文章编号:1009-2552(2015)03-0202-04 DOI:10.13274/j.cnki.hdzj.2015.03.050

云计算数据安全关键技术研究

王希忠，吴 琼，黄俊强，宋超臣

（黑龙江省电子信息产品监督检验院，哈尔滨 150090）

摘 要：针对云计算国内外发展现状及趋势，阐述了云计算数据安全与隐私保护问题，分析并探讨了云计算数据安全所面临的挑战及关键技术，针对云模式下的数据安全提出了相应的解决方案。

关键词：云计算；数据安全；关键技术

中图分类号：TP309 **文献标识码**：A

Research on key technology of cloud computing data security

WANG Xi-zhong, WU Qiong, HUANG Jun-qiang, SONG Chao-chen

(**Heilongjiang Provincial Electronic & Information Products Supervision Inspection Institute, Harbin** 150090, **China**)

Abstract: For the cloud computing technology development status and trends of domestic and abroad, this paper expounds the cloud computing data security and privacy issues, analyzes and discusses on the challenges and the key technology of cloud computing data security, then proposes the corresponding solutions in the cloud model of data security.

Key words: cloud computing; data security; key technology

0 引言

美国国家标准和技术研究院(NIST)为云计算给出如下定义:云计算就是以快捷、按需的形式,利用网络从可配置的资源共享池中获取服务的一种计算模式[1]。自“云计算”(Cloud computing)概念首次提出后,云计算就以其便捷、经济、高可扩展性等优点得到国内外产业界、学术界、政府的广泛关注。但与此同时,作为一种新型技术,其应用服务的推广使用情况并没有人们想象中的那么乐观,最主要的原因就是由于大规模资源共享所带来的数据安全问题。与传统信息系统安全问题相比,大规模数据的集中存储使得云计算平台必将成为黑客攻击的主要目标[2]。2009 年 Gartner 调研报告显示,70% 以上企业因对云计算数据安全和隐私性保护存在顾虑而对云计算应用持观望态度;欧洲网络和信息安全研究机构 ENISA 也表示,云计算数据安全性、隐私性以及应用的稳定性将成为用户是否使用云服务以及选择何种云计算服务商的主要衡量准则。近几年,云计算倡导者 Google,以及 Microsoft、Amazon 等云计算服务提供的霸主屡屡被爆出各类隐私数据泄露事件,进一步加剧了人们对云计算数据安全的担忧。因此,要想让更多的机构和企业大规模使用云计算应用平台,放心将海量数据交付于云计算提供商集中管理,首先应着手解决的就是云计算数据安全问题。

1 云计算数据安全挑战

在云计算环境中,用户数据主要以两种形态存在:静态存储和动态传输。当处于静态存储时,用户数据可进行备份处理;当处于动态传输时,用户数据可储存在磁盘缓冲区或网络中[3]。所谓数据的生命周期,即用户数据从创建、传送至云平台数据中心直至彻底销毁的全过程,其可细分为 7 个阶段,如图 1 所示。

当信息安全向云计算过渡时,云计算平台特有的模式结构将给传统的数据安全方法带来挑战,在

收稿日期：2014-05-13

作者简介：王希忠(1968-),男,研究员级高级工程师,研究方向为网络与信息安全、物联网、信息系统风险评估等。

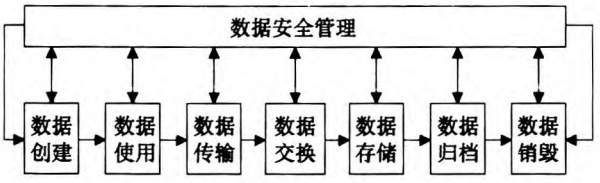

图1 数据安全生命周期模型

整个云计算数据生命周期中，主要的安全挑战如下：

(1)数据丢失与泄露风险。云计算采用大规模数据集中管理方式，但其对数据的安全控制力度并不够，安全机制的缺失以及安全管理的不足都可能引发数据丢失和泄露，无论是国家重要数据或者个人隐私数据，一旦丢失或被窃取都将造成非常严重的后果。

(2)数据访问控制风险。云中存储着海量数据、应用和资源，如果云平台没有完善的身份验证机制，入侵者将会非常轻松地获取到个人信息，甚至利用所获得的信息进行非法操作。

(3)数据隔离风险。用户对云计算有不可控性，因此不同用户之间的数据应采用有效的隔离或加密措施，以保障用户数据在使用、传输和存储过程中不与其他用户数据混合，同时防止其他不发份子非法获取他人数据。

(4)数据传输和存储风险。由于病毒和恶意攻击的威胁，仅采用加密技术是不能完全保证数据安全性的，同时用户数据也面临着传输和存储信息完整性受到破坏所带来的风险。

(5)剩余数据风险。数据必须彻底有效地去除才被视为销毁，不彻底的数据清除、硬件设备的维修与保费都可能导致敏感数据被泄露所带来的风险。因此，必须具备一种有效的技术，实现云计算数据的准确定位，并保证数据的彻底清除和销毁且无法恢复。

(6)数据可用性及恢复风险。由于自然或人为因素造成数据损坏在所难免，因此，必须保障备份数据的可用性，云计算数据备份和恢复计划必须到位、有效，以防止因数据丢失、意外覆盖或破坏所带来的风险。

2 云计算数据安全关键技术

云用户数据传输、存储、处理等操作均与云计算系统有直接关系，在云计算虚拟化的应用环境下，云用户面临的数据安全威胁更加突出。为了给云用户提供全面的信息安全与隐私保护，访问控制、数据隔离、加密传输、安全存储等关键技术必不可少，只有保证此类安全技术的有效实施，才能确保云计算数据安全。

2.1 数据访问控制

在云计算用户重要信息数据的访问控制方面，可采用基于身份认证的授权控制技术，对用户身份进行实时监控和权限认证，以防止云用户之间的非法越权访问。针对云计算虚拟应用环境，可以对虚拟环境下网络边界的安全访问控制策略进行设置，例如通过虚拟防火墙等方法来实现虚拟机组内部重要数据的访问控制。

2.2 数据安全隔离

数据的集中存储不可避免会出现相互干扰的安全风险，为实现不同用户信息数据的安全隔离，可根据实际需求，采用物理隔离、虚拟化隔离等技术手段将各类服务器和域名完全隔离，在减少单点故障的同时，采用不同数据库存储不同应用系统数据的方式，保障每个云计算用户信息数据的安全与隐私。

2.3 数据加密传输

在云计算环境下，数据传输不可避免，因此数据传输过程中的安全性保障非常重要。数据加密技术可在网络链路层、传输层以及网络层实现，通过加密技术可保障云计算用户信息数据的完整性、机密性、可用性。在前段，可采用 SSL、SSH 等加密协议为数据传输提供加密通道，保障并维护数据安全；在后端，可采用 VPN、SSL 等方式防止非法攻击者对数据的窃取和篡改，为云计算用户提供网络传输数据的安全性。

2.4 数据安全存储

服务 DaaS，即云计算平台的存储服务，是服务 IaaS(云计算基础设施)的重要形式之一。云平台存储中的数据均为静态数据，探讨此类数据的安全性问题，直观的方法即是对数据进行加密。假若加密后的数据被恶意窃取，对于不发份子来说，他们获取的只是一段乱码，并且无法获悉其具体信息。因此，在加密算法的选择上，应选用如 3DES、AES 等国际通用的、加密性能较高的算法，亦可选择我国国有商密算法 SCB2 等。在密钥管理方面，为实现用户信息数据的高效安全管理，可以采用集中式密钥管理和分发机制。对于服务 DaaS，云计算系统应支持数据加密存储服务，以防止不法份子的恶意窥探，而对于虚拟机等服务，建议云计算用户对个人敏感信息的上传、存储采用必要的加密技术。

3 云计算数据安全防护方案

3.1 云计算数据安全体系架构

云计算最主要的安全问题莫过于数据安全和隐私保护，因此，国内外已有研究者提出了以数据安全

为核心的云计算安全体系架构。DSLC(Data Security Life Cycle)就是一种数据安全防护体系,该体系由管理策略、安全技术以及监管机制组成,按三个步骤为云平台中的数据提供安全可靠保障。首先,由于数据在云中的存储形式有所不同,因此需先对云中数据进行获取、存储、传输和处理;随后,建立包括创建、使用、传输、交换、存储、归档和销毁等6个阶段在内的数据安全生命周期;最后,明确数据安全生命周期内每个阶段的数据安全保护机制,将云平台使用者所有可能的行为限制在一定安全范围内。文献[4]提出了一种参考性的云计算数据安全框架,其主要包括数据安全服务体系和安全标准及测评体积两大部分。其中,数据安全服务体系又分为云安全基础服务、可信云基础设施服务以及云安全应用服务,该体系结合云环境的不同层次为保障数据安全提供技术支撑;而数据安全标准及测评体系则为数据安全服务体系提供必要的技术和理论支撑。文献[5]则从运营管理、技术防护、政策保障等方面提出了一种可信云计算环境来保障云中数据安全。

3.2 身份认证

在云环境下,用户选择不同的云服务提供商,因为拥有不同的身份标识,容易被混淆或遗忘,为了保障用户身份的可控性,目前主流的身份认证方法有单点登录、联合身份认证等。

(1)单点登录(Single Sign-on,SSO),即用户身份信息及相关属性能够安全传送至云服务的能力。单点登录允许本次信息管理系统可以向其他云计算系统认证该用户身份,因此用户只需在使用某项云服务时注册并登陆一次,从而减轻不必要负担。目前典型的单点登录协议是OpenID协议,Google服务商支持OpenID协议的单点登录技术;另外SAML也是一种XML单点登录开放标准,Salesforce服务商支持该技术。

(2)联合身份认证,即在不同服务商的身份信息库间建立关联。当用户在使用某个云平台服务并实现登录时,该用户就可以访问与之相关的其他已被信任的云平台,无需重复注册多个账号并登录。联合身份认证基于单点登录技术,如SAML联合身份认证,该方法权威通过数字签名发布一个令牌给一个用户,该用户可使用令牌跨域访问其他已被信任平台,无需重复登录认证。此外,PKI联合身份认证技术也是目前较为广泛使用的一种联合身份认证方案。

3.3 数据隔离防护

密文处理技术是保护数据机密性的一种最直接的方法。文献[6]提出全同态加密技术,该技术利用理想格的数学对象建立了隐私同态算法,能够实现数据在加密状态下的操作。文献[7]将可信计算与同态加密技术相结合,能够有效地为用户提供云计算服务。随着加密技术的发展,一些基于策略模型的安全机制也被应用到了云计算动态数据的隔离保护中。文献[8]提出了一个虚拟化安全保护框架,利用沙箱机制对云计算数据进行隔离。该框架采用Linux系统的chroot命令创建了一个独立的虚拟系统,并利用chroot命令可更改路径的功能创建新的指定目录,在新的指定目录中,用户无法访问旧系统中的数据及文件,由此将云数据进行安全隔离。文献[9]构建了一种可信SaaS平台TSP,并为SaaS提供了一个封闭的环境,能够保障用户隐私数据只能在Terra平台专用虚拟机中执行和处理。

3.4 数据安全存储

云平台中存储的数据多为静态数据,因此数据存储的安全性、完整性、可用性成为用户关注的主要问题。目前最为直观的解决方法就是对数据进行加密处理,文献[10]提出了一种基于用户端的隐私数据管理工具,可为云服务用户提供一个信息模型,帮助用户控制隐私数据在云平台中的存储和使用。文献[11]提出了一种基于数字签名的完整性校验技术,验证者可以通过验证自己存储在校验模块中的数字签名,从而确定存储数据是否是完整的。在数据的可用性上,Google GFS提出了3个副本的容错技术,可实现存储数据效率和可靠性的平衡,此外,秘密共享和纠删编码等技术也常用于保证数据的可用性。

3.5 可信云计算

将可信计算与云计算相结合,可使云计算服务商以一种可信赖的方式为用户提供服务,因此可信云计算技术也成为云安全领域中的一个重要研究方向。可信计算的核心思想就是可信传递,从可信根出发,通过扩展信任边界从而确保整个系统的可信。在云计算平台中,文献[12]提出了一种可信云环境的安全框架,引入信任传递和可信根的概念,实现了Guest OS kernel、虚拟机监控以及云计算应用服务的安全性度量与验证功能。文献[13]提出基于虚拟机架构的可信云计算平台Terra,该平台通过一个具有防篡改功能的可信硬件平台,利用可信虚拟机监控器建立了多个互相隔离的具有高可用性的虚拟机,并利用远程证明机制向远程用户端证明自身数据的完整性。

4 结束语

目前，如 Amazon、Microsoft、IBM 等云服务提供商纷纷提出并部署了云计算数据安全解决方案，电信运营商 Verizon 也推出了云安全特色服务。随着云计算技术的发展，如何确保用户隐私数据不被窃取或丢失，如何保障云服务提供商的访问控制机制和安全管理机制符合云服务用户的安全需求，如何避免云环境下多用户共存所带来的潜在危险都将成为云计算所面临的安全挑战。本文围绕云计算数据安全周期和主要威胁等问题进行了阐述，并综合访问控制、数据隔离、加密传输、安全存储等关键技术，对云计算数据安全解决方案进行了系统研究，今后研究的重点将着重于具体数据安全防护措施的技术研究上以及云计算数据安全应急机制的研究。

参 考 文 献：

[1] 林闯，苏文博，孟坤，等. 云计算安全：架构、机制与模型评价[J]. 计算机学报，2013，36(9)：1765－1784.

[2] 杨建，汪海航，王剑，等. 云计算安全问题研究综述[J]. 小型微型计算机系统，2012，33(3)：12－14.

[3] 孙弘逸. 云计算数据隐私保护方法的研究[D]. 南京：南京邮电大学，2012.

[4] 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.

[5] 沈昌祥. 解析“云计算”的安全问题[J]. 中国高新区，2011(12)：20－21

[6] Gentry C. Fully homomorphic encryption using ideal lattices[C]. Proc. of the 2009 ACM Int'lSymposium on Theory of Computing, 2009.

[7] Sadeghi AR, Schneider T, Winandy M. Token-Based cloud computing: Secure outsourcing of data andarbitrary computations with lower latency [C]. Proc. of the 3rd Int'l Conference on Trust and Trustworthy Computing, 2010.

[8] Jianxin Li, Bo Li, Tianyu Wo, et al. CyberGuarder: A Virtualization Security Assurance Architecture for Green Cloud Computing[J]//Future Generation Computer Systems, 2012.

[9] Chaoliang Zhong, Jun Zhang, Yingju Xia. Construction of a Trusted SaaS Platform[C]//IEEE International Symposium on Service Oriented System Engineering, 2010.

[10] Mowbray M, Pears on S. A client-based privacy manager for cloud computing [C]. Proceedings of the 4th International ICST Conference on Communication System Software and Middleware, New York, USA: Association for Computing Machinery, 2009.

[11] Wang Qian, Ren Kui, Lou Wen-jing, et al. Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance[C]// IEEE INFOCOM 2009 proceedings, 2009.

[12] 沈昌祥. 云计算安全与等级保护[J]. 信息安全与通信保密，2010，1：16－17.

[13] Garfinkel T, Pfaff B, Chow J, et al. Terra: A virtual machine-based platform fortrusted computing[C]. Proc. SOSP'03, 2003.

责任编辑：么丽萍

(上接第 201 页)

4 逻辑功能验证

对系统的逻辑功能验证是基于电机空载并由 LED 指示继电器状态的方法，本文自定义验证模式 1 和验证模式 2 分别对车门控制单元逻辑功能进行验证，这两次验证可以遍历系统几乎所有的特定逻辑状态。

验证模式 1(控制台全车操作)：控制台选择左后视镜操作、全车模式，保持按下右后门车窗升按键、后视镜水平调节按键和后视镜垂直调节按键，按动右前门车窗降按键和中控门锁按键，观察五个节点的 LED 状态。重点观察的是：主控节点和左前节点外后视镜垂直调节 LED 亮；按下右前门车窗降按键时，四门车窗升降 LED 均亮，弹起右前门车窗降按键时，四门车窗下降 LED 熄灭；按动中控门锁按键时，四门门锁运行 LED 与门锁锁止 LED 相应触发。

验证模式 2(控制台与车门按键协调)：控制台选择右后视镜操作、单门模式，保持按下右后门车窗降按键和后视镜水平调节按键，在左后节点、左前节点和右后节点上按动车窗升按键和门锁按键，观察五节点的 LED 状态。重点观察的是：主控节点和右前节点外后视镜水平调节 LED 亮；右后节点的车窗下降 LED 保持点亮，其余各门车窗和门锁的 LED 均随本地按键触发与变化。

5 结束语

利用全新的汽车总线标准 FlexRay 研究了一种新型的车门控制系统，实现包括车门控制单元中车窗、后视镜和门锁几个方面的联动功能和本地的防夹功能，使得车门节点的实时性更好，并且有助于未来整车的网络标准统一，减少不必要的网关节点，增加车身电子控制系统的实时性和可靠性。

参 考 文 献：

[1] 王绍铣，李建秋，夏群生. 汽车电子学[M]. 2 版. 北京：清华大学出版社，2011.

[2] Daniel ROUCHE. 汽车车载网络(VAN/CAN/LIN)技术详解[M]. 北京：机械工业出版社，2006.

[3] 王锴，王宏，徐皑冬. 下一代车载网络 FlexRay 及其应用研究[J]. 计算机工程与应用，2008，44(20)：77－79，98.

[4] Freescale Semiconductor. MC9C12XF reference manual[EB/OL]. www. freescale. com.

[5] 宋磊，马季雯. 电动窗防夹力的标定[J]. 汽车电器，2007(5)：51－53.

责任编辑：肖滨