云计算环境下的计算机网络安全与维护

杨文波　郭太祥　吴　鹏　赵　晔
河南金数智能科技股份有限公司　河南　郑州　450000

摘　要：云计算技术虽带来了计算资源的高效利用与灵活配置，但其环境下的计算机网络安全问题日益凸显。本文深入分析了云计算面临的数据传输与存储安全风险、云服务提供商安全性不足及用户安全意识欠缺等挑战，并提出了包括加强云服务提供商安全能力、数据加密技术应用、数据备份恢复策略实施、访问控制与安全认证强化，以及提升用户安全教育与培训等综合维护策略，旨在构建安全可靠的云计算环境。

关键词：云计算环境；计算机网络；安全与维护

引言：随着云计算技术的蓬勃发展，其在为企业提供计算资源高效利用与灵活调配的同时，也为计算机网络安全带来了新的挑战。云计算环境下的数据传输与存储、云服务提供商的可靠性、以及用户安全意识与技能等问题，直接影响到数据的安全性与业务的连续性。因此，深入探讨云计算环境下的计算机网络安全问题，并制定有效的维护策略，对于保障企业在云时代的稳健发展具有重要意义。

1 云计算概述

1.1 云计算定义与特点

1.1.1 云计算的概念

云计算是一种基于互联网的计算模式，它通过虚拟化技术将计算资源、存储资源和网络资源封装成一个独立的虚拟环境，专为用户提供按需使用、灵活配置的计算资源和服务。这种计算模式打破了传统IT架构中计算资源固定分配、难以扩展的局限性，实现了计算资源的高效利用和灵活调配。用户无需在本地部署大量硬件设备，只需通过互联网连接到云端，即可享受各种计算服务，大大降低了IT成本，提高了工作效率。

1.1.2 云计算的主要特点

（1）资源共享：云计算最大的特点之一是资源共享。在云端，大量的计算资源、存储资源和网络资源被封装成一个独立的虚拟环境，由多个用户共享。这种共享模式不仅提高了资源利用率，还避免了重复建设和资源浪费。用户可以根据自身需求灵活调配资源，实现按需使用。（2）按需付费：云计算采用按需付费的计费模式，用户只需为实际使用的计算资源和服务付费。这种模式极大降低了企业的初期投资成本，使得企业能够根据实际业务需求灵活调整IT支出，避免了传统IT架构中高昂的固定资产投入。（3）弹性伸缩：云计算的另一个重要特点是弹性伸缩。随着业务的发展，用户对计算资源的需求会不断变化。云计算平台能够根据用户的实际需求自动调整计算资源的规模，实现资源的弹性伸缩。这种能力使得企业能够轻松应对业务高峰期的挑战，保证业务的连续性和稳定性。（4）高可用性：云计算平台通过分布式部署、数据冗余和容灾备份等技术手段，确保用户数据的安全性和服务的可用性。即使某个节点或某个区域出现故障，也能够迅速切换到其他节点或区域，保证服务的持续运行[1]。

1.2 云计算应用领域

1.2.1 云计算在企业信息化、电子商务、大数据处理等领域的应用实例

（1）企业信息化：云计算在企业信息化领域的应用广泛。许多企业选择将ERP、CRM等核心系统迁移到云端，通过云计算平台实现资源的集中管理和高效利用。此外，云计算还为企业提供了便捷的协同办公工具，如在线会议、文档共享等，提高了员工的工作效率和企业的竞争力。（2）电子商务：在电子商务领域，云计算为电商平台提供了强大的支撑。通过云计算平台，电商平台可以轻松应对大规模并发访问和高数据量处理的需求，确保交易的顺畅进行。同时，云计算还为电商企业提供了智能化的数据分析服务，帮助企业深入挖掘用户行为数据，优化营销策略和提升用户体验。（3）大数据处理：大数据处理是云计算的又一重要应用领域。云计算平台提供了强大的数据存储和计算能力，使得企业能够轻松处理海量数据。通过云计算平台，企业可以进行复杂的数据分析和挖掘工作，发现潜在的市场机会和商业价值。此外，云计算还为企业提供了便捷的数据可视化工具，帮助企业将复杂的数据转化为直观易懂的图表和报告。

1.2.2 云计算技术带来的便利性和效益

云计算技术的引入为企业带来了诸多便利性和效

益。首先，云计算降低了企业的IT成本，使得企业能够将更多资金投入到核心业务上。其次，云计算提高了企业的工作效率和竞争力，通过提供便捷的协同办公工具和智能化的数据分析服务，帮助企业实现业务流程的优化和决策的智能化。最后，云计算还提升了企业的服务质量和用户体验，通过提供高可用性和可伸缩性的服务保障，确保用户能够随时随地享受到高效、稳定的服务。

2 云计算环境下计算机网络安全面临的挑战

2.1 数据传输与存储安全风险

（1）安全威胁分析。在云计算的广阔蓝海中，用户数据的传输与存储如同航行的双桨，驱动着服务的运行，但也暴露在风雨之中。数据传输过程中，数据如同在公开水域航行，面临多种威胁。黑客利用复杂多变的攻击手段，如网络钓鱼、数据窃听、中间人攻击等，试图拦截或篡改传输中的数据。同时，恶意软件如同海洋中的暗礁，潜伏在网络各处，等待时机感染用户设备或云服务系统，进而窃取或破坏数据。数据存储环节同样充满挑战。云服务提供商的数据中心虽然拥有先进的防护技术，但也可能因系统漏洞、配置错误或人为疏忽而暴露于风险之中。未经加密或加密不当的敏感数据，如同未上锁的宝箱，极易被不法分子轻易获取。此外，数据存储的权限管理也是一大难题，若权限设置不合理或监管不力，将直接导致数据被非法访问或滥用。（2）数据泄露和非法访问的严重性。数据泄露和非法访问的严重性如同海啸般巨大，对个人、企业和国家都可能造成无法估量的损失。个人数据的泄露可能导致身份盗用、财产损失、名誉受损等后果，严重影响个人的生活质量和社会信任度。企业数据的泄露则可能涉及商业秘密、客户资料等敏感信息，导致企业竞争力下降、经济损失惨重，甚至引发法律纠纷和信任危机。更严重的是，当政府或关键基础设施的数据被非法访问或篡改时，可能引发国家安全和社会稳定的重大问题。

2.2 云服务提供商的安全性问题

云服务提供商作为云计算的基石，其安全防护能力和策略执行至关重要。然而，现实中不乏一些云服务提供商在安全方面存在短板。首先，安全防护能力的不足可能导致其无法有效抵御外部攻击，如未能及时更新安全补丁、缺乏高级威胁检测能力等。其次，安全策略执行的不严谨也可能带来风险，如权限管理混乱、日志审计不足、应急响应机制不健全等。这些不足不仅会威胁用户数据的安全，还可能损害云服务提供商的声誉和市场份额。

2.3 用户安全意识与技能不足

在云计算的浪潮中，用户既是受益者也是参与者。然而，不少用户在使用云计算服务时却忽视了自身的安全责任。安全意识不强的用户可能随意点击来路不明的链接、下载未经验证的附件、使用弱密码等，这些行为都为黑客提供了可乘之机。同时，技能不足的用户可能无法正确配置云服务的安全设置、无法识别潜在的安全风险，从而增加了数据泄露和非法访问的风险。因此，提高用户的安全意识和技能水平是保障云计算环境安全的重要举措之一。

3 云计算环境下的网络安全维护策略

3.1 加强云服务提供商的安全能力

（1）鼓励云服务提供商加强安全体系建设。云服务提供商作为云计算服务的基石，其安全能力的高低直接影响到用户数据的安全。因此，鼓励云服务提供商加强安全体系建设是首要任务。这包括但不限于建立严格的安全政策与流程、组建专业的安全团队、引入先进的安全技术和管理工具等。通过构建全面而深入的安全体系，云服务提供商能够有效抵御外部攻击，保障用户数据的机密性、完整性和可用性。在具体实施上，云服务提供商可以借鉴国际安全标准（如ISO27001、SOC2等）来构建和完善自身的安全体系。同时，还应积极参与行业内的安全交流与合作，不断提升自身的安全防护能力[2]。（2）要求云服务提供商定期进行安全审计和漏洞扫描。安全审计和漏洞扫描是发现和修复安全隐患的重要手段。云服务提供商应定期进行全面的安全审计和漏洞扫描工作，以确保及时发现并修复系统中的安全漏洞和弱点。此外，云服务提供商还应建立快速响应机制，对于发现的安全问题能够迅速采取措施进行处置和修复。为了确保安全审计和漏洞扫描的有效性，云服务提供商可以邀请第三方专业机构进行独立的安全评估。这些机构通常具有丰富的安全评估经验和专业的技术实力，能够客观地评估云服务提供商的安全水平并提出改进建议。

3.2 采用数据加密技术

（1）数据加密技术的基本原理及其在云计算环境中的应用。数据加密技术是一种通过特定算法将明文转换为密文以保护数据机密性的技术手段。在云计算环境中，数据加密技术的应用尤为关键。通过将用户数据进行加密处理后再上传至云端进行存储或传输可以有效防止数据在传输过程中被截获或在存储过程中被非法访问。常见的数据加密技术包括对称加密和非对称加密两种类型。对称加密算法使用相同的密钥进行加密和解密操作，具有较高的加密效率和较低的计算成本；而非对称加密算法则使用一对公钥和私钥进行加密和解密操

作，具有较高的安全性和灵活性。在云计算环境中，可以根据具体应用场景和需求选择合适的数据加密技术来实现数据的保护[3]。（2）数据传输和存储过程中使用加密技术的重要性。在云计算环境下，用户数据在传输和存储过程中面临着诸多安全风险。因此，在数据传输和存储过程中使用加密技术显得尤为重要。通过使用加密技术可以确保数据在传输过程中不被截获或篡改，同时在存储过程中也能够有效防止未授权访问和数据泄露的风险。为了确保数据传输和存储的安全性，云服务提供商应提供端到端的数据加密服务。这包括在数据传输过程中采用SSL/TLS等加密协议对数据进行加密传输，以及在数据存储时采用透明数据加密（TDE）或其他先进加密技术，确保数据在云存储介质上的安全性。此外，云服务提供商还应提供密钥管理服务（KMS），允许用户对自己的加密密钥进行完全控制。这意味着用户可以将密钥存储在自己的系统中，仅在必要时将加密的数据发送到云端进行处理或分析，从而确保即使云服务提供商自身也无法解密用户数据，进一步增强了数据的安全性。

3.3 实施数据备份与恢复策略

（1）制定完善的数据备份与恢复计划。数据备份与恢复是保障业务连续性和数据可靠性的重要措施。在云计算环境下，由于数据集中存储在云端服务器上，一旦发生数据丢失或损坏，将对企业造成重大损失。因此，制定完善的数据备份与恢复计划至关重要。该计划应明确备份的频率、范围、备份介质的选择以及恢复策略和流程等关键要素。同时，还需要考虑备份数据的可访问性、可恢复性和可验证性，确保在需要时能够迅速恢复数据。（2）强调数据备份的多样性和异地性。为了提高数据的可靠性和安全性，应强调数据备份的多样性和异地性。多样性意味着采用多种不同的备份方式和备份介质来存储备份数据，以减少单点故障的风险。例如，可以将备份数据存储在本地磁盘、磁带库、云存储等多种介质上，以确保数据的冗余性和可恢复性。异地性则是指将备份数据存储在远离原数据中心的地理位置上，以应对自然灾害、人为破坏等突发事件的影响。通过异地备份，可以确保在灾难发生时，备份数据仍然可用，从而保障业务的连续性[4]。

3.4 加强用户安全教育与培训

（1）提高用户的安全意识。用户是网络安全的第一道防线。提高用户的安全意识是防范网络安全风险的重要手段之一。云服务提供商和用户组织应定期开展网络安全教育活动，向用户普及网络安全知识、网络诈骗手法和防范措施等关键信息。通过教育用户识别网络钓鱼邮件、恶意软件等常见安全风险，并教授用户如何采取相应的防范措施，可以降低用户被攻击的风险。（2）培训用户正确使用云计算服务。除了提高用户的安全意识外，还需要培训用户正确使用云计算服务。由于云计算服务的复杂性和多样性，用户在使用过程中可能会遇到各种安全问题。因此，云服务提供商和用户组织应提供详细的操作指南和培训课程，帮助用户了解云计算服务的功能和特性，掌握正确的使用方法和安全操作规范。通过培训用户正确使用云计算服务，可以避免因操作不当导致的安全问题，提高整个云环境的安全性。

结束语

综上所述，云计算环境下的计算机网络安全与维护是一项复杂而系统的工程，需要云服务提供商、企业及用户等多方共同努力。通过加强安全技术研发与应用，强化安全管理与制度建设，提升用户安全意识与技能，我们可以有效应对云计算带来的安全风险，构建起一个安全、可靠、高效的云计算生态环境。未来，随着技术的不断进步和应用的深入，云计算网络安全将面临更多新挑战，我们需保持警觉，持续创新，为云计算的健康发展保驾护航。

参考文献

[1]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.

[2]张彦林.探索云计算环境中计算机网络安全技术[J].信息记录材料,2021,22(01):179-180.

[3]吴坤星.基于“云计算”环境下的计算机网络安全分析[J].数字技术与应用,2020,38(11):166-168.

[4]曹楠.基于“云计算”环境下的计算机网络安全分析[J].计算机产品与流通,2020(11):74-75.