文章编号:1671-4598(2019)05-0199-04 DOI:10.16526/j.cnki.11—4762/tp.2019.05.044 中图分类号:TP3 文献标识码:A

# 基于云计算的数据安全风险及防御策略研究

王晓妮[1], 段 群[2]
(1. 咸阳师范学院 信息中心, 陕西 咸阳 712000; 2. 咸阳师范学院 计算机学院, 陕西 咸阳 712000)

**摘要**: 云计算因其存储容量大和计算能力强等优点深得人心, 然而云技术却为数据安全带来新的威胁; 由于云平台与用户间存在大量数据交互, 故在整个数据生命周期中存在的一系列安全风险; 文章针对这些数据安全风险从国家监管、专业人员的技术研发、云供应商的可信服务和云相关人员的防范意识这四个方面来展开研究, 提出了相应的数据安全保护模型和防御策略, 能够较好的解决云计算数据安全风险问题。

**关键词**: 云计算; 数据安全; 防御策略

# Research on Data Security Risk and Defense Strategy Based on Cloud Computing

Wang Xiaoni[1], Duan Qun[2]
(1. Information Center, Xianyang Normal University, Xianyang 712000, China;
2. School of Computer Science, Xianyang Normal University, Xianyang 712000)

**Abstract**: Cloud computing is popular because of its large storage capacity and computing power. However, cloud technology brings new threats to data security. Due to the large amount of data exchanged between the cloud platform and users, there is a series of security risks in the whole life cycle of the data. According to these data security risks, this paper studies from four aspects: state regulation, technical research and development of professionals, credible services of cloud providers and prevention awareness of cloud-related personnel, and puts forward corresponding data security protection models and defense strategies. It can solve the problem of cloud computing data security risk better.

**Keywords**: cloud computing; data security; defense strategy

## 0 引言

随着计算机网络和信息化技术的迅速发展和应用, 目前云计算这种新型的服务模式和计算技术应运而生, 因其成本低、存储容量大、计算能力强、按需分配和便于管理等优点深得人心[1]。云计算是信息领域内的一场技术革命, 使信息技术正朝着集约化、规模化和专业化的方向发展, 这引起了各大 IT 企业和各国政府的高度重视。随着云计算应用的不断普及和应用, 它为人们的日常生活提供了许多便利。然而糟糕的是频发的云计算数据安全事件对人们的生活造成严重的影响, 同时也制约了云计算的发展[2]。例如 Google (2009 年 3 月)、Apple (2010 年 6 月)、索尼 (2011 年 4 月) 等公司都发生过用户数据泄密事件; 2012 年亚马逊的数据中心宕机事件; 2014 年 12 月第三方漏洞报告指出铁路 12306 网站存在漏洞, 导致客户信息数据 (账号、密码和身份证等) 泄密, 使许多企业和用户遭受损失, 影响恶劣。由于云计算将计算任务和用户数据管理全部交由云平台去处理, 导致用户对其数据管理无法具体控制, 彻底打破了传统的分布式计算中的用户数据存放在本地由用户自己监管, 这样就出现用户隐私数据频繁泄露的事件。云计算作为新兴技术目前正处在发展期, 人们对其安全问题缺乏深入的研究, 故其数据安全问题亟待解决。

## 1 云计算技术

### 1.1 云计算的概念

云计算 (Cloud Computing) 是一种由计算机网络和通信技术创新发展而来的商业化计算模型, 融合了并行计算、网格计算、效用计算、分布式计算、负载均衡、网络存储和虚拟化等计算机网络技术[3]。该模型采用在资源池上分布计算任务和按需分配业务模式, 根据实际需求为用户提供相应的计算能力、信息数据、存储空间或软硬件资源和优质的服务, 从而实现一定范围内便捷的计算机网络资源共享。云计算具有可度量服务、广泛的网络访问、按需自助服务、资源共享和快速的可伸缩性这五个基本特征[4]。按照美国 NIST 的定义, 采用混合云、社区云、私有云和公有云这四种类型来部署云计算[5], 云计算包括这三个云服

**收稿日期**:2018-10-30; **修回日期**:2018-11-26。
**基金项目**:陕西省教育科学"十三五"规划 2017 年课题 (SGH17H196); 咸阳师范学院专项科研基金资助项目 (13XSYK087)。
**作者简介**:王晓妮(1977-),女,陕西乾县人,硕士,工程师,主要从事计算机应用、网络安全方向的研究。
段 群(1980-),女,陕西礼泉人,硕士,副教授,主要从事 CUDA 并行计算、大数据技术方向的研究。

务：平台即服务（PaaS）、软件即服务（SaaS）和基础设施即服务（IaaS）。通常按照基云层次栈来划分云计算的结构体系，如图 1 所示，大致可分为云服务供应商和云用户两大部分，具体来说由管理层、应用层、资源层、用户访问层和平台层组成[6]。

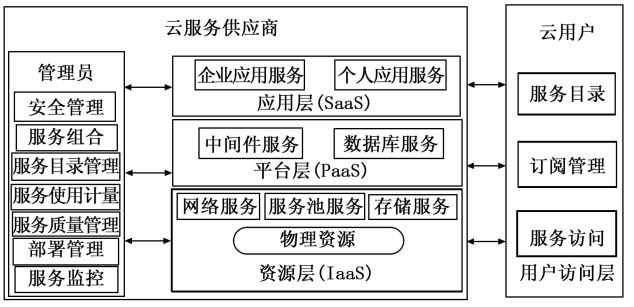


图 1 云计算体系结构图

### 1.2 云计算数据生命周期

云计算用户数据一般以静态存储和动态传输这两种形态存在，在静态存存储时可以进行数据的备份；在动态传输时用户数据常被存储在网络或硬盘缓冲区中。在云计算环境中，用户云数据通常存在生命周期[7]，其生命周期模型如图 2 所示。云数据的生命周期共分为数据创建、使用、传输、交换、存储、归档、迁移和销毁这八个阶段，包括了云数据从产生、传送至云数据中心到最终彻底销毁的整个过程。

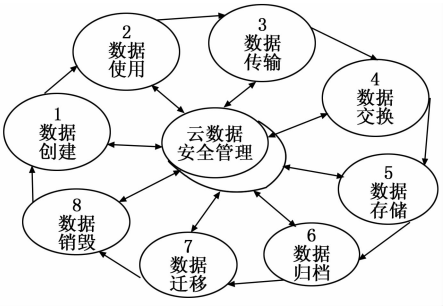


图 2 云数据生命周期模型

## 2 云计算存在的数据安全风险分析

自从云计算这种崭新的服务模式诞生以来，更多的用户把数据存储在了云端服务器上，数据计算、存储和保护等这些任务都是通过网络交由云平台服务器来实现的。对用户来说云相当于黑盒子，数据在什么地方的什么服务器上是如何存储的一概不知，纯粹依赖云计算提供商全权管理，而用户完全失去了对其数据的监控权，这就使云数据更集中化。然而云平台的结构复杂化、环境虚拟化、用户多样化、网络开放化和数据动态化等这些特点，有别于以往的传统网络下数据安全。通常传统网络环境中能用边界防护技术如 IDS 和防火墙等，而这些技术在边界模糊的云计算虚拟环境下是无用的[8]。故数据风险基本贯穿在云数据的整个生命周期中，主要来自以下几个方面。

### 2.1 数据传输风险

云计算环境中，用户数据都是通过网络来传输的，而数据传输要经过许多通信设施和设备，这就难免在传输过程中既遭遇电磁波干扰或泄密，又存在通信线路被监听或数据非法截获，一旦发生网络硬件设备故障或软件技术失误就容易造成病毒感染、黑客入侵和非法操作等安全风险。故用户数据传输过程中需要考虑如何确保数据传输通道的安全[9]？

### 2.2 数据存储风险

云计算中能够实现资源共享的重要环节就是数据存储，其存在的潜在风险：1）存储设备的老化或服务器宕机，直接造成用户数据的损坏。2）云平台中加密后的数据难以实现检索或运算等操作，故用户数据未被加密或进行动态保护，以文本的形式静态存储在云端服务器上，一旦黑客利用此漏洞盗取或篡改数据，导致大规模的数据损坏、泄露和扩散。3）云提供商为了降低成本，把不同用户的数据存储在同一虚拟集群中，所有用户数据未进行有效隔离杂糅在一起，而是采用标记来区别和调取不同的数据。此时如果在应用执行层中数据标签被破坏或发生冲突，就会出现数据被错误调取。4）云供应商为了节省存储空间，没有对数据进行必要的容错或异地备份，一旦灾难发生就无法及时完全的恢复数据。5）由于各国针对网络安全的法律政策和管理办法不同[10]，而云计算的数据存储又存在跨国性，这便造成各国对数据安全的管理差异很大，导致跨国存储的云数据存在一定的泄密风险。

### 2.3 数据使用风险

云供应商或用户由于自身原因有意或无意的对数据进行了非法操作，造成数据在使用过程中存在这些风险：1）云供应商对管理员没有实现责权分开和缺乏必要的员工培训，导致管理员对数据中心的管理权限太大，一旦管理员违背职业道德，对云端服务器进行错误的配置或操作失误，都会造成用户数据泄露或破坏。2）由于云计算对用户要求较低，只需终端设备能通过互联网访问云端服务器，加之用户安全意识淡薄和缺乏专业知识，既不能正确保管自己合法授权信息，又无法保证其终端设备的安全。云终端由于技术上的缺陷存在一些不可避免的漏洞，严重的威胁着终端设备的稳定性，增大了其被木马病毒攻击和感染的概率，造成数据的直接外泄和损坏。

### 2.4 数据迁移风险

任何技术都不是万能的，故云端服务器有可能会出现“宕机”，但必须保证正在进行的服务不受影响，这就需要把正在工作中的进程快速的迁移到别的服务器中。其实迁移进程就是迁移与进程相关的存储在硬盘上的静态数据或内存或寄存器中的动态数据（进程快照），而且只有快速迁移才能让用户体会不到发生过“宕机”时间[11]。在迁移的过程中必须保证所有数据的完整性和正确性，才能使进程在新的服务器上恢复正常运行。迁移对正在进程中运行的

隐私数据，存在较大的泄密、丢失或损坏风险。

### 2.5　数据销毁风险

数据用完后需要从云端服务器中销毁，但一般云管理员采用的是直接删除或覆盖的方式，这就会引起数据残留现象。虽然逻辑上看数据是被删除了，但它在物理上还是存在的[12]，并未彻底的销毁。而把这些残留数据通过设备硬件维护或保养便能恢复出部分敏感数据，造成隐私数据泄露风险。

### 2.6　数据审计风险

云服务为了确保用户数据的完整、有效和准确，在操作时需要第三方认证机构对数据进行必要的审计。审计主要任务是确保用户存储在云端的外包数据归用户所有，任何非授权用户不得使用[13]。由于用户数据存放在云端服务器上，增加了审计的难度。因为用户无法承受巨大的通信费用故不能将全部数据下载后再审计，只能下载少量代表性的核心数据，交给审计机构通过概率分析或某种知识证明协议等手段来判断云端数据的完全性。故在数据审计过程中，存在审计时效性差、准确率低和数据泄密等风险。

## 3　云计算数据安全风险的略防御策略

从上面的分析可知，云计算中的数据在其整个生命周期中都面临着许多风险，这将严重阻碍云计算技术的广泛应用和迅速发展。针对云计算数据安全的这些威胁，结合云计算虚拟化、多租户和动态性的特点，建立一个云计算数据安全保护模型[14]，如图 3 所示。该模型从国家监管、专业人员技术研发、提供商云服务和用户运用这四个方面多层次和多角度来立体纵深来建立一种可信云计算防御体系架构，确保云计算数据在其整个的生命周期的安全。

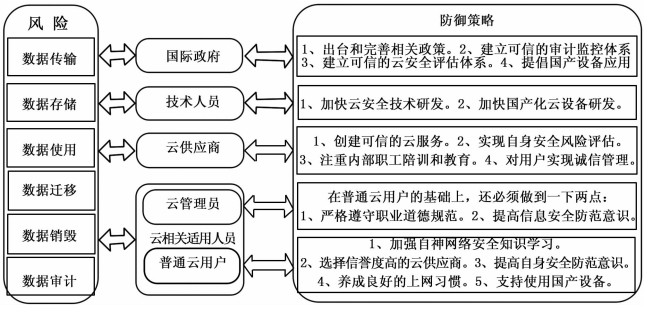


图 3　云计算数据安全保护模型

### 3.1　国家应建立可控的云安全监管体系

国家政府部门必须针对目前云计算的数据安全问题采取这些必要措施。

1）出台和完善相关的法律制度，弥补现有政策法规的不足。建立符合跨境信息流动的法律政策，使国家信息安全标准国际化。以便在处理跨国信息传输过程中出现的国际矛盾与冲突时有法可依。限制那些肆虐猖獗的破坏数据安全的违法行为，加大对黑客非法攻击网络的惩罚力度，确保授权用户的数据安全，建立和谐的云计算网络环境。

2）针对云数据安全建立可信的审计监控体系。推行实现第三方数据安全审计和监管，使云服务运营制度化和数据安全管理常态化。要把前期审计和后期监管相结合，提前检查分析和预测云计算中会发生的数据安全问题，做好预防措施，尽量杜绝出现管理或技术漏洞。

3）建立可信的云安全评估体系。①对云计算供应商的诚信度，建立详细明确的评估标准。②对云计算的基础设施、服务协议、潜在威胁、风险意识和防范措施进行评估和检测。使用户在选则云供应商时心中有数，有据可依。

4）大力提倡、支持和奖励国有设备的生产及应用。同时相关部门要制定相关奖励政策，提高云计算专业人员的技术研发工作积极性。

### 3.2　专业人员要加强云安全新技术的研发

在云计算应用过程中，滞后的技术存在漏洞和缺陷直接威胁着数据安全。

1）加强云安全技术的研发和应用，这是确保云计算数据安全的有效措施和得力保障。

（1）不断完善数据加密、入侵检测、身份认证、数字签名、融在备份和防火墙等传统网络安全技术存在的漏洞和不足。（2）根据云计算技术发展的趋势和特征，着重虚拟化、全同态加密、可信访问控制、数据（隔离、擦除、销毁、追回）、隐私保护、强效加密、权限控制、智能防火墙、海量数据的分布存储和过滤等技术的研发运用。

2）加快国产云技术设备普及和研究，早日实现云计算安全技术的自主可控。华为、中兴和浪潮等国内大型 IT 企业要积极响应国家号召，了解前沿技术和行业特点，抓住机遇加大国产云计算技术设备的研发和生产应用，尽快改变我国云计算核心技术设备和关键基础设施对国外高度依赖的现状。

### 3.3　云计算供应商要提高诚信度，提供可靠的云服务

既然用户把数据存储在云端服务器上，那么云服务商就要负责数据安全和监控管理。

1）创建可信的云服务确保数据安全。结合多种认证方式、可信算法、虚拟化和分布式计算技术建立从底层到顶层的可信云计算系统，为用户提供可靠的云服务。为了确保用户数据安全，具体采用这些云服务安全防御措施：（1）云计算服务安全架构。IaaS 层采用权限管理设置、用户认证、VPN 通道和智能防火墙等；SaaS 层采用身份认证、授权认证、Web 浏览器安全配置和访问控制等；PaaS 层采用身份认证、权限管理、单点登录、SSL 和 TLS 安全协议等策略来确保云计算基础服务安全。（2）数据安全架构。①数据传输。采用可靠安全的网络传输协议、同态加密技术、部署安全组策略、智能防火墙和信任机制来预防网络黑客木马攻击，确保数据的安全传输。②数据存储。对相互干扰或冲突的数据采用隔离存储，对核心的数据采用异地容灾备份和分级存储技术，结合数据备份和迁移策略，尽量

降低数据存储风险发生概率。③数据使用。采用过滤器技术来监控正在被使用的数据，防止数据被窃取。④数据销毁。采用可擦除技术和彻底销毁物理硬盘的办法来处理残留数据泄密的问题。

2）实现自身安全风险评估。云供应商要根据相关的法律政策和自己的实际情况制定出符合国家标准、适合自身条件和满足用户需求的安全服务等级，让用户以此作为科学依据对云服务商所提供的云计算相应等级服务进行判断，对其提供的云应用和服务进行风险评估。云供应商必须配合审计机构，确保服务的安全可靠，尽量减少用户数据的泄密风险。

3）注重内部职工的安全培训和教育。不断完善内部培训机构，进一步规范和加强内部员工的日常管理工作，提高其职业道德和操守。对系统管理员建立严格的身份和权限管理制度，禁止随意移动和更换硬件设备。采用责权分明和最小权限法，细化安全级别使不同级别人员享有不同的系统管理权限。将云管理员分为核心数据操作员和普通系统维护员。核心数据操作员能处理所有数据，但必须遵守一定的流程和制度，要保存好详细的造作日志记录。普通维护员负责云服务安全，管理一般数据的日常维护，无权操作核心数据。必须要提供详细真实、完整可靠的系统日志来全面监控整个系统的正常安全运行。防止少数人权限太过集中，杜绝管理员因为操作失误或为了经济利益而盗窃篡改合法用户数据事件发生。

4）对用户实现诚信管理。按照信任级别和云用户业务需求，根据评估量化的用户行为数据来规范监督用户行为，对所有用户按诚信级别来进行权限划分和数据访问控制。不断健全云用户安全访问控制服务和身份鉴别机制，采用数字签名、实名制、USB Key 身份认证和动态口令等多种用户认证技术相结合对用户进行管理，以此来确保用户身份的合法性、安全性和唯一性。增加用户身份验证流程和环节，使用指纹、特殊认证（虹膜、声音、指纹）和人脸识别技术，动态和静态密码相结合，以此来全方位、多角度验证用户信息。加大信息安全的宣传力度，为用户提供必要的网络安全培训机会。使用户系统全面的认识信息安全，理解云数据安全的重要性，能够按要求进行规范操作，提高防范意识，尽量降低泄密事件和误操作发生概率，便能降低数据风险发生概率。

### 3.4 增强相关人员的云计算数据安全防范意识

为了更好利用和发展云计算技术，必须树立和增强相关人员的网络安全防范意识。

#### 3.4.1 普通云用户

1）加强自身网络知识的学习。经常了解云计算新技术，关注信息安全动态，更新网络安全知识，熟悉隐私数据保护措施和网络终端设备的使用。2）选择信誉度高的云供应商。良莠不齐的云供应商提供的服务质量差别悬殊，为了确保服务质量和数据安全，要结合国家标准和自身需求尽可能的选择规模大和知名度的云供应商。只有诚信度高的供应商才有实力为用户提供专业的技术设备、优质的基础服务和有力的数据安全防御措施。3）提高自身安全防范意识。保管好自己的授权信息，密码设置时尽量采用字母和数字相结合，提高密码的复杂度和经常更改密钥。定期整理重要或敏感的隐私数据，必须经过加密后才能把数据传输和存储在云端服务器上，及时定期进行异地手动备份。尽量避免利用公用的 WIFI 账号或设备来共享，访问云端的隐私数据。4）养成良好的上网习惯。所有上网的终端设备必须安装云杀毒软件，定期进行软件更换、病毒库升级、漏洞扫描和查毒。禁止非法用户对自己设备的随便访问，不打开或访问不明来历的邮件、连接和网站。要通过可靠的网站下载软件。5）尽量选用国产设备。改变传统观念，增强对对国产设备和技术要有信心，竭尽全力优先使用能够自主可控的国产新技术新设备。对待国产设备的不足和缺陷要给予高度理解，要给这些网络设备厂商试用和完善的机会。只有让国产设备和技术尽快发展和迅速强大，才能有效促进我国云计算进步，有实力保护对外竞争激烈的机密数据和国家信息安全。

#### 3.4.2 云服务管理员

在普通云用户的基础上还要做到几点：1）严格遵守职业道德规范，提高自身修养，经得起巨大的经济诱惑和考验，避免出现内部泄密事件。2）提高信息安全防范意识，确保用户数据的保密性和安全性。①数据加密。利用 DES（传输）和 RSA（存储非对称文件或密钥）加密技术巧妙结合的方式来处理用户数据，合法用户必须通过私钥才能访问和使用相关数据。②数据存储。对数据存储结构进行优化，分层次按类型对用户数据相互隔离存储。为了更好的进行数据灾难恢复，先把核心数据地址进行伪装，然后在普通数据的掩护下再把这些机密数据分散存储在云端网络数据库的不同区域。③实时监控。利用过滤器（Vericept 或 Websense）技术随时监控用户数据传输或远程操作过程，一旦发现可疑数据或者是非法入侵破坏行为及时进行过滤和拦截，防止木马病毒的攻击和和用户数据泄露。

## 4 结束语

云计算技术是目前信息时代的核心技术，并在人们的日常生活中被广泛应用，为人们的工作和生活带来许多便利。但是云计算毕竟是个新兴技术，正处于发展阶段，难免会存在一些网络安全问题和数据风险，严重阻碍了云计算的发展和用户体验。本文通过国家监管、专业人员的技术研发、云供应商的可信服务和云相关人员的防范意识这四个方面来展开研究，采取相应具体措施组建起云计算数据安全保护模型，不但能够较好的解决云计算数据风险问题，而且推动了云计算技术向更好的方向良性发展。

（下转第 225 页）