCom 2010 Proceeding[C]. San Diego: IEEE Press, 2010.1 – 9.
[41] Hao Z, Zhong S, Yu N Y. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability[J]. IEEE Transactions on Knowledge and Data Engineering, September 2011, 23(9): 1432 – 1437.
[42] Yu S C, Wang C, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[A]. InfoCom 2010 Proceedings[C]. San Diego: IEEE Press, 2010.1 – 9.
[43] Wang G, Liu Q, et al. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services[A]. Proceedings of the 17th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2010. 735 – 737.
[44] Hong C, Zhang M, et al. Achieving efficient dynamic cryptographic access control in cloud storage[J]. Journal of China Institute of Communications, 2011, 32(7): 125 – 132.
[45] Chow SSM, Chu C K, et al. Dynamic secure cloud storage with provenance[J]. Lecture Notes in Computer Science, 2012, 6805: 442 – 464.
[46] Tsai CS, Lee CC, et al. Password authentication schemes: Current status and key issues[J]. International Journal of Network Security, 2006, 3(2): 101 – 115.
[47] ISO/IEC 9594-8: 2001, Information technology Open Systems Interconnection The Directory: Public-key and attribute certificate frameworks[S].
[48] Yan L, Rong C, et al. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography[J]. In Cloud Computing of Lecture Notes in Computer Science, 2009, 5931: 167 – 177.
[49] Li H, Dai Y, et al. Identity-based authentication for cloud computing[J]. In Cloud Computing of Lecture Notes in Computer Science, 2009, 5931: 157 – 166.
[50] Bertino E, Paci F, et al. Privacy-preserving digital identity management for cloud computing[A]. Bulletin of the IEEE Computer Society Technical Committee on Data Engineering [C]. New York: IEEE Press, 2009.21 – 27.
[51] Hao Z, Zhong S, Yu N H. A time-bound ticket-based mutual authentication scheme for cloud computing[J]. International Journal of Computers, Communications & Control, 2011, 6 (2): 227 – 235.

[52] Li W J, Ping L D. Research on trust management strategies in cloud computing environment[J]. Journal of Computational Information Systems, 2012, 8(4): 1757 – 1763.

[53] Song H, Zhang B, et al. A credibility model of web service on internet[J]. Advances in Intelligent and Soft Computing, 2012, 136: 533 – 540.

[54] Groß S, Schill A. Towards user centric data governance and control in the cloud[J]. Lecture Notes in Computer Science, 2012, 7039: 132 – 144.

[55] Amazon. Amazon Elastic Compute Cloud[EB/OL]. http://aws.amazon.com/ec2/, 2012 – 03 – 15/2012 – 10 – 08.

[56] Bleikertz S, Schunter M, et al. Security audits of multi-tier virtual infrastructures in public infrastructure clouds[A]. Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop[C]. New York: ACM Press, 2010. 93 – 102.

[57] Laurikainen R. Improving the efficiency of deploying virtual machines in a cloud environment[D]. Finland: Aalto University, Programme of Computer Science and Engineering, 2012.

[58] Zhao HM. A study on architecture of private cloud based on virtual technology[J]. Lecture Notes in Electrical Engineering, 2012, vol. 126: 155 – 165.

[59] Deboosere L, Vankeirsbilck B, et al. Efficient resource management for virtual desktop cloud computing[J]. The Journal of Supercomputing, 2012, vol. 62: 741 – 767.

[60] Peng C Y, Kim M, et al. Virtual machine image distribution network for cloud data centers[A]. IEEE International Conference on Computer Communications (INFOCOM 2012)[C]. Orlando, IEEE Press, 2012. 181 – 189.

[61] Azab A M, Ning P, et al. HyperSentry: enabling stealthy in-context measurement of hypervisor integrity[A]. Proceedings of the 17th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2010. 38 – 49.

[62] Wei J P, Zhang X L. Managing security of virtual machine images in a cloud environment[A]. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security[C]. New York: ACM Press, 2009. 91 – 96.

[63] Bugiel S, Nürnberger S, et al. AmazonIA: when elasticity snaps back[A]. In Proceedings of the 18th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2011. 389 – 400.

[64] Amazon SimpleDB[EB/OL]. http://aws.amazon.com/simpledb/, 2012-03-15/2012-10-08.

[65] Amazon Web Services: Overview of Security Processes. http://aws.amazon.com/, 2008-09/2012-10-08.

[66] Liu H. A new form of DOS attack in a cloud and its avoidance mechanism[A]. Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop[C]. New York: ACM Press, 2010. 65 – 76.

[67] Ristenpart T, Tromer E, et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds[A]. Proceedings of the 16th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 2009. 199 – 212.

[68] Okamura K, Oyama Y. Load-based covert channels between Xen virtual machines[A]. In Proceedings of the 2010 ACM Symposium on Applied Computing[C]. New York: ACM Press, 2010. 173 – 180.

[69] FIPS PUB 197: 2001, Advanced Encryption Standard (AES)[S]

[70] Rivest R L, Shamir A. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[71] Cooney M. New technology performs calculations on encrypted data without decrypting it[EB/OL]. http://www.computerworld.com/s/article/9134823/, 2009-06-25.

[72] Li M, Yu SC, et al. Authorized private keyword search over encrypted data in cloud computing[A]. In ICDCS, 2011[C]. USA: IEEE Press, 2011. 383 – 392.

[73] Boldyreva A, Chenette N, et al. Order-preserving symmetric encryption[J]. EUROCRYPT 2009 (A. Joux, ed.) of Lecture Notes in Computer Science, 2009, 5479: 224 – 241.

[74] Wong WK, Cheung DW, et al. Secure KNN computation on encrypted databases[A]. In Proc of SIGMOD[C]. SIGMOD Press, 2009. 139 – 152.

[75] Goldreich O. Foundations of cryptography[M]. Cambridge Univ. Press, 2004. 1 – 320.

[76] Okamoto Takashima K. Hierarchical predictate encryption for inner-products[J]. In Advances in Cryptology-ASIACRYPT of LNCS, 2009, 5912: 214 – 231.

[77] Deswarte Y, Quisquater J J. Remote integrity checking[A]. In Sixth Working Conference on Integrity and Internal Control in Information Systems[C]. Kluwer Academic Publishers, 2004. 1 – 11.

[78] Filho DLG, Barreto PSLM. Demonstrating data possession and uncheatable data transfer[J]. Cryptology ePrint Archive, 2006, Report 2006/150: 1 – 9.

[79] Sebe F, Domingo-Ferrer J, et al. Quisquater. efficient remote data possession checking in critical information infrastructures[J]. IEEE Trans on Knowledge and Data Engineering, 2008, 20: 1034 – 1038.

[80] Curtmola R, Khan O, et al. MR-PDP: Multiple-replica provable data possession[A]. ICDCS′08[C]. USA: IEEE Press, 2008. 411 – 420.

[81] Wang Q, Wang C, et al. Enabling public verifiability and data dynamics for storage security in cloud computing[J]. 14th European Symposium on Research in Computer Security, 2009, 5789: 355 – 370.

[82] Zhu Y, Wang H, et al. Efficientprovable data possession for hybrid clouds[J]. Cryptology ePrint Archive, Report 2010/234:1 – 3.

[83] Hao Z, Yu NH. A multiple-replica remote data possession checking protocol with public verifiability[A]. The Second International Symposium on Data, Privacy, & E-Commerce (ISDPE), 2010 Second International Symposium[C]. USA: IEEE Press, 2010. 84 – 89.

[84] Chang E C , Xu J. Remote integrity check with dishonest storage server[J]. 13th ESORICS, 2008, 5283:223 – 237.

[85] Chen B, Curtmola R, et al. Remote data checking for network coding-based distributed storage systems[A]. In CCSW '10: Proceedings of the 2010 ACM workshop on Cloud computing security workshop[C]. New York: ACM Press, 2010. 31 – 42.

[86] Curtmola R, Khan O, et al. Robust remote data checking[A]. In StorageSS' 08: Proceedings of the 4th ACM international workshop on Storage security and survivability[C]. New York: ACM Press, 2008. 63 – 68.

[87] Wang C, Wang Q, et al. Ensuring data storage security in cloud computing[A]. In Quality of Service, 2009. IWQoS. 17th International Workshop[C]. Chicago: IEEE Press, 2009. 1 – 9.

[88] Diffie W , Hellman ME. New directions in cryptography[J]. IEEE Transactions in Information Theory, 1976, 22(6):644 – 654.

[89] Goodrich M. T. , Tamassia R, et al. Implementation of an authenticated dictionary with skip lists and commutative hashing [A]. DARPA Information Survivability Conference and Exposition II[C]. USA: DARPA Information Survivability Conference Press, 2001. 68 – 82.

[90] Papamanthou C, Tamassia R, et al. Authenticated hash tables [A]. Proceedings of the 15th ACM conference on Computer and communications security[C]. New York: ACM Press, 2008. 437 – 448.

[91] C. Merkle R. Protocols for public key cryptosystems[J]. Proc. 1980 Symposium and Privacy, 1980, 122 – 134.

[92] Boneh D, Lynn B, et al. Short signatures from the weil pairing [J]. ADVANCES IN CRYPTOLOGY—ASIACRYPT 2001, 2001, 2248:514 – 532.

[93] D. Bowers K, Juels A, et al. HAIL: a high-availability and integrity layer for cloud storage[A]. In CCS'09: Proceedings of the 16th ACM Conference on Computer and Communication Security[C]. New York: ACM Press, 2009. 187 – 198.

[94] Sandhu R S, Coyne E J, et al. Role-based access control models[J]. Computer, 1996, 29(2):38 – 47.

[95] F. Ferraiolo, D, Sandhu R, et al. Proposed NIST standard for role-based access control[J]. ACM Trans Inf Syst Secur, 2001, 4(3):224 – 274.

[96] Goyal V, Pandey O, et al. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM conference on Computerand communications security[C]. New York: ACM Press, 2006. 89 – 98.

[97] Blaze M, Bleumer G, et al. Divertible protocols and atomic proxy cryptography[J]. Lecture Notes in Computer Science, 1998, 1043:127 – 144.

[98] Kallahalla M, Riedel E, et al. Plutus: Scalable secure file sharing on untrusted storage[A]. In Proceedings of the 2nd USENIX Conference on File and Storage Technologies[C]. Berkeley: USENIX Association Press, 2003. 29 – 42.

[99] Green M, Hohenberger S, et al. Outsourcing the decryption of ABE ciphertexts[A]. In Proceedings of the 20th USENIX Security Symposium[C]. San Francisco: USENIX Association Press, 2011. 1 – 16.

[100] Gamal T E. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. CRYPTO, 1985, 196:10 – 18.

[101] Liu Q, Tan C C, et al. Reliable re-encryption in unreliable clouds[A]. Proceedings of GLOBECOM 2011[C]. USA: IEEE Press, 2011. 1 – 5.

[102] Gentry C, Silverberg A. Hierarchical id-based cryptography [J]. Advances in Cryptology—Asiacrypt 2002, 2002, 2501: 149 – 155.

[103] Bethencourt J, Sahai A, et al. Ciphertext-Policy attribute-Based encryption[A]. IEEE Symposium on Security and Privacy[C]. USA: IEEE Press, 2007. 321 – 334.

[104] Plouffe C R, Hulland J S, et al. Research report: Richness versus parsimony in modeling technology adoption decisions understanding merchant adoption of a smart card-based payment system[J]. Information Systems Research, 2001, 12(2):208 – 222.

[105] Wang C, Zhou Y. A collaborative monitoring mechanism for making a multitenant platform accountable[A]. HotCloud'10 Proceedings of the 2nd USENIX conference on Hot topics in cloud computing[C]. Berkeley: USENIX Association Press, 2010. 18 – 18.

[106] Haeberlen A, Aditya P, et al. Accountable virtual machines [A]. Proceedings of the 9th USENIX conference on Operating systems design and implementation[C]. Berkeley: USENIX Association Press, 2010. 1 – 16.

[107] Murray D G, Milos G, et al. Improving Xen security through disaggregation[A]. VEE '08 Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments[C]. New York: ACM Press, 2008. 151 – 160.

[108] Dai W, Jin H, et al. TEE: a virtual DRTM based execution environment for secure cloud-end computing[A]. CCS '10Proceedings of the 17th ACM conference on Computer and commucations security[C]. New York: ACM Press, 2010.

663 – 665.

[109] Barham P, Dragovic B, et al. Xen and the art of virtualization [A]. Proceedings of the nineteenth ACM symposium on Operating Systems Principles (SOSP'03) [C]. New York: ACM Press, 2003. 164 – 177.

[110] Aviram A, Hu S, et al. 2010. Determinating timing channels in compute clouds [A]. CCSW'10 Proceedings of the 2010 ACM workshop on Cloud Computing Decurity Workshop [C]. New York: ACM Press, 2010. 103 – 108.

[111] 张尧学,周悦芝.一种云计算操作系统 TransOS:基于透明计算的设计与实现[J].电子学报,2011,38(5):985 – 990.

Zhang Yao-xue, Zhou Yue-zhi. A new cloud operating system: Design and implementation based on transparent computing[J]. Acta Electronica Sinica, 2011, 38(5): 985 – 990. (in Chinese)

作者简介

俞能海　男,1964 年生于安徽无为.中国科学家技术大学信息科学技术学院教授,博士生导师.研究方向图橡处理体内容安全、互联网信息检索与数据挖掘.

E-mail: ynh@ustc.edu.cn