云计算下的信息安全问题与解决方案分析

高健凯[1] 岳 翔[2] 李冰冰[3]
1. 曙光云计算集团股份公司 天津 300000
2. 南京城市云计算中心有限公司 南京 210000
3. 曙光云计算集团股份公司 天津 300000

摘 要：云计算作为一种基于互联网的计算模式，集中管理和共享资源，但也带来了严峻的信息安全挑战。为应对这些挑战，需建设完善的安全架构体系、安全管理体系和人员能力保障等措施。同时，构建全面的安全监控与漏洞管理，完善应急响应与恢复机制也至关重要。通过综合应用这些解决方案，可以有效保障云计算环境下的信息安全。

关键词：云计算；信息安全；问题；解决方案

1 云计算安全概述

云计算是将计算资源、存储空间和应用程序等服务通过互联网提供给用户，实现了对资源的集中管理和共享利用。云计算模式的出现极大地促进了各行各业的数字化转型和业务创新，但同时也带来了严峻的信息安全风险。首先，当用户将业务和数据迁移到云计算环境时，大量的数据和应用程序被集中存储和处理，形成了数据集合，这样集中化的特性使得云计算环境成为了攻击者的主要目标。攻击者会利用各种手段，如网络攻击、数据泄露、恶意软件等，来窃取或破坏云平台中的数据，从而存在给企业带来巨大的损失的风险。其次，用户业务上云后，将对业务数据失去了管理与控制权，无法自主采取有效安全措施来保障数据的安全性，容易导致数据泄露风险。另外，云计算的分布式和虚拟化特性也为安全管理带来了新的难度。在分布式的云计算环境中，数据和应用可能跨越多个物理和逻辑边界，增加了管理和监控的复杂性[1]。最后，虚拟化技术将资源的动态分配和管理变得更加灵活的同时，也带来安全隔离失效和资源滥用的可能性。

2 云计算背景下面临的信息安全问题

2.1 数据安全问题

云服务模式会集中存储和处理大量的数据，一旦云计算平台遭受恶意攻击或发生故障，就可能导致大量敏感数据的泄露或丢失，对个人和组织将造成不可预计的损失。

2.2 恶意攻击威胁

恶意攻击是对数据安全构成严重威胁的外部因素之一。（1）黑客攻击：黑客会利用0day漏洞、SQL注入、XSS（跨站脚本攻击）、XXE（XML外部实体拓展攻击）非法入侵云计算平台，窃取、篡改或删除敏感数据。（2）病毒和恶意软件攻击：云计算平台常遭受勒索病毒攻击和挖矿病毒感染。勒索病毒攻击是一种通过锁定云平台系统或文件，会对系统或文件进行加密锁定，即使支付赎金，也无法保证文件数据的恢复。挖矿病毒是一种通过在计算机中运行特定算法来消耗计算资源并产生加密货币的恶意软件，会对云平台的计算资源和存储资源造成严重的消耗，以及数据丢失泄露等风险。（3）DDoS攻击：分布式拒绝服务（Distributed Denial of Service）攻击通过控制大量僵尸主机，向受害系统发送无用的请求流量，以拥塞云计算服务的带宽和资源，会导致企业的重要数据和应用程序无法访问，造成业务中断风险[2]。（4）钓鱼攻击：是社会工程学攻击一种，攻击方式通常是伪装成合法来源的电子邮件或消息，诱骗用户点击恶意链接或下载恶意附件，一旦用户点击触发，攻击者就可获取用户的登录凭证或其他敏感信息，进而访问云服务业务系统和关键数据。

2.3 身份认证问题

云服务商可能存在对内部人员或服务外包人员数据访问权限管控不到位的情况，可能导致敏感数据泄露给未经授权人员。其次，薄弱的身份认证机制也是云计算环境中普遍存在的问题。许多云计算服务提供商在身份验证方面仅使用用户名和密码的传统方式，这种方式容易被攻击者利用。此外，云服务商虽然实施多因素身份验证机制，但安全组织建设不完善，未能实现专人专岗，安全机制落地执行困难。

2.4 供应链安全问题

云计算平台是通过计算、网络、存储、安全设备和软件系统协同集成而成。云计算平台的持续稳定运行需要安全的供应链体系保障。随着供应链全球化的发展，云计算供应链生态变得逐渐复杂，存在供应商突发暂停

提供维护服务和产品供应的风险。

3 云计算下信息安全问题的解决方案

3.1 数据加密与保护

云计算中实现数据加密与保护需要采取一系列的策略和措施。首先，数据加密是确保数据在存储和传输过程中不被非法访问或篡改的关键。采用强加密算法，如AES-256或RSA，对数据进行加密处理，可以确保数据在云端存储时的安全性。同时，对于数据的传输过程，应使用SSL/TLS等安全协议进行加密，防止数据在传输途中被截获。其次，为了实现对敏感数据的有效保护，可以实施访问控制机制。通过基于角色的访问控制（RBAC）或属性基础的访问控制（ABAC），可以确保只有经过授权的用户或应用程序才能访问特定的数据资源。另外，对于数据的操作行为，如读取、写入、删除等，应建立审计和监控机制，及时发现并应对异常行为[3]。数据脱敏技术也是保护敏感数据的有效手段，通过对敏感数据进行脱敏处理，即将数据的实际值替换为随机生成的值，可以降低数据泄露的风险。

3.2 防范恶意攻击威胁

首先，加强网络安全防护是关键，通过部署先进的防火墙、入侵检测系统（IDS）和网络安全监控工具，能够实时检测并防御来自外部的恶意攻击。其次，为了提高身份验证的安全性和可靠性，应采用多因素身份验证技术，如动态令牌和指纹识别等，从而降低黑客攻击的风险。另外，防范勒索病毒和挖矿病毒的防范，需定期更新和修补系统漏洞，加强防病毒软件的监控和防御能力，确保能够及时发现并清除这些恶意软件。防御分布式拒绝服务（DDoS）攻击同样重要，通过配置高性能的抗DDoS设备或流量清洗服务，可以提升云计算平台的抗攻击能力，确保服务的稳定性和可用性。最后，为了防范钓鱼攻击，需要加强用户教育和培训，提高用户对钓鱼邮件和恶意链接的识别和防范能力，并实施邮件过滤和链接检查机制，以防止恶意链接和附件的传播。

3.3 强化访问控制和身份认证

根据业务需求和安全要求，对不同的人员和角色按照最小权限原则实施配置。对不同职责的人员赋予相应的权限，实现细粒度的访问控制。除了传统的用户名和密码认证方式外，引入动态令牌、生物特征识别等技术，提高身份认证的安全性和可靠性。同时，对不同安全级别的访问要求采用不同的身份认证方式，例如双因素认证或多因素认证，增加非法访问的难度。随着云计算的发展，越来越多的业务逻辑通过API接口实现。因此，要对API接口进行严格的安全管理和控制，确保API接口的安全性和可靠性。采用API网关进行统一管理和控制，对API请求进行身份认证、权限校验和数据加密等处理。对用户的访问行为和操作进行记录和监控，及时发现异常行为和安全事件。最后，相对传统边界安全理念零信任一种新的网络安全架构，网络中心化转变为身份中心化，将防护重点转移到身份管理和建立更细粒度的访问控制策略[4]。

3.4 加强供应链的保护

为了加强供应链的保护，并降低潜在的风险，需要确保所采购的计算设备、网络设备、存储设备、安全设备和软件都经过严格的筛选和审核。明确采购产品必须经过第三方权威认证，这是确保产品质量和安全性的关键步骤。通过与权威认证机构合作，能够验证产品是否符合国家和国际的安全标准，并评估其可能存在的安全隐患。在采购过程中，一旦发现任何安全隐患，应立即采取行动，明确应对措施，可能涉及到与供应商协商解决问题，或寻找替代产品和解决方案。通过与供应商建立紧密的合作关系，可以更好地了解产品的供应链安全状况，及时防范供应链风险。

3.5 安全架构体系建设

在云计算环境下，构建一个全面、高效且稳固的安全架构体系是保障信息安全的核心所在。该体系以网络架构为基础，通过设计多层次、高冗余的网络布局，结合负载均衡、漏洞扫描、安全资源池、防火墙和入侵检测等技术手段，确保服务的高可用性、网络边界和虚拟机的安全。同时，制定全面的安全防护策略，涵盖定期更新与补丁管理、强制访问控制、身份验证以及安全审计和云灾备机制，保障业务安全性和连续性。这样构建的技术导向安全架构体系，不仅全面保护云计算环境的数据安全和服务稳定性，还具备足够的弹性和可扩展性，灵活应对不断变化的安全威胁和业务需求。

3.6 安全组织与人员管理

面对复杂的云计算架构和不断演进的网络威胁，仅仅依赖技术防护是不够的，更需要完善的安全组织和人员安全意识提升。建立信息安全组织是落实信息安全工作的第一步，一般信息安全组织分为三层，包括安全决策层、安全管理层和安全执行层。安全管理层负责信息安全具体工作管理，对安全决策层的决策推动执行层落地。信息安全管理层设计年度安全培训计划，应注重提升在虚拟化、云架构、云存储、云灾备、云安全规范等方向的安全意识。除了传统的现场培训和在线学习，还可以利用云计算平台的特点，开展渗透测试和应急演练，让员工在真实的安全场景中学习如何应对威胁，有效提升组

织的应急响应能力。安全意识培训不仅要在新员工入职时进行，更应作为一项长期的工作来持续推进。

4 云计算下的信息安全管理和实践

4.1 完善安全策略和安全规范

为确保云计算服务安全稳定，构建一个全面高效的信息安全体系至关重要。该体系不仅注重技术层面的防护，更强调管理、流程和审批等制度建设。需明确安全目标、责任分工和应急响应机制，确保安全策略和流程得以有效执行。制定详细的安全管理体系，明确各级人员职责，设立专门的安全合规审计团队进行监督和执行，促进安全策略落地。建立应急响应领导小组，不断更新应急预案，在安全事件发生时能迅速采取有效行动，减轻损失和风险。建立严格的身份认证和访问控制管理要求，确保仅授权用户和系统可访问和操作数据。建立完善的日志审计系统，记录所有操作和行为，以追踪和调查潜在安全风险。健全安全监控和预警机，部署专业安全监控设备和系统，实时监控网络流量、系统日志和用户行为，发现异常和可疑行为并及时预警，采取相应措施[5]。

4.2 强化漏洞管理

定期的漏洞扫描和评估能够迅速识别系统中的安全漏洞，而及时的漏洞修复工作则能有效防止恶意攻击者利用这些漏洞。在发现安全事件或漏洞时，组织应建立快速响应机制，确保相关专业团队能够迅速介入，采取有效措施隔离受影响的系统或资源，并启动应急预案以降低安全事件对业务的影响。通过持续的安全监控和漏洞管理，组织能够在云计算环境中构建一道坚实的安全防线。

4.3 建立应急响应与恢复机制

在云计算环境中，由于系统的复杂性和动态性，安全事件和故障难以完全避免。因此，建立完善的应急响应和恢复机制对于业务连续性至关重要。这要求组织首先建立明确的应急响应流程和责任分工，确保在安全事件发生时能够迅速启动应急计划，采取有效措施应对。同时，定期的应急演练和评估也是必不可少的，通过模拟真实场景检验应急响应预案的有效性，发现并改进潜在的问题和缺陷。在恢复措施方面，组织应提前制定详细的恢复计划，包括数据备份、系统恢复、紧急安全配置变更等步骤，以确保在安全事件或故障发生后能够迅速恢复服务和系统的正常运行。通过不断完善和优化应急响应与恢复机制，组织能够在面临安全挑战时保持冷静、高效应对，最大程度地保护数据和资源的安全。

结束语

通过理解和分析云计算下面临的信息安全问题，并采用相应的解决方案，可以有效保护数据和资源的安全。云计算下的信息安全管理是一个持续的过程，要不断地适应和更新，以确保信息系统的安全性和可用性。只有充分认识和重视信息安全，加强对安全威胁识别防范和安全风险评估管理，才能保障云计算下的信息安全。

参考文献

[1]赵凯,何文海,阎冰冰.云计算下的信息安全问题与解决方案分析[J].中国新通信,2019,21(1):64.DOI:10.3969/j.issn.1673-4866.2019.01.051.

[2]刘小磊,宋玉龙,梁希望.云计算下网络信息安全问题与解决对策分析[J].电子世界,2020(09):176-177.

[3]张激.云计算技术在计算机数据处理中的应用及其发展对策[J].信息与电脑（理论版）,2019(08):24-25.

[4]赵靖雯,陆雨韬,万志涛,肖俊宇.零信任数字政府网络安全防护体系研究[J].网络安全技术与应用,2024(03):90-94.

[5]侯双双,陈莉,郭伟.云计算技术下的企业信息安全技术探讨[J].中国新通信,2020,22(18):139-140.