云计算背景下计算机安全问题及对策

孙莹莹
新疆天山职业技术大学　新疆　乌鲁木齐　830017

摘　要：随着云计算技术的迅速发展，其在各行各业的应用日益广泛。然而，云计算环境下的计算机安全问题也日益凸显，包括数据泄露、隐私侵犯、虚拟化安全威胁等。本文首先概述了云计算的定义、特点及其服务模式和部署模式，随后深入分析了云计算背景下计算机安全面临的主要问题，并在此基础上提出了针对性的安全对策，旨在保障云计算环境下的数据安全与隐私保护。

关键词：云计算；计算机安全；对策

引言

云计算作为信息技术的重要组成部分，正深刻改变着企业的运营模式和个人的生活方式。然而，随着云计算应用的不断深入，其面临的安全挑战也日益严峻。如何在享受云计算带来的便利的同时，有效保障数据安全和个人隐私，成为当前亟待解决的问题。本文将从云计算技术的基本概念入手，研究其中存在的安全风险，并给出具体的破解策略。

1 云计算概述

云计算，这一基于互联网的创新计算方式，正引领着信息技术的变革。它通过网络，为用户提供动态、可扩展、虚拟化的资源，极大地提升了计算的灵活性和效率；云计算的核心特点在于其按需自助服务的能力，用户可以根据实际需求，随时获取所需的计算资源，而无需进行繁琐的前期准备；广泛的网络访问使得用户可以通过各种设备，随时随地访问云计算服务，实现了真正的移动计算。资源池化是云计算的另一大特点，它将大量的计算资源汇聚成一个巨大的“资源池”，用户可以根据需要从中获取资源，而无需关心资源的具体位置和管理细节，这种模式极大地提高了资源的利用率和灵活性。快速弹性则是云计算应对突发需求变化的重要能力，它可以迅速扩展或收缩资源，以满足用户的实际需求；最后，按使用量计费使得用户只需支付实际使用的资源费用，降低了计算成本，提高了经济效益。云计算的服务模式丰富多样，主要分为设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）；这些服务模式为用户提供了从基础设施到应用软件的全方位服务，满足了不同用户的需求。而根据云计算的部署模式又分为公共云、私人云和混合云，客户可按照实际需要选用合适的部署模式，以实现更加灵活、高效的计算服务[1]。

2 云计算背景下的计算机安全问题

2.1 数据安全问题

（1）数据泄露是云计算环境中一个严重的安全隐患。由于数据集中存储和处理，一旦云服务商的安全防护措施不到位，或者存在内部人员恶意泄露的情况，就可能导致大量敏感信息的非法获取和滥用。（2）数据篡改也是云计算环境下面临的一个重要问题。在数据传输、存储或处理的过程中，如果攻击者能够利用安全漏洞进行非法访问，就有可能对信息实施非法修改，致使信息的完整性和真实性受到破坏。（3）数据丢失也是云计算环境下不容忽视的安全风险。云服务商的存储设备或网络设施一旦出现故障，或者遭受天灾等不可抗力原因的影响，也可以造成资料的永久性损失，对使用者造成不可估量的伤害。

2.2 隐私泄露问题

（1）云服务商可能未经用户明确同意，就擅自使用或泄露用户的私人信息。这种行为严重侵犯了用户的隐私权，可能导致用户的敏感信息被不法分子利用，进而引发身份盗窃、金融诈骗等严重后果。（2）云计算环境中的隐私泄露还可能源于不安全的数据传输和存储。如果云服务商没有采取足够的安全措施来保护用户数据，那么黑客或其他恶意攻击者就有可能通过渗透云系统、窃取传输中的数据或破解存储的加密信息来获取用户的私人信息。（3）隐私泄露问题还可能因为云服务商的内部管理不善而加剧。例如，员工可能未经授权就访问用户数据，或者将用户信息泄露给外部人员；这种内部泄露往往难以察觉和防范，给用户的隐私安全带来极大威胁。

2.3 虚拟化安全问题

（1）虚拟机逃逸是虚拟化环境中一个严重的安全威胁。如果攻击者能够利用虚拟机软件的漏洞或配置错误，就有可能突破虚拟机的隔离边界，进而攻击宿主机

或其他虚拟机，造成整个云计算环境的崩溃。（2）虚拟化软件漏洞也是不容忽视的安全风险。虚拟化软件作为云计算的底层支撑，其安全性直接关系到整个云计算环境的稳定；但由于虚拟化软件的复杂性，难免存在漏洞和缺陷，这些漏洞一旦被攻击者利用，就可能对云计算环境造成严重的破坏。（3）虚拟化环境的管理和配置也可能引发安全问题。如果管理员对虚拟化环境的配置和管理不当，就可能为攻击者提供可乘之机，进而引发一系列的安全事件[2]。

3 云计算安全对策

3.1 数据加密技术

在云计算安全对策中，数据加密技术占据核心地位；它通过对保存和发送的信息进行保密管理，保证即便信息被非法获取，也无法被未授权的第三方解读，从而有效保护数据的机密性和完整性。（1）对称加密是一个很古老的信息加密技术，它通过对称的加密方式对信息进行了保密和解码。这种加密方法速率较快、效率高，很适合于进行大数据的加密；但对称加密的密钥管理是一个挑战，因为所有参与方都需要共享相同的密钥。为缓解这种矛盾，非对称密码理论应运而生。（2）非对称密码必须采用一对钥匙：公钥与私钥。公钥用来保密数据，而私钥则用来解密；这种加密方式的安全性更高，因为即使公钥被泄露，私钥也能保持安全；非对称加密适用于需要高度安全性的场景，如数字签名和身份验证。（3）除了对称加密和非对称加密，同态加密也是一种重要的加密技术。同态加密允许在加密的数据上执行计算，而无需先解密数据；这意味着云计算服务商可以在不暴露用户数据的情况下，对数据进行处理和分析；同态加密在保护用户隐私的同时，也实现了数据的可用性和可计算性。（4）在云计算环境中，数据加密技术的应用需要综合考虑多个因素。第一，加密算法的选择应根据数据的敏感性和处理需求进行，对于高度敏感的数据，应使用更强的加密算法和密钥管理策略；第二，加密技术的实施需要与其他安全措施相结合，如访问控制、身份认证和监控等，以形成多层次的安全防护体系；第三，云计算服务商应定期评估和改进其加密技术，以适应不断变化的安全威胁和法规要求。

3.2 访问控制策略

在云计算安全对策中，访问控制策略扮演着至关重要的角色。其核心目标是确保只有经过授权的用户才能访问特定的资源，从而有效防止未经授权的访问和数据泄露；为了实现这一目标，基于角色的存取控制（RBAC）和基于属性的访问控制（ABAC）就形成了2个广泛应用的技术。（1）RBAC技术是一种将访问权限与用户在组织中的角色相关联的方法。在这种策略下，用户根据其担任的角色获得相应的访问权限；例如，系统管理员可能拥有对所有系统资源的访问权限，而普通用户则可能仅限于访问其工作所需的数据；RBAC策略的优势在于其易于管理和扩展，因为新用户可以根据其角色快速获得适当的访问权限。（2）相比之下，ABAC策略则更加灵活和动态。它根据用户的属性（如职位、部门、项目等）和资源属性（如敏感级别、数据类型等）来授予访问权限；ABAC策略能够更精细地控制访问权限，因为它考虑了更多的上下文信息；例如，一个项目经理可能只被允许访问与其负责的项目相关的数据，即使他/她拥有较高的职位。（3）在云计算环境中，访问控制策略的实施需要综合考虑多个因素。第一，策略的制定应根据组织的业务需求和安全要求进行，以确保访问控制的合理性和有效性；第二，策略的实施需要与其他安全措施相结合，如身份验证、数据加密和监控等，以形成多层次的安全防护体系；第三，云计算服务商还应提供灵活的访问控制机制，以支持用户根据实际需求自定义访问策略[3]。

3.3 安全审计与监控

在云计算安全对策中，安全审计与监控是确保云环境持续安全的关键环节；这一策略通过日志分析、异常检测和实时监控等手段，对云计算环境进行全面的安全审计和监控，旨在及时发现并应对潜在的安全威胁。（1）日志分析是安全审计与监控的基础。云计算系统会生成大量的日志数据，包括系统操作、用户访问、资源使用等信息；通过对这些日志数据进行深入分析，可以识别出异常行为、潜在的安全漏洞以及未授权的访问尝试；日志分析还可以协助安全团队理解攻击者的活动方式，以便提出更加合理的防护对策等。（2）异常检测是安全审计与监控的另一个重要手段。它通过分析云计算环境中的网络流量、系统调用、用户行为等数据，识别出与正常模式不符的异常行为；这些异常行为可能表明存在安全威胁，如恶意软件感染、数据泄露或未授权的访问；一旦发现异常行为，安全团队可以立即采取行动，防止安全事件进一步恶化。（3）实时监控是确保云计算环境持续安全的关键。通过实时监控云计算系统的运行状态、网络流量、用户活动等信息，可以及时发现潜在的安全风险，并采取相应的处理对策；实时监控还可以帮助安全团队了解云计算环境的整体安全状况，以便及时调整安全策略，提高防御能力。（4）为了实施有效的安全审计与监控，云计算服务商需要建立完善的

安全管理制度和流程，确保日志数据的完整性、准确性和可追溯性；安全团队还需要具备专业的安全知识和技能，能够熟练运用各种安全工具和技术，对云计算环境进行全面的安全审计和监控。

3.4 身份认证技术

在云计算安全对策中，身份认证技术占据着举足轻重的地位。它是确保用户身份真实性和可靠性的关键手段，对于防止未授权访问和数据泄露具有重要意义；为了实现这一目标，多因素验证和生物指纹识别等新型的身份验证技术被广泛应用于云计算环境中。（1）多因素认证是一种结合多种验证方式的身份认证方法。它通常包括用户所知道的（如密码、PIN码）、用户所拥有的（如手机、智能卡）以及用户所特有的（如指纹、面部特征）等因素。通过结合这些因素，多因素认证能够提供更高级别的安全保障，因为即使攻击者获取了用户的密码，也无法在没有其他验证因素的情况下访问用户的账户。（2）生物识别技术则是另一种先进的身份认证技术。它利用人类的生物特征，如指纹、面部、虹膜、声纹等，进行身份验证；生物指纹识别功能拥有高度的独特性和稳定性，因此能够提供更为可靠的身份认证；在云计算环境中，生物识别技术可以用于用户登录、数据访问、交易验证等多个场景，有效防止身份冒用和非法访问。（3）为了实施有效的身份认证技术，云计算服务商需要采用先进的加密技术和安全协议，保证了用户身份信息的传递和存储过程中的信息安全；还必须设置严密的身份验证过程和制度，对用户身份信息实施全面的认证和审查，保证了只有合格用户才可以访问云计算资源。（4）云计算服务商还应定期评估和改进其身份认证技术，以适应不断变化的安全威胁和技术发展；还应提供灵活的身份认证机制，以支持用户根据实际需求选择适合的身份验证方式[4]。

3.5 虚拟化安全技术

在云计算领域，虚拟化技术作为核心支撑，极大地提升了资源的灵活性和利用率；但随着虚拟化环境的广泛应用，其安全性问题也日益凸显。为了应对这一挑战，虚拟化安全技术应运而生，它通过虚拟机隔离和虚拟化软件安全补丁等手段，显著加强了虚拟化环境的安全防护能力。（1）虚拟机隔离是虚拟化安全技术的重要一环。它通过在虚拟化层实现严格的隔离机制，确保不同虚拟机之间的资源和数据无法相互访问，从而有效防止了虚拟机逃逸等安全威胁；这种隔离机制不仅保护了虚拟机的操作系统和应用程序，还确保了虚拟机之间的网络通信和数据传输的安全性。（2）虚拟化软件安全补丁也是虚拟化安全技术的重要组成部分。由于虚拟化软件的复杂性，难免存在漏洞和缺陷。这些漏洞一旦被攻击者利用，就可能对虚拟化环境造成严重的破坏；于是，云计算服务商需要定期发布虚拟化软件的安全补丁，及时修复已知漏洞，提高虚拟化环境的整体安全性。（3）在实施虚拟化安全技术时，云计算服务商还需要考虑其他相关因素。例如，他们需要确保虚拟化环境的配置和管理符合最佳安全实践，以防止因配置错误或管理不当而引发的安全问题；还需要对虚拟化环境进行定期的安全审计和漏洞扫描，以便及时发现并应对潜在的安全威胁。

结语

云计算，作为信息技术领域的一颗璀璨明珠，其发展与应用无疑为各行各业带来了前所未有的变革与机遇。然而，伴随其广泛应用的同时，安全问题也日益凸显，成为不容忽视的挑战。本文通过深入剖析云计算所面临的主要安全问题，并提出了一系列具有针对性的安全对策，旨在为云计算的安全应用提供有益的参考与指导。展望未来，我们有理由相信，随着技术的不断革新与完善，云计算的安全防护体系将更加坚不可摧，为各行各业的数字化转型之路铺设更加坚实的安全基石。

参考文献

[1]陈晓煦.计算机网络工程安全问题及其对策[J].电子技术与软件工程,2020(06):194[2019-04-30].

[2]范兴亮.探究计算机网络工程安全问题与解决策略[J].数码世界,2020(09):222-223.

[3]盛丹丹.基于云计算环境下计算机网络安全问题的思考.电脑知识与技术,2020,14(14):31-32

[4]王若镔.基于云计算环境下的计算机网络安全问题研究.数码设计（上）,2020(10):27-29.