云计算环境下计算机网络安全设计

唐玉涛
南京优玛软件科技有限公司　江苏南京　210000

摘　要：伴随计算机网络的不断发展，云计算应运而生。其独有的特点，强大的优势，极大地改变了传统的网络应用方式。目前，已经作为一种新型互联网技术，它已经广泛地应用于人们的生活中，给人们的生活带来极大的便捷。为保证云计算得到安全、有效应用，需要重视安全防范工作，提升安全防范意识、优化安全措施，以改善云计算发展背景下计算机网络安全问题。文章简述了云计算技术的特点，分析了云计算环境下计算机网络安全方面存在问题，进一步探讨可采取的安全防范策略。

关键词：云计算；计算机网络完全；问题分析

The Design of Computer Network Security in Cloud Computing Environment

Yutao Tang
Nanjing Yuma Software Technology Co., Ltd. Jiangsu Nanjing 210000

Abstract: With the continuous development of computer networks, cloud computing came into being. Its unique characteristics and powerful advantages have greatly changed the traditional network application way. At present, as a new Internet technology, it has been widely used in people's life, bringing great convenience to people life. To ensure the safe and effective application of cloud computing, it is necessary to pay attention to the security prevention work, enhance security awareness, and optimize the security measures, to improve the computer network security problems under the background of cloud computing development. This paper briefly describes the characteristics of cloud computing technology, analyzes the problems existing in the computer network security in the cloud computing environment, and further discusses the available security prevention strategies.

Keywords: cloud computing; computer network Security; problem analysis

引言：

本文主要以云计算环境下计算机网络安全防范作为研究的课题，笔者在对文献资料进行收集和整理的基础之上，对课题进行了细致化的分析和研究。文章在阐述相关理论基础之上，对云计算环境下计算机网络安全防范存在的问题进行分析，而后则是提出云计算环境下计算机网络安全防范的优化措施，以期通过本文的研究可以为云计算环境下计算机网络安全防范的优化和完善提供一定的借鉴和帮助。

1　计算机网络安全特征

云计算技术是在电子通信技术、互联网技术等技术的基础上发展而来的技术。现如今，我国社会生活与生产中的各个领域都对云计算进行了广泛应用，推动了计算机网络的多样化发展[1]。所以，对于云计算环境下的计算机网络安全问题来说，主要有以下几方面特点：（1）完整性。针对云计算环境下的计算机网络，没有给予用户授权的情况下无法删除与更改计算机网络中存在的数据信息，因此具有完整性的优势。（2）保密性较高。云计算环境下的计算机网络数据信息具有较高的隐私性，在没有得到相关授权操作的同时无法共享与传播现有的数据信息。（3）信息审核性良好。对于计算机网络安全问题来说，常常会发生多样化的安全风险与安全隐患，计算机网络通过云计算的方式可对用户进行授权，帮助其对自身的数据信息进行安全保护。（4）可操作性较高。在云计算的环境下，计算机网络如果没有得到用户的授权，则无法对用户的数据信息进行应用、共享、传播与

处理操作。

2 云计算环境下计算机网络安全现状

2.1 病毒黑客问题

病毒黑客问题一直是影响计算机网络安全的重要问题，云计算环境下黑客与病毒的窃取目标更加明确，并且手段更加多样化。云计算环境下黑客是网络安全的重大威胁，并且在云计算环境下由于内部数据数量更多，内容更加驳杂，黑客入侵后的不确定性也逐渐加大，有黑客进入云系统针对性复制并窃取资料，也有黑客是抱着证明自身技术实力入侵云系统，但无论黑客抱有何种目的，对云系统的破坏和云计算的影响都是极为恶性的，云计算环境下黑客对于云计算的干扰和危害必须加以重视，为了提升云系统对于黑客的抵御能力，当前各方网络安全团队都在不断加固安全系统的防护措施[2]。病毒问题是影响计算机网络安全的重要因素，也是云计算环境下比较常见的问题，现阶段云计算环境下的网络病毒发生了很大的变化，传统传染病模型如SIS、SIR、SEIR等在云计算环境下都发生了新的变化和改变，为云计算环境的网络安全带来了不利影响。而当前针对云计算环境下病毒的研究也在不断提升，网络安全专家会根据云系统病毒传播特点以及隐匿方式等进行分析，通过对应的杀毒软件以及系统升级的方式对病毒进行清除。

2.2 云计算安全隐患

云计算自身存在安全隐患是计算机网络安全面临的一大威胁，采用分布式计算其数据处理和计算速度快，但向云端系统传输数据安全风险较大，掌握了破解密钥即可轻松获取大量数据信息。云计算应用中，涉及用户个人隐私和大型企业商业数据上传、存储，这些数据价值极高，虽然云计算服务商为企业和个人提供信息不被泄露担保，但企业内部人员存在不确定性以及内部数据价值的诱惑下，云计算环境中数据信息风险增加。近年来数据泄露案例中，很多情况下都是企业内部人员知法犯法导致的恶性事件，因此云计算环境下加强计算机网络安全防范除了要对外部风险加以防范外，还要采取有效、规范的内部密钥储存。

2.3 安全技术问题

安全技术问题一直是计算机网络安全问题中最为关键的问题，在云计算环境对于计算机的安全技术需求越来越高，安全技术方面暴露的问题也越来越多，云计算环境下的计算机安全技术存在较多的不足，特别是在保障性安全技术方面。现阶段关于云计算相关的安全防护软件以及安全防护系统仍处于一个不断发展和完善的阶段，云计算环境下的网络安全技术往往是与安全威胁相对应的，云计算环境下常见的隐私窃取、资源冒用、病毒感染等问题都是迫切需要可靠安全技术进行处理的问题。当前信息安全防护技术仍存在一定的局限性，特别是在云计算环境下，云计算平台中储存了大量的数据和信息，由于安全防护技术方面的薄弱，容易被不法分子窃取，安全防护技术是云计算环境下保证网络安全需要不断完善的一项技术。同时，用户在使用云计算进行数据运算时，数据传输连接过程中，数据加密技术严谨性较差，密钥容易被破解等，也是当前安全技术中较常见的不足之处。

3 云计算环境下加强计算机网络安全防范相关策略

3.1 加密技术的合理化运用

提升信息数据的安全性以及保障用户合法权益是十分重要的。在提高安全性以及保密性的过程当中，最常规也是操作性较强的方法，就是使用加密技术，在运用这一项技术时，一般情况下是在云管理以及云储存服务器当中对数据进行安全性的传输。在现如今最常使用的加密技术就是RSA非对称性加密算法，这一种算法会对用户端当中存在的密匙，进行服务器和用户端直接非对称性的数据传输，在进行数据传输时，一般情况下会运用DES对称性加密算法。用户在实际生活当中，想要对数据进行储存时，数据会进入与之相对应的数据库，再由用户端的加密技术对数据进行加密处理，在虚拟网络的环境之下，使用多元化的验证模式对用户的身份实施验证，而后云计算安全系统就能够在保证信息安全的同时，提升安全系统的保密性。

3.2 提升客户端的安全防范的意识

在云计算背景下，不容忽视用户的安全防范意识，要持续提升和教育用户的防范意识。首先，做好用户的个人身份认证，实名认证及短信认证可有效避免不明身份者、不法分子及黑客的入侵，可实现对非授权用户的严格监管，能有效实现负面影响的集中控制。其次，用户要学习具备基本的网络安全知识和良好的计算机操作习惯，避免在公用计算机进行数据信息及相应存储密码的设置操作。要定期对计算机进行安全体检、扫杀病毒、修复漏洞、安装补丁，防止客户端的非法侵入。企业用户要根据自身特点，制定特有的安全保证措施，比如为云平台提供服务的企业，可以借助过滤、防范手段切实提高计算机系统的防护水平。常用的方式，使用开源加密软件TrueCrypt对磁盘加密，使用RSA、DES对用户信息加密，添加Websense对恶意代码进行拦截，使用

Vontu对机密软件进行数据防护，使用Vericept工具对个人用户计算机中的数据信息传输进行监控，及时发现安全隐患，并对恶意信息进行过滤拦截，保证数据信息的安全性。

3.3数据备份与还原

为保障云计算环境下计算机网络安全，需要进行必要的数据备份与还原，避免数据损坏和丢失后用户造成严重损失[3]。用户操作过程中，容易出现操作失误和病毒攻击等情况，需采取数据备份还原措施保障数据完整。具体在云计算环境中，信息数据的存储是采用离散方式进行的，这种方式可以使数据快速还原，因此定期备份数据可以保障数据安全。数据损坏、丢失情况下也可还原恢复，避免用户损失。

3.4构建安全防护体系

为了对计算机网络安全管理模式进行完善与优化，相关工作人员可积极构建计算机网络安全防护体系，包含工作站防护、服务器防护两个模块。工作站防护属于计算机网络安全防护体系中的最底层防护，是最后一道安全防御措施。服务器防护不仅拥有监控病毒的能力，同时还应包含病毒码自动更新功能、报警功能和远程安装功能等。大部分用户的电子邮件与网页浏览次数较多，使得病毒入侵路径数量不断增加。可通过设置新关卡的方式来确保用户数据信息的安全。对于用户的网络数据信息资源来说，一旦发生安全事故将产生较大的损失。因此，用户可以通过对计算机网络内的数据信息进行定期备份的方式来确保其数据安全，比如备份系统日志以及服务器数据等。一旦计算机网络发生意外，可以对用户的数据信息及时恢复。用户可通过购买专业的网络备份软件的方式来降低计算机网络安全事故所带来的不良影响。

3.5对信息数据实施集中管理

建立云计算所需安全模型，整合计算机信息数据资源，进行全方位的管理。注重对边界信息数据的管控，实行动态化资源管理，并对其分析研究，为信息数据的构建制定更合乎逻辑的流程，促进物理结构发展，在物理边界安全性领域上保证系统安全，在云计算环境下更好保证相应操作的流量及信心安全。此过程中的数据管理实施两级人员负责制，普通运维人员仅负责对服务器的日常维护、操作，核心人员则有更为严格的运维流程约束，控制其对用户数据信息的篡改、删除与使用，大大加强计算机网络的安全，保证数据的安全性和保密性。

4 结束语

综上所述，伴随着互联网的崛起和发展，人类已然步入到了信息化的时代，云计算技术也在获得发展和完善，这一项技术为社会的发展提供了助力，其促使人民群众的生活更加的便捷。但是云计算也可以称之为一把双刃剑，这一项技术能够为人民群众的工作以及学习提供便捷，但是也存在一些网络安全问题，针对出现的问题，通过大力加强安全技术的研发以及应用，提高客户端的安全防范意识，对信息数据实施集中管理以及加紧完善相关法律等措施，可有效保障云计算环境下的计算机网络安全。

参考文献：

[1]陆欢荣.云计算环境下的计算机网络安全防范研究[J].网络安全技术与应用，2021（08）：76-77.

[2]高雯雯.云计算环境下计算机网络安全存储系统设计[J].电脑知识与技术，2021，17（08）：62-64.

[3]何振贤.云计算环境下的计算机网络安全问题分析[J].福建电脑，2021，37（01）：62-63.