基于云计算的计算机网络安全研究

卢　毅　张铕辉
（郑州城建职业学院　郑州　450000）

摘　要　云计算环境为数据共享提供了便利，但存在诸多计算机网络安全隐患。这些隐患主要涉及数据隐私泄露、多租户环境带来的安全挑战、虚拟化技术的安全漏洞、服务供应商的安全性、数据备份、灾难恢复等。针对这些安全隐患，需要采取一系列措施来加强网络安全，如加密数据，多层次安全防御，定期安全审计，加强虚拟化安全管理，建立灵活的灾备与恢复机制等。文中探讨了云计算环境下的网络安全隐患及解决方案，以提高云环境中的数据和信息的安全性、可靠性。

关键词： 云计算环境；计算机网络安全；安全隐患
中图分类号　TN915.08

Research on Computer Network Security Based on Cloud Computing

LU Yi and ZHANG Youhui
（Zhengzhou Urban Construction Vocational College,Zhengzhou 450000,China）

Abstract　Cloud computing environment facilitates data sharing, but there are many cyber security risks. These risks mainly involve data privacy leakage, security challenges brought by multi-tenant environment, security bugs of virtualization technology, security of service providers, data backup, disaster recovery, etc. To address these security risks, a series of measures need to be taken to strengthen cyber security, such as encrypted data, multi-level security defense, regular security audits, strengthening virtualization security management, and establishing flexible disaster recovery and recovery mechanisms. This paper discusses cyber security risks and solutions in cloud computing environment to improve the security and reliability of data and information in cloud environment.

Key words　Cloud computing environment,Computer network security,Security risks

0　引言

在数字化时代，人们的日常生活和工作高度依赖于计算机和网络。因此，确保计算机网络的安全性至关重要。网络安全不仅涉及个人隐私和敏感信息，还关系到企业的机密数据、财务信息以及全球的关键基础设施。网络安全不仅是一个技术问题，更是一项涉及政策、教育、意识和技术的综合工程。只有重视和加强网络安全措施，才能更有效地应对日益增长的网络威胁和风险，确保网络稳定、可靠、安全地运行。

1　云计算的主要特征

1.1　数据共享

在云计算环境中，用户可以共享存储在云端的数据和资源。这种共享模式使得多个用户能在不同的地点和时间访问、共享同一份数据，提高了工作的效率和协作性。不过，数据共享也带来了一些安全隐患，需要通过严格的访问控制和加密机制来保护敏感信息，防止未经授权的访问，避免数据泄露。

1.2　提高安全性

强调安全性是云计算的突出特点。云服务提供商采取了多重安全措施，以确保云端数据的安全性[1]。这些措施包括实施物理安全措施、数据加密技术、身份验证、严格的访问控制、监控和审计机制等。综合应用这些安全措施，能为用户提供水平较高的安全保护。通过这些措施，用户可以更放心地将数据存储在云端，减少数据泄露或损坏的风险，确保数据的隐私性和完整性。

1.3　强大的功能性

云计算提供了多种服务模式，如基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。这些服务模式赋予用户极大的灵活性，使其可以根据需求选择不同的服务类型。用户无需在本地部署和维护昂贵的软硬件设施，便可获取所需的计算资源和功能。为了确保其安全性和可靠性，对云计算的严格管理和控制尤为重要。用户和企业需谨慎使用，充分了解其功能特点，并实施适当的安全措施，以充分利用其潜力，避免潜在的风险。

作者简介：卢毅（1981—），本科，中级工程师，研究方向为计算机网络技术；张铕辉（1991—），本科，助教，研究方向为网络工程。

2 基于云计算环境的计算机网络安全隐患

2.1 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，仍然存在潜在的安全漏洞，需要加强保护措施，以防范这些潜在风险。

2.2 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。

2.3 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[2]。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。这些安全漏洞使得云环境中的数据和服务面临着未经授权的访问或控制的风险。

2.4 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。

2.5 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。

3 基于云计算环境解决计算机网络安全隐患的措施

3.1 加强数据加密和访问控制

加强数据加密和访问控制，是在云计算环境中应对计算机网络安全隐患的关键措施之一。

数据加密技术在保障数据传输和存储的安全性方面发挥了关键作用。高级加密标准（AES）等先进的加密算法被广泛应用，其可以对云端数据和传输中的数据进行强化加密，有效预防未经授权的访问和窃取。这种数据加密技术不仅确保了数据在存储和传输过程中的安全性，还能在数据意外泄露或遭受外部攻击时维持数据的保密性，保护其免受外界的影响[3]。

严格的访问控制策略同样至关重要。通过建立认证和授权机制，限制和管理用户对数据的访问权限，可以防止未经授权的个人或实体获取敏感信息。有效的访问控制策略可以保证只有经过授权的用户或实体才能访问数据，大幅降低数据被窃取或滥用的风险。实施细致和全面的访问控制措施非常关键，如多种层次的认证机制、严格的身份验证流程、基于角色的访问控制和精细的权限管理。采用这些策略，可以确保每个用户或实体仅能访问其所需的数据和资源，最大限度地减少系统内外威胁对数据的影响。这些措施共同构成了维护云环境中的数据安全的坚实基础，保障了敏感信息的保密性和完整性。

3.2 多层次安全防御机制

在云计算环境中，网络安全设备是建立多层次安全防御机制的基石，如入侵检测系统（IDS）、入侵防御系统（IPS）等，其可以通过监控网络流量和检测异常行为来及时发现并应对潜在的威胁。IDS系统可以识别潜在攻击并通知管理员，IPS则可以采取主动措施阻止网络攻击行为。这种安全设备有助于及时识别网络威胁，维护云计算环境的整体安全性。（1）防火墙在多层次安全防御中扮演着关键角色，其可以监控和筛选网络流量，有效防止未经授权的访问，阻止有害数据进入系统。通过配置灵活的防火墙，根据实际需求和安全策略灵活调整策略，可以增强系统对外界威胁的抵御能力，确保云计算环境的安全性。（2）加密技术和身份验证同样重要。强大的加密技术能在数据传输和存储过程中保护数据的隐私和完整性，而严格的身份验证措施（如双因素认证），可以确保只有得到授权的用户才能访问系统和敏感数据。这些安全措施是保护云计算环境，防止未经授权的访问，避免数据泄露的关键措施。（3）不断更新和维护安全措施是确保多层次安全防御的有效性的重要方法。定期评估和改进安全措施，采用最新的安全技术，有助于应对不断变化的网络威胁和攻击手段，提升云计算环境对各种安全威胁的抵御能力。这种不断演进的安全策略是保障云计算环境的安全性的关键。

3.3 定期进行安全审计与监控

安全审计与监控以有效的安全审计机制为基础，以确保对云计算平台进行全面评估和审计。例如，利用安全信息和事件管理系统（SIEM）等工具，可持续监控系统，以及时发现和应对异常行为或潜在威胁。这种定期的安全审计为发现和解决潜在的安全漏洞或攻击提供了支持。在进行安全审计时，首先需要全面评估和审查云计算环境，对系统

安全性、网络连接稳定性、应用程序强壮性等进行详细评估。通过仔细检查各项指标，可以发现并定位潜在的安全风险，为制定和执行有效的安全策略提供基础。定期的审计和监控对于识别系统中的异常行为或非法访问至关重要。这些异常是潜在的威胁、攻击或安全漏洞的外在表现[4]。安全团队通过分析和跟踪这些异常情况，能及时识别出安全威胁，并采取相应措施来应对和解决问题，确保云计算环境的安全性和稳定性。此外，定期的安全审计有助于验证安全政策和措施的有效性、合规性。通过审计已实施的安全政策，可以评估现行安全策略的实施情况，并在必要时调整和优化策略，以确保其符合最佳实践和法规要求。这种审计可以确保安全政策的贯彻与执行，并为应对不断变化的安全威胁提供支持。

3.4 加强虚拟化安全管理

加强虚拟化安全管理是云计算环境下解决计算机网络安全隐患的关键举措。虚拟化技术在云计算中的广泛应用，使得保障虚拟化环境的安全性至关重要。(1)通过实施安全配置管理来确保虚拟化环境的各项安全配置符合最佳实践和标准，这对减少系统风险至关重要。(2)及时更新和管理安全补丁也是确保虚拟化安全的关键。定期审查并及时应用安全补丁，能有效地修复系统漏洞，提升系统的整体安全性。(3)实施有效的虚拟机监控和管理。监控虚拟机的活动和行为，可及时识别并应对异常情况和潜在风险，这对于预防或最小化安全威胁对系统造成的影响至关重要。强大的监控措施能及时发现潜在的安全隐患，并采取必要的措施，以提高系统的整体安全性和稳定性。

3.5 建立灵活、完备的灾备与恢复机制

在云计算环境下，建立灵活、完备的灾备(Disaster Recovery，DR)与恢复机制是确保计算机网络安全的关键。(1)采用多样化的备份和恢复策略，以应对随时可能出现的灾难性事件，确保数据和系统能在遭受严重威胁或灾难时，快速、有效地恢复正常运行。(2)建立灾备中心和备份数据中心[5]。这些中心需具备实时备份和同步数据的能力，即使在灾难发生时，也能保障数据的完整性和可用性。在不同的地理位置建立灾备中心和备份数据中心具有必要性，这可以有效防范自然灾害或区域性网络攻击带来的风险，确保数据的安全性和可靠性。(3)采用弹性、可扩展的架构。系统需要具备自动化的扩展和恢复功能，以便在面临威胁时快速调整和执行必要的措施，保障数据和服务的连续性。这种灵活性能有效缓解突发事件对系统的冲击，确保系统持续、稳定地运行。(4)制定并持续优化完善的恢复计划。这些计划应定期进行测试和演练，以确保在发生灾难时可以迅速、有效地执行。经常性的演练有助于发现潜在问题和瓶颈，从而优化恢复策略，提高系统的灾难应对能力。

这些措施不仅可以提高系统的应变能力，也保障了系统在不可预测的情况下的安全性，确保服务的连续性和稳定性。通过建立灵活、完备的灾备与恢复机制，云计算环境下的系统能更好地应对各种威胁和灾难，最大程度地保障数据的完整性和可用性。这不仅可以缩短系统停机时间，还能提高业务的连续性和稳定性，确保云计算系统在各种挑战性的稳健运行。

3.6 合规性和合约管理

在云计算环境下，合规性和合约管理是确保网络安全的重要途径。(1)确保合规性意味着云服务提供商需要遵守国家法规、行业标准和规范，以保障用户数据的隐私性、安全性和可靠性。云服务提供商应建立严格的合规性框架，包括数据加密、访问控制和信息安全管理，以确保数据在传输和存储过程中的完整性和安全性[6]。(2)合约管理则需要建立清晰明确的合约和服务协议，以明确规定云服务提供商、用户的责任和权利。这些协议通常包括隐私政策、安全保障措施、服务级别协议等，以确保云服务的安全性和可信赖性。通过建立完备的合约和服务协议，可以提高服务的透明度和可预见性，帮助用户更好地了解服务提供商的责任和义务。

合规性和合约管理有助于确保用户数据的隐私性和安全性，规范云服务提供商的行为。这种严谨的管理框架，有助于构建用户和服务提供商之间的互信基础，同时提高服务提供商的责任感和透明度，增强计算机网络在云计算环境下的安全性。

4 结语

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。

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析[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.