云计算视角下网络信息安全问题及其解决策略

邓 郁[1] 吴学飞[2]
1 国家移民管理局常备力量第二总队，云南 昆明 650214
2 中华人民共和国阿日哈沙特出入境边防检查站，内蒙古 满洲里 021400

[摘要]随着云计算的快速发展，网络信息安全问题成为云计算视角下的一个重要关注点。云计算的兴起为企业和个人带来了无数的便利和机遇，但同时也带来了潜在的安全威胁。网络信息安全的挑战涵盖了数据隐私、身份认证、访问控制以及恶意攻击等方面。为了确保云计算环境的安全性，必须采取一系列有效的解决策略。这些策略包括加强数据加密、建立强大的身份认证和访问控制机制、实施完善的监控和日志记录以及定期进行漏洞扫描和安全评估等。通过这些措施，我们能够更好地保护云计算中存储和传输的数据，维护用户的隐私和机密性，以确保云计算的可靠性和安全性。
[关键词]云计算；网络信息安全；解决策略
DOI：10.33142/sca.v6i4.9016 中图分类号：TP393.08 文献标识码：A

Network Information Security Issues and Solutions from the Perspective of Cloud Computing

DENG Yu [1], WU Xuefei [2]
1 The Second Brigade of the Standing Force of the National Immigration Administration, Kunming, Yun'nan, 650214, China
2 Arihashate Border Checkpoint of China, Manzhouli, Inner Mongolia, 021400, China

Abstract: With the rapid development of cloud computing, network information security has become an important concern from the perspective of cloud computing. The rise of cloud computing has brought countless convenience and opportunities to businesses and individuals, but at the same time, it has also brought potential security threats. The challenges of network information security include data privacy, identity authentication, access control, and malicious attacks. In order to ensure the security of cloud computing environments, a series of effective solutions must be adopted. These strategies include strengthening data encryption, establishing strong identity authentication and access control mechanisms, implementing comprehensive monitoring and logging, and conducting regular vulnerability scans and security assessments. Through these measures, we can better protect the data stored and transmitted in cloud computing, maintain user privacy and confidentiality, and ensure the reliability and security of cloud computing.
Keywords: cloud computing; network information security; solution strategy

云计算视角下的网络信息安全问题具有跨界性和共享性的特征。跨界性使攻击者能够利用一个环节的弱点来渗透整个云环境，而共享性增加了数据隔离和访问控制的复杂性。通过数据加密、访问控制、网络安全设备和监控、用户教育与培训以及备份和灾难恢复策略等措施，可以有效应对这些特征带来的安全挑战，确保云计算环境中的数据隐私、完整性和可用性。

1 云计算视角下网络信息安全问题的特征

1.1 跨界性

云计算涉及多个层面和环节，包括网络、服务器、存储和应用等。这种跨界性意味着攻击者可以利用一个环节的弱点来渗透整个云环境，从而威胁到整个系统的安全性。一方面，云计算的网络基础设施是网络信息安全的一个关键环节。网络作为云计算环境中数据传输和通信的基础，容易受到网络攻击和入侵的威胁。黑客可能通过网络入侵手段，如网络钓鱼、拒绝服务攻击和端口扫描，进入云环境并获取敏感数据或控制系统。因此，必须采取网络防火墙、入侵检测和预防系统（IDS/IPS）、虚拟专用网络（VPN）等安全措施来保护云计算网络基础设施的安全。另一方面，云计算的服务器和存储设备也是安全的关键组成部分。这些设备存储了大量的用户数据，包括个人隐私信息、商业机密和知识产权等。如果黑客能够入侵云服务器或窃取存储的数据，将会导致严重的数据泄露和隐私侵犯。因此，必须采取强大的身份认证和访问控制机制，如多因素身份认证和基于角色的访问控制（RBAC），以限制对服务器和存储设备的访问权限，并加密存储的数据以确保数据的机密性[1]。

1.2 共享性

云计算提供共享的资源和服务，多个用户可以共同使用同一基础设施和网络。然而，这种共享性增加了数据隔离和访问控制的复杂性，一旦有用户的安全出现问题，可能会影响其他用户的数据安全性，进而扩大安全风险范围。首先，数据隔离是共享性所带来的挑战之一。在云计算环境中，多个用户的数据存储在同一服务器或存储系统中。如果没有适当的隔离措施，一个用户的数据可能会被其他用户访问、修改或删除，导致数据泄露和隐私侵犯。因此，

云服务提供商必须实施严格的数据隔离机制，确保不同用户的数据被妥善隔离和保护。其次，访问控制是共享性所面临的另一个挑战。由于多个用户共享同一基础设施和网络，确保每个用户只能访问其授权的资源变得更加复杂。如果存在访问控制的漏洞或错误配置，某个用户可能会访问其他用户的数据或资源，导致潜在的数据泄露和非法操作。因此，云服务提供商需要建立健全的访问控制策略，如基于角色的访问控制（RBAC）和细粒度的权限控制，以确保用户只能访问其授权的资源和操作。

2 目前网络信息安全问题

2.1 数据隐私泄露

随着大量个人和企业数据存储在云端，数据泄露和滥用的风险也相应增加。首先，数据隐私泄露可能由黑客攻击引起。黑客可以利用各种技术手段，如网络钓鱼、恶意软件和社交工程等，获取用户的敏感信息。一旦黑客入侵云计算环境，他们可以窃取存储在云中的数据，包括个人身份信息、财务记录和商业机密等。这种数据泄露不仅对个人隐私造成严重威胁，也对企业声誉和竞争优势带来损害。其次，第三方滥用数据也是一个问题。云计算服务提供商可能会访问用户的数据，以提供服务或进行分析。然而，有时这些提供商可能会滥用数据，违反用户的隐私权。例如，他们可能将用户数据用于广告定位或与其他机构共享数据，而没有获得充分的用户授权。这种滥用行为对用户造成了隐私权的侵犯，并损害了用户对云计算的信任。

2.2 身份认证与访问控制

当前存在的身份认证与访问控制问题给云计算带来了安全风险。首先，弱密码是一个常见的身份认证问题。许多用户使用简单或容易猜测的密码，容易受到密码破解或暴力攻击。黑客可以利用弱密码入侵用户账户，从而获取敏感数据或进行未经授权的活动。其次，恶意访问和未经授权的访问是另一个关键问题。攻击者可能通过冒充合法用户的身份或使用盗取的凭据，进入云环境并获取敏感信息。此外，内部威胁也是一个考虑因素，员工滥用访问权限可能导致数据泄露或未经授权的数据操作。

2.3 恶意攻击威胁

恶意攻击威胁是云计算环境中一个日益严峻的问题，涉及各种恶意行为和攻击手段，对云计算基础设施和用户数据造成严重威胁。首先，网络病毒和恶意软件是恶意攻击的常见形式。黑客通过在云计算环境中植入恶意软件或病毒，能够远程控制系统、窃取敏感数据，甚至将系统感染传播给其他用户。这些恶意软件和病毒可能以虚假软件更新、欺骗性的电子邮件附件或恶意网站等形式传播。其次，勒索软件攻击也是一种严重的威胁。黑客通过加密用户数据，并要求支付赎金才能解密，使用户面临数据丢失和业务中断的风险。勒索软件攻击对个人和企业而言都具有巨大的经济和声誉损失。另外，分布式拒绝服务（DDOS）攻击是恶意攻击的另一个常见形式。攻击者通过控制大量的僵尸计算机或网络设备，向目标服务器发送大量的请求流量，以过载目标系统的资源，导致正常用户无法访问服务。这种攻击对云计算基础设施造成了严重的可用性和性能问题[2]。

3 云计算视角下网络信息安全问题的解决策略

3.1 数据加密与访问控制

数据加密与访问控制是云计算环境中保护数据隐私和控制数据访问的重要措施。首先，数据加密是通过使用密码算法将数据转换为密文的过程，以保护数据在存储和传输过程中的机密性。在云计算中，数据通常以加密形式存储在云服务器上。这确保即使黑客获取了存储介质，也无法解读数据内容，因为只有持有正确的解密密钥才能还原数据。加密可以采用对称密钥加密或非对称密钥加密，具体取决于数据的安全需求和应用场景。其次，访问控制是一种控制用户对数据和资源访问权限的机制。在云计算环境中，需要建立严格的访问控制策略，以确保只有经过授权的用户才能访问数据。这可以通过身份认证、授权和权限管理来实现。身份认证涉及验证用户的身份信息，通常通过用户名和密码、生物特征、令牌等进行。授权确定用户可以访问的资源和操作权限。权限管理确保只有合法用户获得适当的权限，并随着用户角色或职责的变化进行及时调整。再次，在数据加密方面，应使用强大的加密算法和安全的密钥管理机制。加密应在数据传输和数据存储的过程中进行，确保数据在云计算环境中的安全性。此外，还可以采用端到端加密来保护数据在客户端和云服务提供商之间的传输过程中的机密性。最后，对于访问控制，应采用最小权限原则，即为用户分配最低必要权限，以减少潜在的滥用和风险。基于角色的访问控制（RBAC）是一种常见的策略，通过将用户分配到不同的角色，并给予相应的权限来管理访问控制。此外，多因素身份认证（MFA）也应用于增强访问安全性，结合密码和其他身份验证因素（如指纹、OTP）进行认证[3]。

3.2 网络安全设备和监控

网络安全设备和监控是保护云计算环境免受恶意攻击的关键措施。它们有助于实时检测和防范潜在的安全威胁，并提供及时响应和应对措施。首先，网络安全设备包括防火墙、入侵检测和预防系统（IDS/IPS）、安全网关等。防火墙作为云计算网络的第一道防线，可以监控和控制数据流量，过滤潜在的恶意流量。IDS/IPS 可以通过监视网络流量和行为，检测并阻止入侵行为，如异常流量、病毒攻击、网络扫描等。安全网关充当云计算环境与外部网络之间的安全网关，监控和管理网络通信，并提供额外的安全功能，如访问控制、反病毒扫描、URL 过滤等。其次，监控是及时发现和应对潜在安全威胁的重要手段。通过实施实时监控和日志分析系统，可以检测和分析异常事件、攻击行为和安全漏洞。监控系统可以监视网络流量、日志

数据、异常活动和安全事件，提供实时警报和通知，使安全团队能够迅速采取措施，应对威胁。最后，网络安全监控还包括行为分析和异常检测。通过分析网络和用户行为模式，监测异常活动，如大规模数据传输、异常访问行为等，能够及早发现并阻止潜在的安全攻击。此外，监控还应包括日志记录和审计功能，记录所有的网络活动和访问日志，用于溯源和安全事件的后期调查。另外，除了部署网络安全设备和监控系统，定期更新和维护这些设备和系统也至关重要。安全设备和监控系统应保持最新的安全规则、签名和软件版本，以应对新型威胁和漏洞。

3.3 用户教育与培训

通过增强用户的安全意识和培训他们正确的安全行为，可以减少人为失误和安全漏洞的风险，增强整个云计算环境的安全性。首先，用户教育的目标是提高用户对网络信息安全重要性的认识。用户应了解网络威胁的类型、常见的攻击方式，以及这些威胁对个人和组织造成的潜在风险。教育用户如何保护自己的身份和敏感信息，如何识别和避免网络钓鱼、恶意软件和社交工程等常见的网络攻击手段。其次，用户培训应重点关注正确的身份认证和访问控制行为。用户应被教育如何创建和管理强密码，以及不与他人共享密码。教育用户多因素身份认证的重要性，并指导他们正确地使用双因素身份验证等额外安全层。此外，用户还应了解授权和权限管理的原则，遵循最小权限原则，并知晓如何使用授权工具和设置权限以限制对敏感数据和资源的访问。再次，教育用户识别和处理垃圾邮件、恶意附件和欺诈性链接也是重要的。用户应了解典型的社交工程手段，例如虚假电子邮件、电话诈骗和钓鱼网站，以及如何避免成为这些攻击的受害者。同时，用户还应掌握安全浏览和下载文件的最佳实践，避免从未知或不可信的来源获取软件或文件。最后，持续的用户培训和更新也是至关重要的。网络威胁和攻击手段不断演变，因此用户培训应定期更新，以跟上新兴的安全威胁和最佳实践。定期进行模拟演练和安全意识活动，如网络钓鱼模拟和安全测试，可以帮助用户提高对威胁的警觉性和应对能力。

3.4 备份和灾难恢复策略

备份和灾难恢复策略是云计算环境中保护数据完整性和业务连续性的重要措施。它们旨在应对数据丢失、系统故障、安全漏洞和自然灾害等不可避免的情况，确保数据能够快速恢复和业务能够持续运行。首先，定期备份数据是保护云计算环境的关键步骤。通过定期备份数据，可以将数据复制到独立的存储媒介中，以防止数据丢失和破坏。备份数据应该存储在离线和安全的位置，远离潜在的威胁和风险。同时，备份数据的完整性和可恢复性应进行定期验证，以确保备份的数据是可用的。其次，灾难恢复策略旨在应对灾难性事件，如系统故障、网络中断、恶意攻击和自然灾害等。灾难恢复策略包括紧急预案和恢复计划。紧急预案应规定在灾难事件发生时的紧急响应步骤和责任分工。恢复计划则指导在灾难发生后的数据和系统恢复过程，包括数据备份的还原、系统配置的重新部署以及业务功能的恢复。再次，备份和灾难恢复策略的有效性需要定期测试和演练。定期进行恢复演练，模拟灾难情景，并验证备份数据的可恢复性和恢复时间。通过这些测试，可以及时发现和纠正潜在的问题，确保备份和恢复过程的可靠性和高效性。最后，为了确保有效的备份和灾难恢复策略，需要考虑以下几个关键因素。备份策略应根据数据的重要性和敏感性进行分类，并根据不同的需求和业务目标制定相应的备份频率和保留期限。关键数据和系统应采用更频繁的备份，并保留较长时间以应对数据历史的需求。此外，备份数据应采用不同的存储介质和位置，以提供冗余和可靠性。备份数据的存储位置应遵循地理分布原则，远离主要数据中心和潜在的灾难风险区域[4]。

4 结束语

在云计算的时代，网络信息安全问题日益凸显。通过数据加密、访问控制、网络安全设备与监控、用户教育与培训以及备份和灾难恢复策略等措施，我们可以更好地保护云计算环境中的数据和系统安全，确保用户的隐私和机密性，实现云计算的可靠性和可信度。然而，安全是一个不断演化的挑战，我们需要持续关注和采取切实有效的安全措施，以应对日益复杂的威胁和攻击。只有通过共同努力和不断创新，才能构建一个安全可靠的云计算环境，为用户提供安全的数字化体验。

[参考文献]

[1]何栋.云计算视角下网络信息安全问题及其解决策略[J].数字通信世界,2022(11):194-196.
[2]李鸣雷.云计算环境下网络信息安全技术发展研究[J].科技创新与应用,2022,12(36):170-173.
[3]李昂.云计算环境下网络信息安全技术发展探究[J].网络安全技术与应用,2022(7):61-63.
[4]程大勇.云计算网络信息安全防护体系构建研究[J].佳木斯职业学院学报,2022,38(8):53-55.

作者简介：邓郁（1984.8—）女，广东中山人，汉族，本科学历，国家移民管理局常备力量第二总队，警务技术二级主管（副高），长期从事通信技术教学研究工作；吴学飞（1985.1—）男，内蒙古兴安盟人，汉族，本科学历，中华人民共和国阿日哈沙特出入境边防检查站警务技术二级主管（中级），长期从事网络通信技术工作。