

云计算环境下的计算机网络安全防范研究

齐 岗 徐培罡

自然资源部第一航测遥感院 陕西西安 710054

摘 要: 随着我国社会经济的快速发展以及科学技术水平的不断提高,信息技术与大数据技术也飞速发展,云计算开始在人们日常生活与工作的各个领域得到了十分广泛的应用,并在社会生产与生活中占据十分重要的地位。据此,结合云计算发展应用背景,探讨计算机网络安全面临的主要问题,并尝试提出与之相应的安全防范技术,以推动云计算环境下优质环境的营造,确保信息数据应用安全。

关键词: 云计算; 计算机; 网络安全

Research on computer network security in cloud computing environment

Qi Gang, Xu peigang

The first Institute of aerial survey and remote sensing, Ministry of natural resources, Xi'an, Shaanxi 710054

Abstract: With the rapid development of China's social economy and the continuous improvement of the level of science and technology, information technology and big data technology are also developing rapidly. Cloud computing has been widely used in various fields of people's daily life and work and occupies a very important position in social production and life. Based on this, combined with the development and application background of cloud computing, this paper discusses the main problems faced by computer network security and tries to put forward corresponding security prevention technology to promote the construction of a high-quality environment under the cloud computing environment and ensure the security of information and data applications.

Keywords: cloud computing; computer; network security

引言:

云计算对人类生产生活有着深远影响,极大便利了人们的工作生活,但同时网络安全问题也进一步受到人们的关注。云计算技术应用中,需要借助开放的互联网系统完成数据的运算处理,在数据传输过程中可能出现信息被窃取、泄露等问题。当前在云计算方面尚缺乏完善的安全保障技术,面对突发情况无法积极抵御,同时

信息时代发展下网络病毒隐蔽性、攻击性增强,黑客的技术水平也在提高,加大了防范工作难度,严重威胁到信息数据安全。要求加强对计算机网络的安全方案,完善安全技术、加强加密等,增强计算机网络安全性。

1 云计算技术的内涵

云计算技术是一种崭新的计算方式,其能够使用户在几秒钟之内处理上亿条信息量的能力,并且其还提供强大的网络服务,云计算技术是分布式的算法、并行处理算法以及网络技术的延伸。在现阶段,云计算这一项技术获得了空前的发展,云计算技术的基础架构在平台方面具备可靠性以及安全性等特征,逐步展现出其强大的稳定性和生命力,被越来越多的用户、企业、政府以及高校等采用^[1]。云计算技术将任务分布在计算机的资源池上,多种应用程序可以参考自身的实际诉求获取所需要的相关资源,这一些庞大且十分丰富的数据将资源

作者简介:

齐岗、男、汉族、1972.03、籍贯:西安、学历:本科、职称级别:工程师、研究方向:地理信息装备保障、邮箱:317955979@qq.com;

徐培罡、男、汉族、1986.04、籍贯:陕西渭南、学历:硕士、职称级别:高级工程师、研究方向:摄影测量与地理信息系统、邮箱:370457225@qq.com。

储存至云计算的平台当中，并在平台当中实施运算，这一种计算方法和传统的计算方法有着明显的差异性，其能够为用户提供便捷的同时，更加经济的运用计算机资源。

2 云计算环境下计算机网络安全防范存在的问题

2.1 安全系统当中身份认证存在一定的欠缺

对现如今网络安全系统进行分析，为了能够进一步的加强网络安全系统抵御外部不安全因素的能力，身份认证这一项技术是十分重要的。可是由于现阶段身份认证这一项技术水平存在一定的局限。在这一项系统当中，还存在着一些不确定的因素和缺陷，所以导致信息数据存在泄露的风险，一些黑客以及不法分子对计算机进行攻击时，通常会利用平台管理器窃取他人的相关信息，而后会使用这些信息登入其他平台，对数据进行非法的盗用和截取。

2.2 网络虚假信息泛滥

由于网络环境的虚拟性，伴随着大量虚假信息的传播，大量的虚假信息、危险链接等内容，使得网络安全受到严重挑战，并诱发严重的信息安全问题^[2]。目前而言，云计算仍然处于完善优化阶段，在安全防护的措施上亟待优化，尤其是缺乏对网络源地址以及源代码的安全性检测、筛查，使各类虚假信息难以被及时甄别，给服务器、软件等带来压力、干扰和损坏，给云计算的深度应用带来威胁。

2.3 云计算安全隐患

云计算本身的安全隐患是威胁计算机网络安全的重要问题。云计算在提高了数据处理和计算速度的同时，大量数据传输到云端系统上本身就具有一定风险性，如同将所有的文件资料储存在一个巨大柜子中，只要掌握了破解云端系统防护的密钥，就可以轻易获取大量的数据和信息，这是当前云计算环境下最核心的风险和问题。云计算涉及的单位以及个人隐私数据的上传和储存，在各类型数据中具有极高的价值，尽管云计算服务商为单位以及个人提供数据不会被泄露的保证，但是单位内部人员本身具有不确定性，加之云计算内部数据本身的价值都在无形中增加了云计算环境下数据信息的风险性。近年来有关资料数据泄露的报道也显示，多数用户个人信息泄露问题都是单位内部人员知法犯法导致的恶性问题。云计算环境下计算机网络安全防范除了需要防范外部的风险外，内部密钥储存的有效性与规范性同样需要注意和重视。

3 云计算环境下计算机网络安全防范

3.1 增强安全防范意识

在云计算环境下，计算机网络安全防范要增强防范意识，这是保障网络安全先决因素和基础要素，云计算用户、服务提供商均需增强自身安全意识。特别是云计算服务提供商需深入分析当前网络安全环境，改进系统安全防护、抵御能力，营造安全的云计算环境^[3]。同时增强安全防范意识的情况下，内部管理加强，云计算系统内部安全隐患得以减少。同样，云计算基础用户与使用单位安全防范意识也要加强，综合考虑云计算服务器综合实力和安全保障水平来选择，与安全防护能力较强机构加强合作，身份识别密钥需严格管控避免泄露。云计算环境下，相关参与方需对网络信息数据保密性原则充分重视，在使用云计算与计算机网络过程中规范操作，来源、用途不明的文件不可点击，避免使用公用电脑和公共网络执行相关操作，尽量降低安全风险。

3.2 加强客户端网络的安全管理

伴随信息时代的发展，每个基于云计算环境下的计算机网络用户，均需要不断强化安全防范能力，在实际使用的过程中能够采取规范、安全的操作，同时定期对安全软件及设备进行维护，做好信息数据的管理与备份，避免数据库受到攻击而损坏^[4]。比如，借助网络安全管理系统中的异常行为分析模块，主要负责对系统客户端的操作实施监测与分析，并与数据库中的权限及数据进行对照，及时掌握异常情况动态，确定操作中是否存在违规行为，一旦确认其属于违规问题，将由防御决策生成模块进行处理，特别是针对所产生的异常行为实施分析，快速生成科学的防御决策，包括USB接口封闭决策、网络切断决策、病毒隔离决策及网络警告决策等，防止云平台中的信息数据被USB接口或者网络渠道窃取，从而自动完成对客户端网络安全问题的应对。利用制度进行使用约束，与云计算一道做好上下游的安全衔接，使网络攻击无所遁形，全面提升信息数据的安全性。

3.3 提高用户信息、数据的安全性与保密性

(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钥，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。

(2) 过滤器技术的运用。在现阶段运用比较广泛的过滤器包含了 Websense 以及 Vericept 等，这一项技术主要是对离开的网络数据进行全过程的监督和管理，并对一些敏感信息进行拦截，全方位的对数据的使用和数据的传输进行监控。

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。

3.5 数据备份还原

云计算环境下网络安全防范必须要做好数据的备份还原工作。数据备份与还原是网络安全中最为重要且关

键的防线，云计算环境下计算机网络安全想要得到保障，需要定期进行数据备份工作，数据备份为后续系统故障、病毒感染或者操作失误等提供了挽回的余地。并且在云计算环境下，云计算技术为备份还原提供了更为便利的条件，通过离散式储存方式进行数据储存，能够在一定程度上保证数据的安全，并且在数据损坏时，将备份储存的数据快速召回，从而减少用户损失。

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，使人们的生活更加的便捷。但是云计算也可以称之为是一把双刃剑，这一项技术能够为用户的工作以及学习提供便捷，但是也存在一些网络安全问题，一旦无法科学的解决这一些网络安全问题，势必会对人民群众的合法权益带来影响，导致用户隐私信息遭到泄露，并且也会制约和谐社会的进一步推进。

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.
- [4]陈海红.探讨新时期云计算环境下的计算机网络安全技术[J].数字通信世界, 2021(01): 175-176+33.