云计算安全风险及对策

杨 巍 李 刚
（南京大学信息管理学院，江苏南京 210093）

摘 要：云计算平台的安全性问题越来越受到广泛的关注，同时也只有完善云计算共享服务的安全性问题，才能有效促进其发展进程。首先对云计算共享服务模式和目前存在的云服务安全风险架构进行分析；然后对云服务面临的新的或传统风险中被忽略而在云计算中被放大的安全风险及对策进行初步探讨。

关键词：云计算；共享服务；安全风险；风险应对
中图分类号：TP399 **文献标识码：**A DOI：10.3772/j.issn.1674-1544.2013.02.018

Security Risks and Its Countermeasure in the Cloud Environment

Yang Wei, Li Gang
(School of Information Management, Nanjing University, Nanjing 210093)

Abstract: Security issues of cloud computing platform have been paid more and more attention to, and security issues of shared services should be improved in order to promote the development of cloud computing effectively. First, the article analyzes shared service model of cloud computing and security risks framework. Second, the article discusses the countermeasures of new security risks or traditional risks magnified in the cloud environment simply. This article has certain significance on solving security risks of cloud sharing service and in-depth study in the future.
Keywords: cloud computing, shared services, security risks, countermeasure for risks

1 引言

Google CEO埃里克·施密特于2006年提出了“云计算”概念，这使计算机领域的发展有了新的导向。特别是近几年来，缘于云计算强大的计算功能、海量的存储能力及低廉的使用成本[1]，使得关注“云计算技术”的组织不再局限于Google、亚马逊、微软、IBM等大型IT公司，越来越多的行业领域开始投入到云计算的应用中来。然而，云计算在迅速发展的同时也引入了大量的安全风险问题[2]。Gartner在于2008年发布的“云计算风险评估”报告中指出，部分企业会先通过第三方中立评估机构获得一个云计算安全评估报告，然后才会考虑是否再应用云计算平台[2]；2009年，“信息管理与信息组织（AIIM)”组织的一项调查显示，在澳大利亚，77%的机构是出于信任机制问题而不愿意使用公共云服务[3]。由此可见，云计算平台的安全性问题越来越受到广泛的关注，其中包括传统IT风险，也包括云计算带来的值得关注的新型风险问题，因此，只有完善云服务的安全性问题，才能有效促进云计算的共享服务。

2 云计算服务模式、部署模式及安全风险

常见的云计算服务模式有3种：SaaS(软件即服务）、PaaS(平台即服务）和IaaS(基础设施即服务），见图1。

SaaS是基于互联网提供软件服务的软件应用模式，SaaS提供大量优质简单易用的软件运作平台，并对软件实施的过程进行安全保管及维护，用户通过互联网就可以使用信息系统，随时随地享受云服务[4],如门户、CRM、即时通信等。PaaS为云计算功能的实施创造环境，PaaS是SaaS模式的一种应

第一作者简介：杨巍（1988- ），女，南京大学信息管理学院硕士研究生，研究方向：档案信息利用。
收稿日期：2012年9月24日。

用，是将一个完整的计算机平台，包括应用设计、应用开发、应用测试、应用托管等，都作为一种服务提供给客户[5]，如并行计算、数据库等各种中间件服务。典型的PaaS平台有微软Windows Azure 平台、Facebook开发平台等。IaaS提供给用户的是与基础设施有关的服务，例如硬件、设备、相关软件等资源，并且基础设施服务可以根据资源需求按比例伸缩[5]，其所涉及的服务有基础管理、基础服务、基础设施等，如图1所示。

以上述3种服务模式为基础，云计算有4种部署模式：公共云、私有云、社区云和混合云[6]。公共云被公众使用，由云服务提供商通过自己的基础设施向用户提供服务；私有云是向单个用户提供服务，并被其独立操作；社区云是由几个有公共关注问题的集团或组织共同操作的云；混合云是由两个或两个以上性质的云组成，通过制定标准或利用专利技术，将不同性质的云结合在一起，使数据和应用程序可以移植，实现资源共享。

通过对云计算服务部署模式的分析，可知云服务已经发展成为跨越互联网、涵盖计算机网络各个层次、涉及各种网络技术的服务。因此，从硬件安全到软件安全，从内部安全到外部安全，网络层次的各项漏洞都不可避免地给云服务带来意想不到的安全风险。云服务的迅速发展同时也给云计算共享服务的安全带来了巨大的挑战，这也引起越来越多的国际组织开始关注云服务安全风险问题。

CSA（Cloud Security Alliance，云安全联盟）根据云服务的3种服务模式，构建了云服务模型的安全防护，按照IaaS、PaaS和SaaS的层次结构，系统需要确定哪些安全控制是必须的，哪些安全控制是系统缺失的，最终实现从云服务模式到云服务安全控制的映射。其安全控制涉及12个关键焦点领域，即治理和企业风险、法规、遵从和审计、信息生命周期管理、可移植性和互用性、传统安全风险、数据中心营运、事件响应、应用安全、加密和密钥管理、身份和访问管理以及虚拟安全[7]。

Gartner在“云计算风险评估”报告中指出，云计算的七大安全风险包括：特权用户准入风险、法律遵从、数据位置、数据隔离、数据恢复、审计支持和数据长期生存性[2]。

IBM从商业的角度，描述商业资源需要考虑的安全风险，从而提出IBM云安全架构，IBM以此为基础提供云安全的专业服务、管理服务和软硬件服务。其涉及的安全风险包括5个方面，即物理设施、网络、流程应用、数据信息和身份识别[8]。

VMware云计算安全架构主要考虑来自虚拟数据中心的安全风险，涉及虚拟环境下的主机、节点、数据、网络、应用等各层次带来的安全风险[9]。

ENISA(欧洲网络与信息安全署)提出一个采用ISO27000系列标准的云计算信息安全保障体系框架，主要涉及的安全风险包括：隐私安全、身份和访问管理、环境安全、法规和物理安全等[10]。

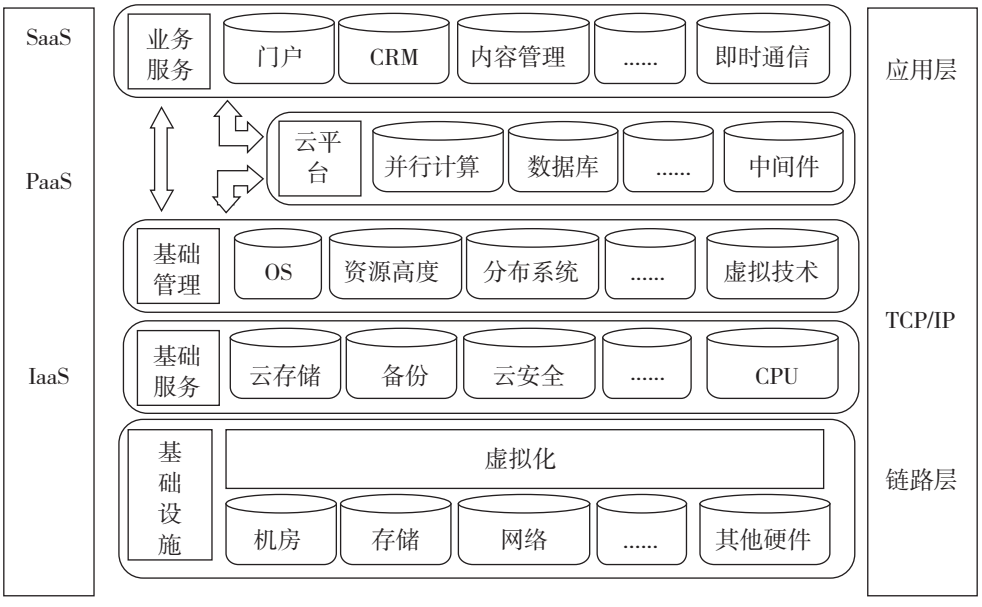

图1　云共享服务模式

另外，信息技术基础设施库（ITIL）、国家标准与技术研究院（NIST）等国际组织以及许多其他标准机构组织专注于自己国家的需求，提出了不同的云服务安全风险，以完善安全控制和架构[5]。

3　面对云计算新安全风险的对策

通过以上分析可知，不同组织提出的云计算安全框架所揭示的安全风险侧重点不同，其中包含传统的IT风险，如物理安全、应用安全、网络攻击，也包含云计算带来的新型的或传统风险中忽略的而在云计算中被放大的风险。笔者通过研究云服务模式（图1），分析其各个层次可能带来的安全风险，并借鉴各安全框架所揭示的安全风险，通过SaaS、PaaS和IaaS这3个层面来研究云计算中新的值得关注的安全风险及其对策。

3.1　SaaS风险及对策

3.1.1　审计和法规遵从风险

传统的服务提供商受到外部审计和安全认证的约束，云服务商拒绝这种外部审查暗示着用户只能接受服务商制定的规则[7]。尽管是服务商为云服务的安全性提供支持，但最终是用户自身对数据的安全负责，这就意味着第三方审计工作尤为重要。用户数据可能位于同一位置，亦会在不断变化的主机和数据中心组之间传播，因此，如果不能获得服务商的支持，外部审计将是很难进行的。而外部审计工作又是保证云服务商满足各种法规遵从的重要手段，服务商只有满足合规性要求才能根本保障各级云计算服务的安全问题，所以审计和法规遵从风险是云服务安全风险不可忽略的重要部分。其应对策略可以从以下几个方面来考虑：法规团队，分析法规遵从范围，审计人员的资格与选择，服务商法规遵从，提供法规遵从证据，审计工作原则。审计工作原则尤为重要，审计工作需要涉及大量的用户数据，并且为平台的安全性提供第三方保障，因此，一方面，审计工作要坚持保密原则，即保障用户数据的隐私性，遵守职业操守，坚守法律制度，避免在审计过程中泄露用户信息；另一方面，审计机构应该秉承公开、公正的原则，使审计工作透明化，起到监督服务商和为用户提供指导的作用。

3.1.2　信息隐私

不同于传统的计算模型，云计算利用虚拟计算技术，用户的个人信息可能分散在不同的虚拟数据中心，甚至跨越国界，而不是留在相同的物理位置[11]，在这个时候，云数据一旦被用户上传到云服务器上，就丧失了对其的控制权[12]，变成对云服务商绝对透明的数据，难以防止云服务商对这些数据信息的泄露、利用等，如挖掘用户信息实现其盈利目的等；同时在开放云环境中很难控制特权制访问人员的数据泄露风险[2]。云计算的这种服务模式对用户的信息隐私造成极大的风险[13]。解决数据隐私风险的对策主要有IAM(身份和访问管理)和隐私保护系统。

（1）IAM，是最主要的应对策略，主要涉及用户身份建立和注销、认证、联合身份管理以及授权和用户档案管理[7]。例如，通过SAML（安全断言标记语言）实现SSO（单点登录）功能，可以完成对云用户的安全集成管理和访问控制，如图2所示。

SSO实现云平台多应用程序的用户集成管理，通过持续动态地维护用户信息中心，确保用户身份的真实可靠；SAML又可以确保管理系统中不同安全域（服务提供商和身份提供商）交换认证和授权数据过程中的安全通信，其中服务提供商可以是Google Apps、Azure、Amazon EC2等云服务平台，身份提供商可以是统一的用户档案数据中心。从图2可知，用户发出登录请求，经过8步，才能通过认证许可，从而获得登录权限，实现对用户的身份认

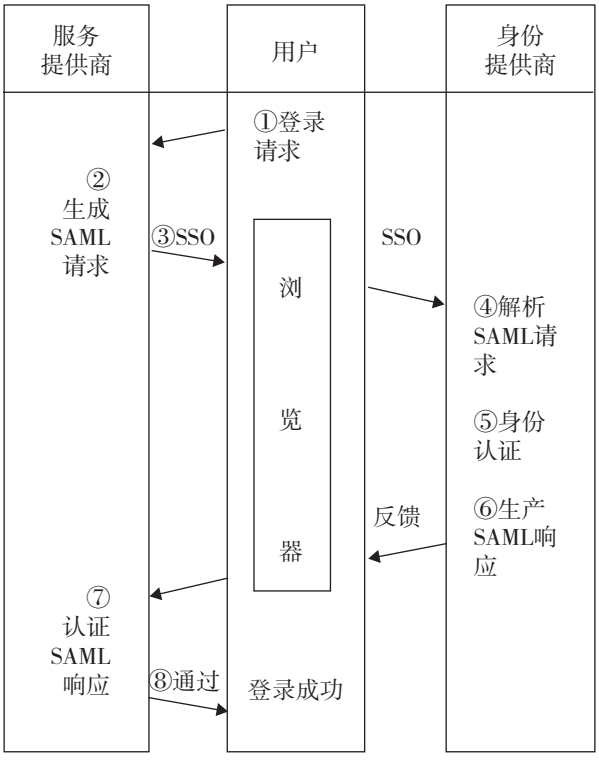

图2　SAML交互步骤

证和访问控制。

另外，为了防止用户非正常登录，系统还应该记录下“是谁登录”、“何时登录”，“从何地登录”、“执行了什么活动”、“访问了什么数据”等用户历史行为[14]，不仅可以方便用户账户管理，还可以实现用户的自助服务，确保身份的真实性。

Google Apps、Office live和Salesforce在用户登录方面的控制信息比较，如表1所示。

表1　平台登录信息对比

	登录事件	源IP	操作事件	读取数据项	数据修改内容	SSO
Google Apps	无	有	无	无	无	有
Office live	无	无	有	有	无	无
Salesforce	有	有	有	无	无	有

由表1可知，Salesforce对用户身份控制最为详尽，可以实现身份认证、访问控制，但没有对数据修改内容的记录，不利于数据因非法修改而带来的修复问题；Office live还没有实现平台用户的集成管理；Google Apps、Office live不记录“登录事件”，只能读取成功登录用户的信息，而不记录失败登录信息，这样不利于对非法登录的管理。

可见，目前，云平台IAM方面还有不完善的地方，云服务商应根据以上内容完善IAM,从入口保护信息隐私。云计算安全公司Symplified的代表产品“SinglePoint”，在IAM实现了包括身份认证、注销用户帐户、按需分配用户访问权限、管理用户身份等方面的功能，具有较好的借鉴意义。

（2）隐私保护系统是保证用户信息隐私权利的系统，例如可以协助用户控制存储在云端敏感信息的使用的隐私管理工具[15]、可用于防止非授权信息泄露的隐私保护系统[16]。

3.2　PaaS风险及对策

云服务是基于互联网而发展起来的一项服务，不可避免地要承受来自互联网的一系列攻击，比如网络病毒、木马、账户盗用等。其在PaaS应用上体现的尤为明显。PaaS是跨站点交互型应用，并需要大量存取存储在云端的数据。这种服务模式给传统IT不流行或危害较小的攻击方式带来了新的发展空间，如CSRF、SQL注入。笔者以SQL注入为例,论述其在PaaS上的风险及对策。

SQL注入攻击有读取和插入数据库信息的能力[17],通过把SQL命令插入到PaaS页面递交或输入域名或页面请求的查询字符串中，实现欺骗服务器执行恶意SQL命令，会对云存储造成极大的危害。

假如在浏览器中输入代码1，则只是对页面的简单请求而不需读取数据库；代码2则在URL中传递变量“id”，于是就向数据库发出了动态请求，等同于向数据库执行了代码3。

```
代码 1：http://localhost:8080/users/Default.jsp
代码 2：http://localhost:8080/users/default.jsp?id='1'
代码 3：select*  from users where id='1'
```

基于以上原理，SQL注入可以通过以下方式对云存储造成恶意攻击。

（1）简单查询。在where子句恒真的情况下，攻击者可以通过SQL注入查询数据库所有信息，这很容易实现。因为“1=1”恒真，所以可以通过代码4实现代码5对数据库的查询，从而获得所有用户信息。

```
代码 4：http://localhost:8080/users/Default.jsp?id
        ='1'or'1'='1'
代码 5：select*  from users
```

（2）利用错误查询获取数据信息。通过插入恶意SQL代码，有些服务器不关闭报错信息，攻击者就可以从报错信息获得有价值的信息。执行代码6可以获得错误信息1，由此攻击者可知，服务商使用的后台数据库是SQL sever。执行代码7可以获得错误信息2。由此攻击者可知，服务商存储的后台数据中有一个名为“enwikibackup”的数据库。

```
代码 6：http://localhost:8080/users/Default.jsp?id=
        '1'or'1'=(select count(*) from usersd)
代码 7：http://localhost:8080/users/Default.jsp?id=
        '1'or'1'=(select count(*)
        from master.dbo.sysdatabases
        where Uname>1 and dbid=6)
```

```
错误信息 1：System.Data.Sqlclient.SqlException:
        对象名“usersd”无效
错误信息 2：在将nvarchar值'enwikibackup'转换
        成数据类型int时失败。
```

（3）捎带查询。攻击者可以将恶意SQL语句放到正常的SQL语句之后，服务器接受正常语句之后，也会捎带执行恶意语句。代码8执行的恶果是删除数据表“users”。

代码 8：http://localhost:8080/users/Default.jsp?
id='1';drop table users--‘

其他，例如可以利用存储过程、Union查询、获取Web虚拟目录等手段获取存储端信息，最终可对服务器造成重大损失。

其应对措施可以是：（1）对传递的用户信息校验，如限制长度、对引号转换。通过代码9可实现对传递语句的校验，例如对恶意代码1的校验结果为错误信息3，并重新定位到“error.jsp”,从而防止了恶意攻击；（2）数据加密存储；（3）用自定义的错误信息包装系统错误信息；（4）为每个访问连接设置访问权限。

错误信息 3：请正确输入

代码 9：

```
public static int SQLinj(String Sqlstring)
//读取传递的SQL语句
  {//使用正则表达式匹配结果
   Pattem p1=Pattem.compile("(\s?or\s*|\s?;\s?|
   \s?drop\s|\s?grant\s|^'|\s?--|\s?union\s|\s?delete\s|
   \s?truncate\s|\s?sysobjects\s?|\s?xp_.*?|
   \s?syslogins\s?|\s?sysremote\s?|\s?sysusers\s?|
   \s?sysxlogins\s?|\s?sysdatabases\s?|
   \s?aspnet_.*?|\s?exec\s?)");
   Matcher m1=p1.matcher(Sqlstring);
   int Mg=0;
   if(ml.find()) Mg=1;
   retum Mg.
   }
   ……
   ……
   public static void detect.SQL(String Sqlstring)
   {
     If(SQLingj(Sqlstring))
   {
    System.out.println("请正确输入");
    response.sendRedirect(“error.jsp”);
   }
     else
         response.sendRedirect(“correct.jsp”);
```

3.3 IaaS风险及对策

3.3.1 虚拟安全

虚拟技术是实现云计算共享服务的关键核心技术之一，因此虚拟安全也是云服务安全最关注的风险之一。云计算服务为了充分利用世界网络资源，将服务器、存储设备等分布在世界各地的资源通过抽象有效地整合起来。例如：一台物理服务器可以虚拟成多个服务器，多个存储设备可以虚拟成一个存储设备，由此而带来的隔离风险、通信漏洞等就是虚拟安全。为建立一个安全的执行环境，虚拟安全的相关工作可分为安全隔离、完整性测量和监测[18]3类。

（1）安全隔离。在近些年的虚拟化技术发展中，虚拟机已经从先前的物理环境隔离，发展到动态业务逻辑隔离。Reiner Sailer等人在IBM的一个研究报告中提出了全方位隔离管理程序sHype。这个架构能够对虚拟机之间的信息流进行监控和控制，实现信息安全隔离[19]。在网格技术环境下，Sriya从虚拟技术的发展中提出了逻辑隔离模型[20]。RajH通过缓存划分的页染色方法,和缓存层次可感知的核心分配方法实现安全隔离模型[21]。在云计算安全领域，虚拟主机监测系统VMM的系列产品“VMware vShield”能够实现不同信任级别应用程序的隔离，并把敏感区域的数据进行分类[8]。

（2）完整性测量。虚拟技术是通过一系列虚拟软件来实现的，而系统不可靠的基本原因之一是由恶意软件或代码造成的系统完整性破坏。因此，确保软件来源于可信方是保证系统内在安全的一个有效方法。完整性测量可以有效地证明供应商和来源是可靠的和负责任的，也就是意味着软件文件没有被损坏或篡改[18]。Reiner Sailer等人提出了Linux系统的完整性测量模型，这个模型把完整性测量扩展到动态的可执行文件内容中，这样就可以检测到数据的不良调用信息[22]。

（3）监测技术是保持虚拟系统健康运行的另一种重要途径。Bradley Wheeler等人对云计算监测技术和管理系统进行了详细的描述，认为云计算监控应该对事件系统的每一个细节进行追踪和监控管理.为此，他们提出了云计算监控系统的改进方案[23]。Benjamin König等人则提出了云基础设施的弹性监测架构，这个架构可以跨层对所有网络系统进行快速监测，并提供详细的监测信息和统计结果，方便对云计算系统进行改进[24]。

3.3.2　数据安全

云计算数据存储服务是以分布式网络、伸缩性存储、虚拟化技术为基础的，数据可能存储在网络上任何一个节点，其数据存储位置不确定、存储边界模糊、数据共享存储[2]等特点给数据安全带来新的不稳定因素，主要涉及数据隔离、数据恢复、数据消除、数据传输、存储边界等风险。其解决对策主要包括以下几个方面。

（1）数据加密。存储在第三方平台上的数据在存储设备上以及传输过程中都变得透明化，只有经过加密处理才能保证基本的数据安全。基本的加密算法有对称加密和非对称加密算法；云数据加密方式主要有存储加密、传输加密、检索加密、密文检索、密文访问等。在数据加密方面，已经取得了比较成熟的研究成果。例如，Kevin提出分布式加密算法以确保数据的完整性[25]。Song D等提出基于密文全文扫描的密文检索方法，匹配密文中每个词语，确认关键词是否存在,然后再统计其出现的频次[26]。云计算安全公司Navajo系统的代表产品“虚拟专用SaaS(VPS)”，可以将存储在云平台和传输过程中的数据加密，保证用户数据安全，而数据返回给用户时会自动解密。

（2）数据隔离。数据加密虽然可以防止数据盗取，但有时加密会意外导致数据无法使用，并且加密算法一般过于复杂[2]，而数据隔离操作相对简单，并且还可以防止多租户共享模式带来的数据盗取、非授权访问等风险。数据隔离一方面可以采取类似上文提到的安全隔离技术，另一方面也要避免将敏感数据存放到公共云上，因为公共云暴露在公开的平台之上，很容易带来数据安全风险。

（3）冗余存储。云存储的分布式和虚拟化模式可能将数据存储在世界的任何一个设备上，数据丢失不可避免，如灾害、硬件问题、病毒入侵等带来的问题，因此，适当采用冗余技术可以有效防止数据损坏、丢失等问题。数据管理中心可以定期将云数据自动备份，并自动识别丢失或损坏的数据，根据数据索引和冗余备份，再在其他设备上恢复数据。另外，当一个设备因其中一个用户出现违规活动，需要安全审查而暂停服务时，其他用户也可读取存放在其他设备上的冗余数据而免受牵连。

（4）数据生命周期管理。信息安全的主要目标之一是保护系统和应用程序的基本数据安全，但在过渡到云计算的过程中，弹性、多租户、新的物理和逻辑架构等现象给传统数据安全策略带来了挑战。据此，数据生命周期管理方法可以比较完善地对云数据进行跟踪管理[7]。从数据的产生到消亡，数据的生命周期包括：数据生成、数据存储、数据使用、数据共享、数据档案管理和数据消亡。数据生命周期管理基于各阶段，层层保证数据的保密性、完整性、可用性、真实性、授权、认证和不可否认性，从而确保云数据整个生命周期的安全性。

4　不同应用领域下的对策建议

根据应用背景，云计算平台的应用领域大致可以分为3个层面：商业领域、非商业公共领域和国家战略领域。例如，电子商务、企业档案管理服务、企业创新科技等属于商业领域；教育等属于非商业公共领域；军工科技等属于国家战略领域。

不同应用领域根据自身需要会采取不同的部署模式。根据各个部署模式的性质，可知其安全性从高到低依次为私有云、社区云、公共云。私有云是独占模式，不存在多个用户之间的共享，可以根据用户自身需求构建，并可以仅在内部局域网内转播，面临的网络风险较小，因此，私有云中注重的安全策略为IAM以实现用户管理，安全隔离以实现用户自身不同安全级别数据的逻辑隔离，完整性测量以避免外部软件的威胁、冗余存储和数据生命周期管理。相较于私有云，社区云增加的最大风险来源于互联网，因此互联网防御、敏感数据的加密传输显得尤为重要。而公共云一般是接受第三方提供的服务，面临的安全风险最大，需要采取全面的风险对策。

各个领域采用的部署模式不同，安全需求不同，所关注的风险对策也不同。通过分析云计算的服务部署模式及其风险特征，笔者认为不同应用领域应该采用的模式和重点关注的风险对策，如表2所示。

商业领域中，私有云适合企业内部的技术支持等，社区云适合企业间的合作发展，公共云适合企业面向大众顾客的服务，因此，商业领域采用较多的模式是混合云，需要全面关注云风险。非商业公共领域一般是教育、图书馆等面向局部服务，采用的是私有云和社区云结合的混合云，需要关注解决私有云和社区云中风险的对策。国家战略领域安全性要求高，目前不适合风险较大的云计算平台，即使有必要，也只能采用安全性相对较高的私有云。

表2 风险应对建议表

		商业	非商业公共	国家战略
部署模式	公共云	√		
	私有云	√	√	√
	社区云	√	√	
	混合云	√	√	
风险对策	审计、法规遵从	√		
	IAM	√	√	√
	隐私保护	√		
	互联网防御	√	√	
	安全隔离	√	√	√
	完整性测量	√	√	√
	监测	√		
	数据加密	√	√	
	数据隔离	√	√	
	冗余存储	√	√	√
	数据生命周期	√	√	√

在这种情况下，只需要关注私有云的安全对策。

5 总结

目前，仍有大量企业因为考虑到云服务安全问题而没有使用或深入体验云服务，并且随着云计算技术的快速发展，云计算的应用也越来越广泛，随之而来也必然会出现越来越多的云服务安全问题，因此，云环境下共享服务的安全风险问题必将成为云计算领域最值得关注的话题之一。本文只是对云服务安全风险进行了简单探讨，难免有不全面之处，还有待更深入全面的研究。

参考文献

[1] Schweitzer J E. Reconciliation of the Cloud Computing Model with US Federal Electronic Health Record Regula−tions[J]. J Am Med Inform Assoc, 2012(19):161−165.

[2] Brodkin J. Gartner: Seven Cloud−computing Security Risks. Info World Security Central News[EB/OL]. [2012−03−01]. http://www.idi.ntnu.no/emner/tdt60/papers/Cloud Computing Security Risk.pdf.

[3] Stuart K, Bromage D. Current State of Play: Records Management and the Cloud [J]. Records Management Journal, 2010,20(2):217−225.

[4] Michael A. Above the Clouds: A Berkeley View of Cloud Computing [EB/OL]. [2012−03−01]. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS−2009−28.pdf.

[5] Loganayagi B. Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques[J]. Procedia Engineering, 2012,30:654−661.

[6] Peter M, Timothy G. The NIST Definition of Cloud Computing[EB/OL]. [2013−03−10]. http://csrc.nist.gov/publications/nistpubs/800−145/SP800−145.pdf.

[7] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1[EB/OL]. [2012−04−27]. http://cloudsecurityalliance.org/csaguide.pdf.

[8] Axel B, Koos L, Harold M. et al. Cloud Security Guidance−IBM Recommendations for the Implementation of Cloud Security[EB/OL]. [2012−04−27]. http://www.redbooks.ibm.com/abstracts/redp4614.html.

[9] VMWARE. Gain Trust in Your Cloud with VMware Shield[EB/OL]. [2012−04−27]. http://www.vmware.com/products/vshield/overview.html.

[10] Daniele C. Cloud Computing: Benefits, Risks and Recommendations for Information Security[EB/OL]. [2012−03−21]. http://www.enisa.europa.eu/.

[11] Jianfeng Y, Zhibin C. Cloud Computing Research and Security Issues[C]. Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on Date of Conference. Wuhan:ieee, 2010: 1−3.

[12] Chow R, Golle P, Jakobsson M, et al. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control[C]//Proc. of the 2009 ACM Workshop on Cloud Computing Security. New York: ACM, 2009: 85−90.

[13] Kaufman L. Data Security in the World of Cloud Computing[J]. IEEE Security and Privacy, 2009,7(4): 61−64.

[14] Andrew B, Alex S, Nathan W. Cloud Computing Security[EB/OL]. [2012−04−27]. https://www.isecpartners.com.

[15] Bowers K D, Juels A, Oprea A. Proofs of Retrievability: Theory and Implementation[C]//Proc. of the 2009 ACM Workshop on Cloud Computing Security. New York: Association for Computing Machinery, 2009: 43−54.

[16] Roy I, Ramadan H, Setty S, et al. Airavat: Security and privacy for MapReduce[C]//Proc. of the 7th Usenix Symp. on Networked Systems Design and Implementation. San Jose: USENIX Association, 2010: 297−312.

[17] Inyong L, Soonki J, Sangsoo Y, et al. A Novel Method for SQL Injection Attack Detection Based on Removing

（下转第104页）

要性及面临的政策法规及技术等问题要达成一致的认识，成立平台构建小组，成员主要由各院所图书馆数字资源、参考咨询等工作人员组成，负责平台的技术攻关、信息维护、推广等工作。

其次，平台的构建与平稳运行需要农民用户的广泛参与。随着信息技术的发展，农民获取、交流和处理信息的手段发生了巨大变化，PC与手机逐渐成为农民获取农业科技信息的重要途径。构建农业类的云服务平台，对于农民来说，可以实时从平台上获取第一手的科技信息。而农民用户广泛使用平台，进行在线咨询更是平台价值的体现。

总之，构建基于云计算的高交互性的农业科技OA平台，不仅可以整合青岛地区农业科研院所的资源，而且能为这些农业科研院所以及青岛市基层科技推广人员和农民提供科技信息。农业OA平台的构建具有实践创新意义。当然，平台的构建既需要地方政府的重视和支持，也需要农民用户的广泛参与。本文希望通过对区域农业OA平台构建的研究能够为青岛地区农业的发展提供一定的参考和借鉴。

参考文献

[1] 陈静,孙继林.开放获取期刊平台发展现状评析[J].图书馆杂志,2012(4):24−28.

[2] 李云祥,陆宇明,温国泉,等.略论我国农业开放存取期刊发展策略[J].广西农业科学,2010,41 (4):400−402.

[3] 李会萍,梁伟文,李泽,等.基于开放式访问的农业科技文献公共服务平台建设初探[J].农业网络信息,2009(1):16−19.

[4] 王洪蕾.中国农业科学院机构仓储框架设计与资源建设研究[D].北京:中国农业科学院,2011.

[5] 毛广卫.基于DSpace的中国农科院机构仓储系统的研究与实现[D].北京:中国农业科学院,2011.

[6] 冯文兰.农业特色开放获取文献资源建设[J].中国科技信息,2011(1):106−107.

[7] 李云祥,韦志扬,甘立,等.广西公共传媒农村信息服务现状及发展策略[J].南方农业学报, 2011,42(2):229−232.

[8] 李会萍,韩威威,李泽,等.德庆县柑桔专业镇科技创新服务平台建设[J].农业网络信息,2010(11):48−50.

[9] 孙岩,马中杰.成长型农业科技期刊开放存取系统建设研究[J].农业图书情报学刊,2010(8):26−28.

[10] 沈波,夏爱红,周广礼,等.《南京农业大学学报》实现Open Access的实践[J].中国科技期刊研究,2008,19(6):1018−1021.

[11] 胡新平,沈洪妹,张志美.区域云数字图书馆构建研究[J].情报理论与实践,2011(2):77−84.

（上接第99页）

SQL Query Attribute Values[J]. Mathematical and Computer Modelling, 2012,55:58−68.

[18] Jianxin L, Bo L, Tianyu W, et al. Cyber Guarder: A Virtualization Security Assurance Architecture for Green Cloud Computing[J]. Future Generation Computer Systems, 2012,28:379−390.

[19] Reiner S, Enriquillo V, Trent J, et al. sHype: Secure Hypervisor Approach to Trusted Virtualized Systems[EB/OL]. [2012−04−27]. http://domino.watson.ibm.com/library/CyberDig.nsf/papers/265C8E3A6F95CA8D85256FA1005CBF0F/$File/rc23511.pdf.

[20] Sriya S, Pradheep E, Andrea A, et al. Deploying Virtual Machines as Sandboxes for the Grid[EB/OL]. [2012−03−21]. http://research.cs.wisc.edu/condor/doc/SandboxingWorlds053.pdf.

[21] Raj H, Nathuji R, Singh A, et al. Resource Management For Isolation Enhanced Cloud Services[C]//Proc. of the 2009 ACM Workshop on Cloud Computing Security.New York: Association for Computing Machinery, 2009:77−84.

[22] Reiner S, Xiaolan Z, Trent J, et al. Design and Implementation of a TCG−Based Integrity Measurement Architecture[EB/OL]. [2012−04−27]. http://static.usenix.org/events/sec04/tech/full_papers/sailer/sailer.pdf.

[23] Bradley W, Bryan G. Cloud Computing Monitoring and Management System[EB/OL]. [2012−04−27]. http://patentscope.wipo.int/search/en/WO2011071624.

[24] Benjamin K, Jose M.Alcaraz C, et al. Elastic Monitoring Framework for Cloud Infrastructures[EB/OL]. [2012−04−27]. http://jmalcaraz.com/wp−content/uploads/papers/AlcarazCalero−IETCom−Preprint.pdf.

[25] Kevin D B, Ari J, Alina O.HAIL: A High−Availability and Integrity Layer for Cloud Storage[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009:489−501.

[26] Song D, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]//Proc. of the IEEE Computer Society Symp. on Research in Security and Privacy. Piscataway: IEEE, 2000:44−55.