云计算安全问题研究

王 磊 孙 琪 刘 琛 刘 赫
中国电子科技集团公司第十五研究所（信息产业信息安全测评中心），北京 100083

[摘要]云计算是一种大众参与的计算模式，它以互联网为基础，以动态、虚拟化和服务方式提供，包括计算能力、存储能力、互动能力等。云计算环境下，将成为云中数据存储安全保障面临的艰巨挑战，数据存储安全面临巨大挑战。
[关键词]云计算；安全；研究
DOI：10.33142/sca.v6i10.10206 中图分类号：TP393 文献标识码：A

Research on Cloud Computing Security Issues

WANG Lei, SUN Qi, LIU Chen, LIU He
The 15th Research Institute of China Electronics Technology Group Corporation (Information Industry Information Security Evaluation Center), Beijing, 100083, China

Abstract: Cloud computing is a participatory computing model that is based on the Internet and provides dynamic, virtualized, and service-oriented services, including computing power, storage capacity, and interactive capabilities. In the cloud computing environment, it will become a daunting challenge for data storage security in the cloud, and data storage security will face enormous challenges.
Keywords: cloud computing; safety; research

1 计算概述

1.1 云计算技术概念

云计算技术是把强大的数据处理能力分解成多个单元，由多个服务器组成的庞大系统。通过多个单元进行处理和计算，来得到最终分析结果传回给回用户，这也被称作分布式计算。最原始的云计算技术，就是把计算问题解决在多个单元的分布式操作系统中，运算结束后，把结果进行汇总。通过分布式计算技术，大量的数据的处理可以在几秒钟的时间内完成，从而实现强大的计算服务。

1.2 系统架构

云计算平台架构体系可分为如图 1 所示的云计算系统架构模型中的基础硬件设施和设备部分，资源抽象和控制部分，云服务部分，运维运营和管理部分。基本硬件设备有物理机房相关设施、服务器操作系统、硬盘、网络和安全设备等。软件包括计算资源池、存储资源池、云控制台、网络和安全资源池等部分；云服务的主要形式涵盖 IaaS 服务模式、PaaS 服务模式、SaaS 服务模式等。

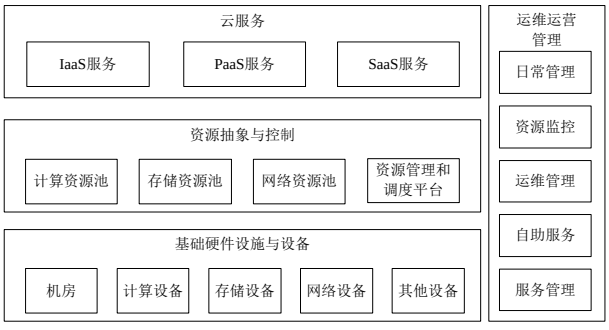

图 1 云计算系统架构模型

1.3 云计算技术特点

云计算技术是一种高性能的分布式计算技术，包括高可用性、计算以及存储扩展性好、VPC 技术成本低。但是，所有基于互联网的应用都存在一定的风险，在存储服务所面临的问题不可避免的情况下，作为服务的云计算也不例外。如果商业用户大规模采用民间机构提供的云计算服务，这些民间机构利用“数据”的重要性向全社会施加压力，即便技术实力再强，也难以避免。对于资讯社会来说，“资讯”是必不可少的。另一方面，尽管对于商业机构来说，提供云计算并没有什么不透明的地方，但云计算中的数据却是数据拥有者之外的机密。这就好比普通人不可能对别人的电话进行窃听，但在电讯公司内部，随便一个电话都能被人轻易地监听到一样。商业机构、政府机构在选择云计算服务的时候，一定要把这些已知风险都列为考虑范围，尤其是在使用外资机构参与控股的云计算公司提供的服务。

1.4 云计算概述

虽然云的应用和推广势在必行，但人们对它的安全性一直耿耿于怀，这是云诞生以来的事情。当云雾缭绕的无形云雾中散播着所有计算行为和数据存储时，人们普遍会产生一种不受控制的恐慌情绪，并会毫无例外地产生这样的疑问：云雾会不会使自己的隐私受到损害，进而使自己的权益受到损害？最新调查显示，美国安全研究机构波耐蒙研究所发现，IT 专业人士担心敏感数据可能被不怀好意的人获取。如果这家企业采用的是云计算技术的话。与此同时，不少受访者坦言，部分可能早已采用云计算的企业员工对这些风险置之不理。

以云服务模式来说，目前已经被大家熟知的三个模式，

可能都不是很合理的。IaaS（基础服务）、PaaS（平台服务）和 SaaS（软件服务），美国国家标准技术研究院对它们的定义如下：

IaaS（基础服务）为用户提供包括操作系统在内的任何软件的基本计算资源的服务，如处理、存储和网络等，用户可以部署并在此之上运行。用户无需对云上的网络设备、物理机房等进行管理，只对云平台上租用的服务器、数据库、存储等计算资源进行管理，在计算资源上搭建属于自由应用系统，通过云控制台对安全资源进行控制，如安全组、云防火墙、入侵检测、防病毒和 VPC 等。

PaaS（平台服务）为用户提供云的平台服务，用户只需在平台上部署相关应用系统，不对底层的服务器、数据库、存储等计算资源进行管理，相关计算资源管理由云平台负责。

SaaS（软件服务）为云用户提供软件服务，云平台只给用户提供应用账号，支撑应用的服务器、数据库、存储等计算资源以及各类云安全防护均由云平台负责，云平台用户只需要负责应用账户的配置和应用的数据备份等。

尽管用户将计算和存储完全委托给云服务提供商，但在使用服务时，从云的三种云服务模式来看，不能只依靠云供应商来处理所有的安全问题。特别是在保障策略上。三款云服务机型安全防护各有不同，无论从方法上还是职责上。SaaS 对云服务商提出了物理、网络、服务器、数据库、软件等方面的安全要求，需要建立起保障服务安全的整体防护体系。但这也限制了使用者自由发挥创意的空间。相反，IaaS 为用户创造所需的计算环境和开发和部署应用程序提供了充分的灵活性。不过，在计算系统的层级架构中，用户也需要对每一层进行自我管理。供应商只需要关注硬件等级的安全性，除了最底层的硬件。PaaS 定位于两款服务模式之间，形成全方位的保护系统。不仅要求云服务商提供基础层面的方案策略，也要求在安全防护上对云的用户提供第三方接口，云的用户可以选择云平台根据的安全服务，也可以通过第三方服务来对云计算资源进行安全防护。同时这也造成了 PaaS 服务模式的安全问题，即模糊了供应商与用户之间的责任界限。

云计算的安全问题究竟出在哪里？

首先，在技术层面上，如果云计算已经实现，用户可能会感到力不从心，因为技术上的问题而导致服务中断。今后，人们很少会在本地硬盘上存储数据，而会在云端保存所有的数据。

其次，云是不透明的、外部化的，涉及到一系列细节，包括用户位置、员工情况、技术使用和操作方法等，云计算服务商对此并未做出具体解释。每一个被接受的外包服务提供商基本上都是将计算处理或数据存储服务以一种隐蔽的方式提供给上层的服务提供商，这样在计算服务由多个服务提供商提供的情况下，各个服务提供商所使用的技术实际上是不受控制的，即存在持续外包的可能。所以每一项服务都是由上一家厂商提供的，如果云服务商非授权访问了用户的数据是可能不被发现的。尽管每个云服务商都声称使用完整性和保密性技术来保护用户的数据不被篡改和获取，但这仅仅是指在处理和存储数据时仍然无法解决对数据的保护，而仅仅是将传输的数据加密到网络上，即使这些数据使用了 SSL 技术来加密。特别是在数据处理上很难获得用户的信任，因为数据已经解密，如何保护数据以赢得用户信任变得困难。

2 云计算应出安全隐患

2.1 对保存文件进行加密

有了密钥才可以进行解密工作，加密技术能够加密文件。加密技术能够让用户在非本地的机房上传数据，也能对数据起到保护作用。

2.2 对 Email 进行加密

Email 是到达你的收件箱的格式，它仍然可以被偷窥者访问。为了保证邮件的安全，你可以自动加密你所接收和发送的所有邮件，例如 Foxmail 程序软件。

2.3 使用信誉良好的服务

推荐使用有名望的服务，他们不会让信息外泄，也不会让信息分享给经销商，不太可能拿自己的名牌冒险。

2.4 考虑商业模式

与那些获得广告资助的服务相比，收费的互联网应用服务或许更为保险。那么在选择存储环境的时候，付费存储是第一考虑的。

2.5 阅读隐私声明

隐私声明必须在数据被存储到云计算环境下才能被读取，这使得隐私政策在一些情况下数据被共享，因为几乎每一个互联网应用都存在漏洞。这样，你就能分辨出你的电脑上应该保存哪些数据，云计算环境下应该保存哪些数据。

2.6 使用过滤器

科技公司为监控离开公司的网络，实用技术手段对敏感数据进行处理。

2.7 安全传输手段

在数据的网络传输过程中，采用完整性和保密性手段确保数据在传输过程中的安全性等多种不同的方式来保护数据的安全。

此外，在业务层面也应采取完整性和保密性等相关手段，让用户放心地使用云计算平台。

第一，云计算服务商规模应选择在国内注册，且经营规模大，有盈利的公司。这样，才能在确保长期提供稳定、安全、可靠服务的同时，也才能在法律监督下遵守驻在国的法律。事故发生后，赔偿或追讨工作才得以顺利开展，因为他们的总部或资产都在国内。

此外，云计算服务商要尽可能不采用私有标准，按照开放标准开展相应应用。至少需要提供一个数据导入和导出的框架，如果没有可遵循的标准来保证和方便数据迁移。

以及必要的数据转换机制来保证数据的迁移。

3 云计算技术等级保护方案介绍

3.1 云计算业务模式发展

云计算技术对网络架构、系统的部署产生了巨大的影响。新的模式是一次重要的信息化变革，让用户在云端享受到各种服务，无论何时何地，都能更灵活、更自由地使用终端设备。

3.2 云计算服务安全需求

终端方面，主要考虑云计算用户使用终端的安全。采用云桌面的方式是一个成熟的方式。把云桌面部署到云计算平台中，云桌面提供虚拟化的管理终端，各类管理员仅能通过个人终端连接云桌面后，方能对云上的服务器、数据库、存储等计算资源的管理进行管理。云平台对云桌面进行了安全处理，可以使云桌面免受外界攻击。

传输方面，我们主要通过密码技术，对各类数据进行真实性、完整性、保密性、不可否认性等保护。

云计算平台方面，云计算平台针对物理环境、通信网络、区域边界、计算环境、管理中心等，通过身份鉴别、访问控制、入侵防范、防病毒、审计、数据备份、信息保护等方式进行安全防护，对整个云环境生命周期的构建，基于客户的实际需求和相关的安全合规标准，以及数据安全体系的构建。数据安全协议的设计涵盖了数据的创建，传输，存储，使用，分享和销毁的所有环节。确保云平台用户的数据在云计算平台的完整性、保密性和可用性等。

3.3 云环境下的等级保护

在等级保护中，云计算平台可分为安全计算、安全网络和安全管理等部分，其中安全管理域是云计算的重要组成部分。安全计算域是由通信网络和接入网络组成的物理主机/服务器集合，这些主机/服务器的安全防护等级相同。安全管理领域是一个系统平台，用于整体云计算中的安全事件收集和控制报警。云计算中的安全计算环境，安全区域边界，安全通信网络，安全管理中心，涵盖了云计算的各个安全区域，与之相对应的安全措施主要有以下几个方面：

（1）安全计算环境[1-2]。云计算环境包含私有云安全计算域（PrivateCloudSecurityComputing）、公共云安全计算域（PublicCloudSecurityComputing）。其中，部署安防设备的重点是私有云安防计算域，主要可采取的安防措施有：主机加固、加密机等 4A 系统、虚拟安防网关、设备及手段等。对扩散到公有云平台上的资源、数据等。

（2）安全区域边界[1-2]。安全区域边界主要通过边界防护、防病毒、访问控制、防入侵、审计等措施对各安全区域的边界进行防护。在云租户控制台云安全组策略上启用指定端口进行跨边界的网络通信，并配置和启用相关安全策略，在云安全防护区边界处部署云防火墙和访问控制模块，并启用了访问控制功能，设备的最后一条访问控制策略为禁止所有网络通信。购买云平台提供的云安全中心包括网络入侵检测服务，能够对外部发起的网络攻击行为进行检测、记录和阻断。部署云防病毒网关，能够对恶意代码进行检测和清除。

（3）安全通信网络[1-2]。安全通信网络主要通过网络架构设计、通信传输保护等来对安全通信网络进行防护。基于业务需求划分不同的安全域，用户已自行配置 IP 地址范围、配置路由器和网关。配置云安全组访问控制策略，通过 VPC 进行区域划分。重要网络区域不部署在边界处。

（4）安全管理中心[1-2]。安全管理中心主要通过系统管理、安全管理、审计管理和集中管控的方式实现安全管理。通过运维审计系统对服务器、数据库、网络设备、安全设备的系统管理员进行身份鉴别，并记录运维人员的操作日志；通过堡垒机对应用系统的系统管理员进行身份鉴别，只允许应用系统管理员通过操作界面进行系统管理操作，并对这些操作进行审计。通过系统管理员对用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等系统资源和运行进行配置、控制和管理。部署了网管平台能够对网络设备的日志进行统一收集、分析和存储，只允许审计管理员通过特定的操作界面进行安全审计操作，并对这些操作进行审计。运维审计系统能够对服务器、数据库、网络设备、安全设备的管理员运维日志进行统一收集、分析和存储，只允许审计管理员通过特定的操作界面进行安全审计操作，并对这些操作进行审计。审计管理员通过网管平台、运维审计系统对审计记录进行分析，根据安全审计策略对审计记录进行管理和查询，审计记录保存 6 个月以上，每天备份一次审计记录，限制审计管理员对审计记录文件的删除操作。通过运维审计系统对服务器、数据库、网络设备、安全设备的安全管理员进行身份鉴别，只允许其通过特定的操作界面进行安全管理操作，并对这些操作进行审计；通过堡垒机对网络设备的安全管理员进行身份鉴别，只允许其通过特定的操作界面进行安全管理操作，并对这些操作进行审计。

4 结束语

在云计算更加普及的当下，应该更加重视安全问题。用户存储在云端的数据如何保证安全，对于云服务提供商而言？云中的数据安全是由云服务提供的，对于用户而言，又如何能够信以为真呢？云计算落地，将是一个刻不容缓的难题。

[参考文献]

[1]GB/T 22239-2019.信息安全技术 网络安全等级保护基本要求[S].北京:中国标准出版社,2019.

[2]GB/T 29448-2019.信息安全技术 网络安全等级保护测评要求[S].北京:中国标准出版社,2019.

作者简介：王磊（1987.4—），毕业院校：中国矿业大学（北京），所学专业：计算机应用技术，当前就职单位：中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)，职称级别：工程师。