互联网时代云计算数据的安全研究

高红军

（辽宁广播电视大学丹东分校　辽宁　丹东　118000）

[摘　要]互联网时代云计算技术因其强大的数据存储和计算功能而成为信息技术发展的方向，但是同时也出现了网络信息安全问题，严重威胁着数据的安全。本文重点介绍互联网时代云计算数据安全保护机制，分析并提出了在当前技术环境下对数据安全的威胁，加强保护数据安全并确立有效机制和相关措施，为信息应用提供更可靠，更高效的环境，以供参考。

[关键词]互联网时代；云计算；数据安全；保护

【DOI】10.12252/j.issn.2096-6288.2021.06.561

前 言

互联网时代云计算是近年来的热门技术，技术特点是可以存储和计算大量的结构化和非结构化数据，是有效利用计算资源并使人们能够动态获取资源的重大创新。为了更好地利用互联网时代云计算的优势，并提供高度可靠和稳定的计算和存储服务，确保信息安全至关重要。

1.互联网时代云计算数据安全保护的需求

在互联网时代云计算环境下，加强数据安全保护是开发新技术应用的基础要求。随着越来越多的网络应用加强云计算数据的运用，因此如何提供一个更加稳定可靠、安全可信的网络环境极为关键，这也是一些对于用户隐私要求较高的网络应用不愿意向云平台迁移的原因，也在一定程度上制约了技术的发展。因此，建立一个全面的保护机制非常重要。所谓保护机制，是指通过有效实施法律、技术、信息安全产业和人员培养而实施的信息安全机制。在高科技平台上提高信息安全性非常重要，该保护机制是在新技术环境中采取措施保护数据安全的过程，并为用户提供可靠的技术平台提供坚实的基础。

1.1滥用引起的服务攻击会构成数据安全威胁

强大的云计算检测技术，如服务功能、虚拟补丁功能、技术手册功能、安全性能监视功能等已引起了大量的滥用，导致了欺诈和其他非法行为，例如窃取密码、僵尸网络等，严重威胁数据安全，侵犯人们的切身利益，并带来安全风险。

1.2接口不安全很容易泄漏信息

云安全检测技术仍然存在在访问点和接口上无法忽略的安全问题，并且云计算技术正在开发和研究中，尚未充分开发，这增加了入侵不安全因素的可能性。因此，需要不断地构建具有更高安全性的访问点和接口，探索更高效，更安全的接口和访问点管理实践，并确保云身份验证、审核、访问和计费的所有细节都安全地运行。

1.3数据泄漏是最常见的云计算数据安全问题

云计算包含大量的高密度信息，这些信息可以穿透数据信息并获得利益。在这种环境中，具有高数据密度的数据和信息特别容易丢失和泄漏，从而为攻击者提供了机会。因此，所有云服务提供商都应努力控制数据和信息的安全性。

1.4存在未知风险

在云安全监控技术的框架内，数据和信息是不对称的，云计算用户无法对云服务的所有功能有全面、多层的了解，从而对数据安全造成隐患，并无意间泄漏了有关数据的信息，我们将此称为未知风险。

1.5操作错误

众所周知，云服务是外包业务。近年来，用户的数量和圈子越来越广泛。用户包括云服务提供商、管理人员、服务人员等，不可避免地会发生操作错误，并且由于人员疏忽而不可避免地会产生数据安全风险。

2.互联网时代云计算数据安全面临的挑战

2.1网络硬件的风险

网络硬件设备的风险也是威胁信息供电网络安全的重要因素之一。一方面，磁盘和硬盘是用于存储信息的重要介质，但是磁盘和硬盘的制造商很多，质量也参差不齐，如果无法保证磁盘和硬盘的质量，则存储的信息可能会丢失。因此，不能保证网络信息的完整性。另一方面，存储介质也会受到外部环境或人为因素的影响。例如，在雷雨期间或在电磁辐射强度高的环境中，由于电磁波的影响，存储的信息会丢失或存储介质可能损坏。人为因素是由于人为错误导致信息丢失而引起的设备故障。

2.2恶意黑客攻击

互联网技术在日常生活中的广泛使用带来了许多便利，但也为黑客的恶意攻击创造了条件。黑客行为会对系统的正常运行造成严重影响，其出于各种目的攻击和破坏网络系统，例如修改、删除和窃取目标信息。这不仅严重破坏了正常的网络秩序，甚至可能导致严重的信息丢失或信息泄漏，从而影响信息网络安全。

2.3系统漏洞

系统漏洞是指硬件，软件和通信协议或系统安全策略的缺陷。这使黑客可以利用安全漏洞进入系统而并获取访问权限，损坏系统或窃取信息。当前，世界上使用最广泛的操作系统是Microsoft操作系统。虽然，微软不断发现漏洞并提供补丁以修复漏洞，但是漏洞依然不断出现。而且补丁中也可能带入新的安全漏洞。因此，在不断发现和解决旧的安全漏洞的同时，新的漏洞不断出现。因此，为了确保信息网络的安全性，有必要根据实际情况（例如操作系统的版本和服务的参数）寻找解决方案。

2.4病毒和特洛伊木马的入侵

特洛伊木马和病毒是使用特定程序对另一台计算机的控制。由于大多数人对信息安全的了解不足，并且安全系统中存在漏洞，因此为特洛伊木马和病毒的传播创造了条件。一些木马还假装诱使用户下载并执行它们。在被特洛伊木马和病毒感染后，特洛伊木马和病毒会破坏或窃取各种文件，甚至犯罪分

子会特洛伊木马和病毒来控制系统。因此，安装有效的防病毒软件并及时更新病毒数据库尤为重要。

3.互联网时代云计算数据安全的关键点

云计算的飞速发展具有巨大的瓶颈，即云计算的安全性。在与云计算相关的挑战中，数据安全性和隐私一直是用户关注的焦点，并且也是普及云计算技术的最大障碍。在云计算中，用户将数据存储在云中，因此他们不再完全控制其数据，并且用户数据的安全性完全不受数据所有者的控制，这要求云服务提供商的CSP提供有效的安全保证。与传统计算相比，云计算的核心特征，如按需服务、公用事业账单、共享的网络计算和存储池、快速灵活的部署以及无处不在的网络访问已导致了云计算的安全性问题，因此安全和隐私保护尤其重要。

3.1互联网时代云计算数据安全关键研究点

用户数据有两种形式：静态存储、动态传输。在静态存储中为了确保容错能力，可以将用户数据复制到多个副本中。在动态存储中，可以存在于诸如内存，网络或磁盘缓冲区之类的介质上。因此，可以创建用户数据并将其上传到云服务器，以完全消灭称为数据的整个生命周期，从而对整个数据生命周期进行数据安全管理。在云计算环境中，对数据安全性和隐私保护的威胁可能来自多种来源，主要来自两个方面，即外部威胁和内部威胁。外部威胁通过云服务器提供给用户的界面与内部云系统进行交互，并利用软件和硬件中的漏洞进行入侵；内部威胁包括意外的操作错误，恶意的内部员工以及系统上的软件和硬件，云基础架构错误和可重用性，对租户环境等的直接或间接攻击，这些攻击会泄漏或破坏用户数据和隐私，并对用户造成不可估量的损失。尽管数据加密是在云计算环境中保护数据的主要手段，并且可以有效地防止未经授权的传输，但它也带来了难以快速检索文档并以密文状态进行搜索的问题。此外，必须在云中解密机密用户数据才能参与计算。因此，存在机密数据泄漏的风险。

（1）密文搜索：接收密文是实现信息共享的重要工具，这是加密存储中需要解决的问题之一。目前，密文搜索方法主要集中在两个方面：一是等效匹配搜索，主要是线性搜索算法；第二种是密文区间搜索，主要包括区间搜索和顺序保留加密算法，实现了数字数据的加密和保护。

（2）完整性检查和所有证明：在云计算环境中，完整性检查主要方法是在加载数据并将其存储在本地可靠存储中时，使用哈希函数来计算数据的哈希值。但是，如果每次都将所有数据下载到本地计算机以检查完整性，则不仅效率低下，而且会消耗宝贵的网络带宽。为此，研究人员提出了所有证明，即CSP可以向用户证明它仍然保持用户数据的良好状态，并且可以在不提供完整数据的情况下检索数据。数据所有权证明是为了验证不受信任的存储服务器是否正确存储数据，并防止存储提供程序删除或修改数据。

（3）隐私保护和隐私请求：云计算中的隐私问题越来越受到关注。研究人员最近对隐私问题进行了研究，例如云计算中的数据发布和数据挖掘，提出了在云计算中寻找有关保护隐私的信息的问题。

3.2全同态加密

全同态加密为云计算中的数据安全性和隐私保护提供了新的机会，主要解决了将数据及其操作传输给第三方时的机密性问题。全同态加密的目标是找到一种加密算法，该算法可以对加密数据执行任意数量的加法和乘法运算，以使对加密数据进行某些运算的结果与加密前的预期数据完全相同。云安全检测技术基于文件，电子邮件和Web信誉评分数据库以及Security Gateway的结合，以实现全自动和完全智能的保护。所有数据都托管在多台服务器上，以确保最大的数据安全性。它的应用范围包括人们日常生活的各个方面，并且在通信、IT行业、大型运营商和政府的支持下，已经得到了大多数用户的认可和接受，具有广阔的发展前景，并且发展趋势相对较好。然而，云计算中的数据安全性仍然不可忽视，因此，对云计算中的数据安全性的研究具有现实意义。全同态加密主要用于云计算环境的以下方面：

（1）数据处理和隐私保护。在云计算环境中，用户使用全同态加密技术以加密形式将存储在云服务器上的数据发送到云服务器，其他用户可以在不知道原始用户数据的情况下直接处理密文数据。随后，用户可以从云服务器接收数据处理的结果，并对其进行同态解密，以便以纯文本形式获得处理后的数据。

（2）密文搜索。传统的加密技术不支持密文提取，而全同态加密技术密文提取方法是基于完全同源性的。在不改变对应的明文的情况下，对提取的数据进行加法和乘法，可以有效保证查询隐私和提高检索效率。

3.3.1互联网时代云计算数据安全保护措施

互联网时代云计算的迅速发展带来了许多新的安全威胁，数据安全面临许多新挑战，迫切需要进行安全保护管理。以下提出几项措施，以应对当前的威胁。

3.3.2建立和完善保护数据的法律制度

加快通过有关数据保护的法律法规，进一步规范政府、企业和有关机构对数据的收集、存储和使用，并依法惩处违反信息安全的行为，以确保信息安全。同时，进一步完善信息安全领域的现行法律法规，完善辅助手段，提高执法机关的效率，严格惩罚数据保护领域的违法行为，增加违法成本并确保逐步建立的数据的安全机制，完善保护数据的法律制度。

结束语

在互联网时代云计算环境下，数据安全受到严峻的威胁，人们对数据安全也越来越关注。本文分析了在互联网时代云计算环境下五个方面的威胁，和保护数据方面当前面临的挑战和原因，最后针对性的提出了应对措施，以更好地保护互联网时代云计算数据的安全。

参考文献

[1]何薇，钱罕林.大数据时代云计算环境下的数据安全研究[J].信息系统工程，2018（03）：72.

[2]冯庆亮.大数据时代计算机网络信息安全与防护策略研究[J].企业科技与发展，2020（01）：94-95，98.

作者简介:

高红军（1975.03-）女，汉族，黑龙江省讷河县，大学本科，讲师，研究方向：计算机软件开发，网络管理。