云计算网络环境下的信息安全研究

凤春飞*
云南电信公众信息产业有限公司，云南 650000

摘　要：随着经济社会的快速发展，当前我国社会已经逐渐转变为信息化社会，计算机网络技术的逐渐成熟更是推动了信息安全研究的发展。随着云计算技术在社会各界受到广泛关注，关于云计算网络环境下的信息安全研究也越来越全面，针对云计算网络自身的高效性和瞬时性等特点，随着云计算的不断普及，云计算网络环境下的信息安全问题已经逐渐成为影响社会安全的关键问题。为了提高云计算网络的信息安全水平，针对信息安全进行的研究逐渐成为重中之重。

关键词：云计算网络；计算机技术；信息安全；研究

一、引言

随着网络时代的发展，云计算的发展也可以称得上是稳步前进，而且与网络之间的联系也更加的紧密，信息资源在共享上也会显得更加的高效。但是从当前的网络现状来看，信息无可避免会存在各种各样的泄露问题，其中较为典型的是在天猫或者淘宝等购物平台进行消费时账号中的钱往往会悄然地被扣除，特别是在上网的过程当中云端可能会被黑客入侵，自己的秘密被窥探，甚至还会损失一些自身的经济利益。如今这些问题日益凸显，甚至会不断加剧，因此要能够意识到这些问题所存在的严重性，并采取各种各样的措施来保证个人的隐私以及信息的安全。

二、云计算概述

云计算具体来说就是依托于互联网通过大量的依据进行费用支付的一种全新的模式。从性质上来说，它是一种新兴化的资源，能够保证网络访问时具有一定的高效性以及可用性从而更好地实现计算机中各种信息资源的共享。清洗的存储百货软件，服务器等都可以称之为资源，这些资源需要根据用户的实际需求来提供服务，无论是在成本还是时间上都会花费较多，当然云计算服务所提供的不仅仅是计算服务这一功能，此外，云计算还提供存储服务，但是当前云计算的服务大多是为一些私人机构所运用，对于商业机构以及政府来说应用的相对比较少，这就导致云服务也不能很好地运用到商业及政府当中，另外信息不管是对于个人还是国家来说都极为重要，但是只要用户使用云服务，那么这些信息就会全部暴露给云服务提供商，信息的保密度也不能得到很好的保证，为此，在云计算当中的信息安全问题必须受到高度的重视。

三、云计算信息安全出现问题的原因分析

（一）数据隔离能效欠佳

云计算技术出现以后，相关应用领域的人员已经采取数据管理措施，并提高了安全防护手段。但实际应用效果并不理想，无法对大量的数据进行及时识别，特别是危险性较高的IP攻击、漏洞攻击以及DOS攻击等。黑客可以从不同角度进行云平台侵入，其方式是植入伪代码进行数据破译和截获。由于计算数据量较大，系统硬件资源有限，无法对传输数据进行高防伪加密，使传输数据容易被黑客持续性的网络攻击。数据隔离效能欠佳与隔离体系的分布有关，部分用户使用隔离手段时，并未进行外部和内部计算机的合理隔离设置，增加了黑客通过外部计算机侵入内部数据的可能[1]。

（二）数据访问风险增强

手机、电脑等设备的存储空间有限，无法满足人们多元化的信息存储需求，所以用户会将自己的数据存储到云环境中，云环境存储是现代数据存储的一种流行趋势。同时，云环境存储属于开放性的存储模式，任何用户都可以进行相关的数据调用和上传，使数据存在较高的安全隐患。其中，数据访问操作是云环境中使用频率最高的操作，也是数

* **通讯作者：**凤春飞，1984 年 2 月，女，汉，陕西宝鸡人，现任云南电信公众信息产业有限公司部门经理，工程师，本科。研究方向：网络安全，信息安全。

据安全风险的主要因素之一。黑客和不法分子可以通过非法手段进行欺骗访问，或者植入木马、蠕虫病毒，实现对云环境数据的篡改、破坏、截获和盗窃，给用户带来较大的风险和损失[2]。

（三）业务数据安全比较低

随着计算机和通信技术应用的深入，云计算环境下的数据量激增，使得业务数据安全成为关注的重点和难点。云计算环境下的业务处理不仅要保证业务双方隐私安全，还要保证相关数据传输安全，并通过数据的唯一性验证数据的有效。由于业务范围扩大，业务数据的传输时间、传输环节不断延长，黑客可以对业务中的薄弱环节进行入侵，并对业务流程进行实时监控，伺机获得业务中的信息内容。如果业务中的一方信息被截获，那么另一方面的信息被截获的风险将会提高，使整个业务信息受到威胁。

四、基于云计算下的网络信息安全问题解决建议

（一）强化与计算机网络信息的加密处理

网络技术人员要针对网络信息内容不断强化安全加密处理，有效提升用户的数据管理和控制能力。首先，要不断强化网络信息加密处理，针对网络文件采取加密控制方式加以保护，用户也可以通过远程云端控制方式来实现对数据的加密。其次，可以充分利用数据的输入和输出来实现统一控制，通过指令控制的方式来实现数据定向传送，这样就能有效避免出现数据传输混乱的问题。另外，针对加密文件还可以充分利用AES技术来实施二次加密，以此来进一步提升信息的安全等级。做为访问者必须要同时正确输入AES密码以及RSA密码才能进行文件删除、下载、阅读，同时也有效提升信息的安全性。如果磁盘存在异常的情况下实施数据删除操作也容易产生信息泄露问题，针对这种状况需要利用实际值技术以及代替键位值的方式来取代删除操作。最后，针对海量数据保存的状况，为了有效避免在数据存储过程中出现信息数据丢失的问题，可以在虚拟技术应用的同时，将SAN技术的优势充分发挥出来，这样就能显著提升备份效果[3]。

（二）推动运营商信息保障平台的发展

云计算网络作为新生的信息时代生产力，其往往也伴随着严重的互联网竞争，甚至是互联网企业竞争中的重要技术支撑，因此所面临的市场环境也就更为复杂和激烈。而由于市场经济的存在，运营商之间往往都拥有专属于自己的独特的云计算平台，不同云计算平台之间技术手段不同，对于信息安全防护的水平也往往不同，甚至由于不同运营厂商之间的竞争关系，往往无法形成统一的运营平台和维持不同运营商之间的沟通交流。因此，如此分散的信息保障平台往往会导致不同程度上的对于云计算资源的浪费，也无法充分发挥出互联网信息技术的全部效能，最终造成云计算互联网环境的恶化，防护能力也会随之下降。

（三）制定安全策略，解决云计算问题

首先要增强信息安全意识，如果收到不知从哪里来的信息文件或者是电子邮件，一律不要随意打开。对于一些意图不明的程序，也不要随意下载，在对软件进行下载时，要从正规的浏览器进行操作，并且在之后用杀毒软件进行扫描，密码的使用以及设置上，要做到定期更换，以及尽可能保证密码复杂化，以便防止对密码进行破解。在防火墙的选择上要能够做到防入侵和防病毒，这些是最为首要的原则。在保护计算机信息安全方面防火墙是最为有利的保障，它可以将内部和外部的网络进行隔离，避免病毒的侵入。要注重应用自理网络代理服务器，对IP地址进行隐藏，这样就算用户不经意间下载了有关木马病毒程序，也无法获取准确的地址，攻击者无法进行攻击，为此可以设定代理服务器，这是对IP地址进行保护的一种有效的方法，实际上，代理服务器可以说是一种媒介，在外部网络需要对那个网络进行防卫的同时，可以由中介进行转接，如果是不正常的信息只能进行处理。

（四）备份云计算内容，实现服务优化

及时备份云计算信息也是一种比较常见的信息安全手段。在一定特定情形下，通过网络信息的安全备份，能够给予用户更多层级，进而实现信息安全的有效保护。数据是云服务迅速发展的依据，数据产生不安全问题，也必将会对云计算的发展产生影响。云计算近年来取得了飞速发展，信息数据也迅速增加，传统的安全备份已经不能满足海量数据的增长，在这种情况下，除了要对云计算备份技术进行不断完善，还需要进一步强化SaaS、IaaS、PaaS等相关技术，另外通过加大IaaS虚拟化技术的应用能够全面提升资源的灵活性和利用率。

五、结束语

云计算的应用进一步提升了传统的数据利用效率，是当今网络大数据时代最佳的一种计算模式。但是云计算技术的应用需要依赖于网络，导致其容易受到网络攻击的影响，进而给数据安全带来威胁。因此，需要进一步完善信息数据安全技术，这样才能满足信息时代下数据的安全需求。

参考文献：

[1]唐志凌.基于云计算的个人信息安全风险以及应对策略——治理信息供应链的途径探析[J].现代商业, 2021(05):43-45.

[2]王晶晶.大数据时代下计算机网络信息安全问题研究[J].电子测试, 2021(04):123-124.

[3]汤荣秀.云计算环境下网络信息安全技术发展研究[J].无线互联科技, 2021,18(03):19-20.