云计算环境下的计算机网络安全防范

李欣

绥化学院，黑龙江 绥化 152000

摘　　要： 在云计算环境中，计算机网络安全问题是不可忽视的挑战，也是激发创新和持续改进的重要动力。研究人员应站在技术的前沿，探索并应对不断涌现的安全挑战，通过深入理解安全威胁，采取多层次、全方位的安全防御措施，在风险与利益之间找到平衡。随着科技的进步，需要以更智慧的方式保护网络安全，同时为用户提供高效、可靠的云计算服务。在这个过程中，需要不断汲取经验和教训，不断完善技术手段，共同建立一个更加安全、稳定和可信赖的云计算环境，为数字化时代的发展提供强有力的支撑。

关 键 词： 云计算；计算机；网络；安全；防范

Computer network security in cloud computing environment

Li Xin

Suihua University, Suihua, Heilongjiang 152000

Abstract: in the cloud computing environment, computer network security is not only a challenge that can not be ignored, but also an important driving force to stimulate innovation and continuous improvement. Researchers should stand at the forefront of technology, explore and respond to emerging security challenges, and find a balance between risks and interests by deeply understanding security threats and taking multi-level and comprehensive security defense measures. With the progress of science and technology, we need to protect network security in a more intelligent way, and provide users with efficient and reliable cloud computing services. In this process, we need to constantly learn from experience and lessons, constantly improve technical means, and jointly establish a more secure, stable and reliable cloud computing environment to provide strong support for the development of the digital era.

Keywords: cloud computing; computer; network ; security; prevention

一、云计算和网络安全的定义

（一）云计算

所谓“云”，是指一种基于网络的服务方式和架构模型，它能够以灵活且易于扩张的方式来分配并利用各种在线或远程的数据中心所提供的可变性的数字资产和服务。这种新型的信息存储及传输方法被称作“云”的原因在于它的便利性和高效性能：客户只需支付他们实际使用的部分费用即可获取所需服务的全部功能，而无需投入巨大的资金去购买服务器硬件设施，或者雇佣专门的技术人员维护系统运营。此外，“云端”还允许个人通过访问权限控制他们的个人信息的安全分享范围——这意味着所有未经许可的人都无法查看这些敏感资料或是对其做出修改等操作行为。因此，当选择信任并且依赖这个由众多企业共同构建起来的庞大平台时，隐私安全也得到了保障。当面临网络安全的挑战时，授权使用者能够利用特定的手段来解决这些问题，从而确保信息的保密性和可靠性[1]。

（二）计算机网络安全

随着时间流逝，现代信息技术与网络通信在其运作中容易遭受外来不良环境的影响。这些负面情况对于中国互联网造成的主要困扰包含信息资料的泄漏、遗失或盗窃。这部分也间接阻碍了中国的信息技术的长远、稳定进步。目前，大数据在中国已然成为现实，我们必须积极应对并解决问题。保障计算机网络的安全是我们未来互联网发展的核心任务。

二、基于云计算环境的计算机网络安全隐患

（一）数据隐私泄露风险

在云计算环境中，数据隐私泄露是一个严重的安全隐患。大量敏感数据存储在云端，包括个人信息、财务数据、商业机密等。黑客攻击、数据泄露或未经授权的访问都可能导致敏感数据的暴露和泄露。这会对个人隐私和企业声誉造成损害，甚至引发法律问题。虽然云服务提供商通常会采取安全措施来保护存储在云端的数据，但在数据的传输和存储过程中，仍然在潜在的安全漏洞，需要加强保护措施，以防范这些潜在风险[2]。

（二）多租户环境的安全挑战

云计算可提供多租户服务，使多个用户能共享同一资源，但这也带来了一些安全挑战。在这种共享环境下，恶意用户可能会利用共享资源进行网络攻击，导致数据混淆、隔离不足等安全问

课题来源：黑龙江省高校基本科研业务费，课题名称：基于云计算的电子信息产业数据服务优化研究，课题编号：YWF10236240126。

作者简介：李欣（1981.07-），男，汉族，黑龙江省绥化市，本科，副教授，研究方向：网络工程、通信工程、物联网。

题。当一个用户的安全性受到威胁时，其他用户的数据和服务也会受到影响。此外，难以完全保证数据在共享环境中的隔离性，这使得用户无法充分控制其数据的安全性和隐私性，进而造成潜在的风险和问题。

（三）虚拟化技术的安全漏洞

在云环境中使用的虚拟化技术同样存在潜在的安全风险。该技术也存在漏洞，黑客可以利用这些漏洞进行攻击。例如，虚拟机逃逸指黑客通过虚拟机内的漏洞，越过虚拟机的隔离边界，进而获取主机操作系统的控制权限；虚拟化层次攻击指黑客针对虚拟化架构中的各个层次进行攻击，导致数据泄露、服务中断、系统崩溃等问题[3]。

（四）服务供应商的安全性

云服务供应商的安全性问题也是一个重要的隐患。用户在使用云服务时，往往需要依赖供应商提供的安全措施和标准，但不同的供应商会采取不同的安全标准和措施，用户难以全面了解和掌控供应商的安全性。若供应商存在安全漏洞或安全措施不力，用户的数据和服务则会受到影响，甚至出现数据泄露或服务中断的风险。

（五）数据备份和灾难恢复

在云环境中，数据备份和灾难恢复也存在一些潜在的安全风险。尽管云服务提供商通常会提供数据备份和灾难恢复服务，但用户仍需关注数据备份的完整性、可靠性和安全性。如果备份不完整或备份数据受到未经授权的访问或篡改，当出现灾难性事件时，用户就无法及时有效地恢复数据，导致数据损失甚至业务中断。

三、在云计算环境下的计算机网络安全技术

（一）防火墙技术

防火墙技术的核心功能在于辨别并阻挡恶意入侵与病毒威胁，以确保计算机系统的安全性。通常可以划分为单机防火墙及网络防火墙两大类。针对单机的防火墙主要是监控程序的使用情况，当发现敏感操作时能够及时处理，防止其干扰到整个系统的稳定运作。而对于线上网络环境中的反病毒应用则更适合于处理网络上的病毒问题，如若在数据交换过程或者网络环境内有潜在的主机攻击者，防火墙会迅速启动扫描检查，从而为计算机提供防御保障[4]。

（二）漏洞扫描技术

作为一种主要的安全隐患来源，网络漏洞常常被恶意攻击所依赖并加以滥用。因此，采用有效的漏洞探测与修正方法可以显著减少潜在的风险。在这个过程当中，漏洞检查对于维护设备及应用软件的健康状况具有关键性的影响：它能够自动化地侦察到所有的 TCP/IP 接口、产生相应的反应报告并且分析其安全的特性等功能于一身，从而快速找到可能存在的薄弱环节或者不足之处（如存在的问题）并在必要时给出明确指示，以便让开发团队获得有用的数据支持，进而提升防护措施的效果及效率。若将虚拟的网络系统比作战场，那么漏洞扫描系统就相当于上空盘旋的侦察机，通过敏锐的“视觉”能准确识别出定位系统漏洞，使程序人员在信息防护战争中抢占先机，为计算机系统创造良好的运行环境。一般情况下，漏洞扫描结果呈现出三种状态。一是推荐修复型：即是系统漏洞会扰乱系统环境，给病毒和黑客提供可乘之机，需要下载安装补丁来完善运行环境；二是选择修复型：使用者可根据计算机情况采取选择性修复的方法，多适用于个人电脑；三是不推荐修复型：不是所有漏洞都建议修复，很多识别的漏洞对计算机安全不会构成威胁，甚至修复会影响计算机性能，所以使用者要酌情科学的利用漏洞扫描技术，确保计算机系统安全[5]。

（三）加密授权技术

密码学是关于如何保护信息的科学，而授权则是控制谁可以访问它。这两种方法都像是一个安全屏障，能够防止恶意软件访问并阻止其传播。通过对信息进行加密，我们就像是在为它们上了把锁一样，只有拥有钥匙的服务方和服务接受方才能够读取这些信息。这样一来，即使有黑客或者病毒试图攻击我们的系统，他们也需要先获得这个密钥才能成功地破译出其中的内容。这就能确保个人隐私不会被盗用或是滥用了。由于云端的数据交换方式可能会涉及到多个参与方，所以这种情况下的不确定因素较多，为了保证信息的安全传递，我们可以采用加密的方式来实现“发送前的封装”与“接收后的拆包”的过程，从而减少因通信过程中出现问题导致的泄漏及修改的可能性。

（四）访问控制技术

三项关键因素构成了网络空间中的安全访问管理：客户端(UserEnd)和服务器端(ServerSide)，同时还有相应的访问策略(AccessPolicy)。一旦客户需要某种服务的支持就会向该平台发送命令，然后由后者接收这些指示并且根据具体情况给予响应——这就是所谓的“访问控制”。它主要包括限制与规范操作者的行为以达到预期的目标，比如确定哪些人可以获得特定的权利或者禁止某些人的进入等措施。这种方法不仅能够确保只有授权的人才能拥有使用的权力，而且还避免了一些恶意攻击的发生，从而保障个人数据的安全性和保密性的目的得以实现。总而言之，“访问控制”（AccessControl）是一种综合手段，包含着诸如“角色定义”，“特性设置”，“互联网上控制”等多种形式的技术应用于实际场景之中并以此为基础构建起一种有效的防护体系用于防范潜在的风险及威胁的存在[6]。

四、云计算视域下的计算机网络安全技术优化的路径

（一）加大技术研发投入

在云计算视域下，计算机网络安全技术的优化离不开对技术研发的投入。随着云计算的广泛应用，网络安全威胁也日益复杂多变，只有不断创新技术手段，才能提升安全防护能力。加大技术研发投入，意味着要集聚更多的研发资源和人才力量，专注于云计算安全技术的突破与创新。通过深入研究云计算环境的特性，可以开发出更加高效、精准的安全防护系统，有效应对各种网络攻击和威胁。技术研发投入还应关注新兴技术的融合应用。

例如，人工智能、大数据等技术可以为云计算安全提供强大支持。利用这些技术的优势，能够实现对网络安全威胁的智能识别和预警，进一步提高安全防护的自动化和智能化水平[7]。

（二）建立多层次安全防护体系

由于云计算的复杂性和开放性，单一的防护手段难以全面应对各种安全威胁。因此，需要构建一个多层次的防护体系，主要包括物理层防护、网络层防护、应用层防护、数据层防护及人员管理等。物理层防护可以确保数据中心硬件和设施的物理安全、防止非法入侵和物理破坏；网络层防护通过设置防火墙、入侵检测、防御系统，部署网络安全设备、过滤和监控网络流量，及时发现并阻断恶意攻击；应用层防护采用安全审计、漏洞扫描与管理、Web 应用防火墙等技术来加强应用程序的安全审计和漏洞管理，防止应用层的安全漏洞被利用；数据层防护通过数据加密技术保护数据机密性，建立备份恢复机制，确保数据完整性，实施访问控制策略，防止未经授权的访问；人员管理通过安全培训、安全管理制度、安全意识提升等策略加强对员工的安全培训，制定完善的安全管理制度，提升员工的安全意识和操作技能。这些层次的有机结合，可以有效应对各种安全威胁，提高云计算环境的安全性[8]。

（三）加强数据安全和隐私保护

随着数据量的激增和共享性的提升，必须采取更加严格的措施来保障数据安全和用户隐私。加密技术是保障数据安全的关键，它通过加密处理敏感数据，可以有效防止数据在传输和存储过程中被非法获取。同时，建立完善的访问控制机制，确保只有经过授权的人员才能访问相关数据，保障数据安全。隐私保护策略的制定与执行也一样重要。云服务提供商应明确告知用户数据收集、使用及共享的目的，并征得用户明确同意，方可对数据进行处理。尤其是对于个人敏感信息的处理，应遵循最小化原则，即只收集实现特定目的所需的最少信息。定期的安全审计和风险评估也是加强数据安全和隐私保护必不可少的手段[9]。

（四）提高云服务提供商的安全管理水平

当前，云服务市场的竞争日益激烈，但安全管理水平的参差不齐却成为行业发展的隐患。为了提升整体安全标准，云服务提供商需要从多方面着手。技术层面，云服务提供商应加大研发投入，不断更新和完善安全防护技术，在面对各类网络威胁时能够积极应对，还应加强安全漏洞的监测和修复，降低系统被攻击的风险；管理层面，建立严格的安全管理制度和流程，明确各部门的安全职责，保证安全工作的有序开展，并加强对员工的安全培训和教育，提升他们的安全意识和操作技能，强化安全管理水平；合作与监管层面，云服务提供商应积极与相关部门和机构合作，共同制定和执行安全标准，推动行业的健康发展，同时接受第三方机构的定期审计和评估，确保自身的安全管理水平符合行业标准[10]。

参考文献

[1]魏式玉. 对计算机网络安全问题及其防范措施的几点思考［J］. 中国新通信，2023,25（11）:91-93.

[2]薛峰. 基于云计算环境下计算机网络安全问题与建议［J］. 信息记录材料，2021,22（9）:65-66.

[3]杨浩南. 计算机网络安全的主要隐患及管理措施思考［J］. 网络安全技术与应用，2021（4）:159-161.

[4]刘熙瑞，叶鑫. 基于云计算环境下计算机网络安全问题的认知与思考［J］. 中国新通信，2020,22（14）:145.

[5]孙亚志. 云计算环境下的计算机网络安全问题探［J］. 科技创新导报，2020,17（5）:136,138.

[6]孙建兰. 云计算环境下的计算机网络安全问题［J］. 电脑知识与技术，2018,14（11）:32-34.

[7]伊文斌. 云计算环境下计算机网络安全技术的优化［J］. 无线互联科技，2023，20（6）：99-102.

[8]林锦忠. 基于云计算环境计算机网络安全技术的优化分析［J］. 网络安全技术与应用，2022（4）：77-78.

[9]刘超. 以云计算为基础的计算机网络安全技术优化路径分析［J］. 现代工业经济和信息化，2022，12（8）：150-152.

[10]刘妍君. 计算机网络安全技术的影响因素与防范策略分析［J］. 信息记录材料，2021，22（10）：74-75.