云计算下的网络安全技术研究

赵坚 罗亚丽

四川大学锦城学院 计算机与软件学院 四川 成都 611731

【摘 要】：在信息化时代下计算机网络安全技术备受瞩目,而云计算的快速发展将给计算机网络安全带来了更加复杂的环境。分析云计算下计算机网络安全技术,有利于进一步保障计算机网络安全。为此，本文对云计算环境中出现的计算机网络安全问题进行了分析和研究，并提出构建云计算安全体系的策略，为解决当下网络安全所出现的问题提供解决途径，从而更好的促进计算机网络安全的健康发展。

【关键词】：云计算；计算机；网络安全

1 引言

随着信息科学技术的快速发展，云计算在各行各业得到了广泛的应用。在云计算技术迅速崛起背后，网络安全防护形势也愈来愈严峻。新兴技术的发展也使得网络攻击行为也变得更加复杂和隐蔽，企业和个人资料信息被恶意攻击和窃取。可见，有效并且正确的利用网络安全技术，促进网络安全健康发展，有着不可忽视的力量。

2 云计算下网络安全的意义

在云计算环境下，计算机网络的数据信息安全与网络安全技术的有效利用息息相关。使用者可以采取积极的措施和相关技术，对共享信息和数据进行保护，防止在工作中信息数据被泄露。

2.1 数据的安全得到保障

云端存储与传统存储相比较，传统存储设备提供的是容器即一个存储空间，数据直接存放存在上面，安全性和隐私性都极其低[1]。当计算机网络出现安全漏洞时，网络黑客、不法分子就可以很轻松的进行入侵并盗取该设备的重要信息，造成用户机密数据信息的丢失和泄露，给用户带来巨大损失。虽然云存储实际也是存在硬件存储设备中的，但是云存储中的数据传输是经过加密处理的，这样就降低了数据被泄漏的风险。数据的存储方式是按照文件块来进行存储的，只有用户有权限进行访问和管理，我们无法直接对其进行访问。

总的来说数据安全主要是分为两个部分即数据的存储以及传输安全性，这里面包括数据的机密性、完整性和可用性。针对数据安全的这三个方面，云计算通过数据加密、多重身份资格认证、访问权限控制、安全日志和审计等手段可以充分保障数据的安全性。

2.2 提高信息共享度

由于采用了物理连接方式，在传统数据信息共享模式的应用中，数据信息共享效率急剧下降，严重影响了网络用户的应用体验。在云计算中由采取了云端存储的方式，不仅提高了用户数据的真实性、完整性，避免了黑客以及不法分子的恶意攻击和窃取而且也大大提高了数据信息的共享效率。利用计算机网络技术，网络用户可以突破时空限制，随时随地地访问和浏览相关数据信息，而且还可以通过异地跨设备的操作的方式，对数据信息直接进行添加、修改和删除等操作。

3 云计算中所面临的网络安全问题

3.1 用户身份管理和未经授权的访问

在我们遇到更复杂的安全问题之前，我们遇到最多的问题是用户不当的身份管理，例如：账户劫持。未经授权方使用有效账户访问会导致数据入侵和泄露，但也可能是由于密码被盗、网络钓鱼等安全漏洞所引发的。

3.2 内幕威胁

当安全问题是内部威胁造成时，例如来自我们的组织或团队。这类攻击是我们不能忽视的风险。安全云存储的正常访问不会产生任何警报。实际上，它基本上是无法察觉的。所幸的是，信息安全最佳实践以及使用详细的日志记录工具可以有效限制这类攻击所造成的破坏。

3.3 网络攻击

与传统网络安全一样，拒绝攻击服务和中间人攻击也是云计算环境中面临的主要网络安全威胁。拒绝服务攻击指攻击者通过占据消耗网络和系统资源，让用户的网络或计算机不能进行正常的操作。在云计算中，黑客以及不法分子对服务器发起拒绝服务攻击时，会向服务器发送数以万计的访问请求，导致服务器不能及时响应客户端的正常访问请求。而

中间人攻击是另一种网络攻击手段。在通信双方不知情的情况下，攻击者拦截或阻塞正常的网络通信数据，并对数据进行篡改和嗅探[2]。

3.4 数据泄漏和丢失

随着存储在云中的数据体量的增大，这就大大增加了大多数云环境的攻击面。例如你忘记开放端口，具有超出其预期用途的运行时访问权限的脚本以及云环境中的其他小漏洞在未及时正确处理时可能会演变成灾难性问题。

本质上云计算是弹性制度的，但这并不意味着完全消除了数据丢失的风险。服务器仍然可能失败，硬件可能停止工作，文件可能会丢失。而忘记维护云环境的在线和脱机备份，可能会导致数据丢失进而引发其他一系列的安全问题。

3.5 虚拟化安全

在云计算中，虚拟化所带来的一系列安全问题也日趋显著。虚拟化的安全主要包括两方面：一是虚拟化技术本身的安全问题，二是由虚拟化引入的新安全问题。

3.5.1 虚拟机管理

（1）虚拟机管理程序

当多个虚拟机的程序被同一台物理机运行时，倘若管理程序的安全出现漏洞，那么攻击者将利用该漏洞访问整个主机，同时在该主机上运行的其他访客虚拟机也可以被攻击者访问。由于管理程序的更新频率很小，一旦被攻击者利用漏洞可能会危及整个系统的安全性。

（2）虚拟机资源分配

在被删除或重新分配的虚拟机中，如果释放的资源被分配给其他虚拟机，则有可能发生数据泄露。新的虚拟机可采用取证调查方法来获取整个物理存储器和数据存储的镜像，并用于分析，从而获得之前的虚拟机留下的重要信息[3]。

3.5.2 虚拟化安全攻击

当攻击者成功地攻下一台虚拟机时，攻击者就能在接下来很长时间下在一个主机上的其他虚拟机。标准 IDS/IPS 软件程序无法检测到虚拟机之间的流量，这种跨虚拟机的攻击方式也渐渐成为主流。不仅如此在迁移过程中也可能受到攻击，例如虚拟机被发送到未被我们进行加密的通道，这可能被攻击者嗅探到，但是执行这一点的前提是攻击者必须提前获得受感染网络上另一台虚拟机的访问控制权限。

4 构建云计算下网络安全体系

4.1 物理安全

与传统网络安全策略基本相同，网络安全技术的发展离不开硬件的更新换代,优质的服务器与处理工具除了能帮助更高效完成云计算之外,也可以对计算机网络安全进行保护。良好的的硬件设施能够提供更加高效的数据处理条件,也能让网络安全技术进一步落实,因此网络安全的保障也离不开硬件设施的保障。

4.2 虚拟化安全

4.2.1 安全运行和隔离

虚拟化技术是一种表示计算机资源的抽象方法，它允许虚拟化以与访问抽象资源之前的资源相匹配的方式访问抽象资源[4]。使其变为一个整体，忽略以往由底层属性和操作方式的不同，并通过建立一种通用的模式来查看和维护资源，保证系统的安全运行。

虚拟化技术将应用程序以及数据，针对不同层次的使用者的需求差别，以不同的形式进行展示，从而能够使使用者方便快捷的开发和维护存储的数据和应用程序。并通过采用云存储数据隔离以及虚拟机隔离加固技术，使得数据和服务端分别隔离，确保相互不受影响，保障其安全。

4.2.3 安全监控

基于虚拟化技术，我们可以进行有效的安全监控。传统网络安全监控技术有很多不足，而在虚拟化环境中网络安全监控技术可以起到很好的作用，借助于云计算强大的信息处理和分析能力，使得网络安全监控技术具体自适应性即可以不断的提高对网络攻击的防御水平[5]。智能防火墙、入侵防御技术等都是在虚拟化技术在网络安全监控技术的具体应用形式。

4.3 数据安全

数据加密技术主要包含算法和密钥这两个部分。其中算法主要用于对传输的数据信息进行加密处理，使其难以解读，即使数据信息在传输的过程中被网络黑客或者不法分子窃取，也不会造成数据的丢失或泄露，大大的增强了安全性和私密性。密钥主要用于对数据信息的解密处理，当数据信息传输结束后，网络用户接收到的乱码会自动被密钥解码，并转变成可以理解的数据信息，便于网络用户的识别和使用。因此，在云计算中通过对加密技术的应用，能够提高数据信息传输的安全性和私密性。

4.4 云管理安全

4.4.1 安全管理模型

由于云计算服务提供模式不同所以创建了不同的安全

管理边界,以及由服务商和用户共享责任的安全管理模型。例如在 Saas，主要由服务商担负责安全管理责任；对 Paas，由服务商和用户共同分担安全管理责任；对 Iaas，服务商仅负责网络、云平台等基础设备安全管理，而用户负责业务系统安全管理。面对不同的数据、应用、平台以及网络，用户和运营商各自承担的管理责任不同，从而得到更好安全管理模型[6]。

4.4.2 安全管理标准

安全管理标准，提供安全管理边界的界定条件的标准，服务商和用户可联动模式等。从而实现云服务的高可用性管理、安全漏洞管理、补丁管理、配置管理以及时间应急响应等。

结语

综上所述，云计算的迅速兴起带来的网络安全问题仍然是当下的一个焦点。云环境中对计算机网络安全提出了更加严格的标准，网络安全问题的出现，将直接影响到云安全。云安全的维护实现，关键在于如何有效的利用网络安全技术建立起综合性的云安全体系。同时为了云计算更好的发展，相关网络安全技术的研发和应用还需要结合人工智能，大数据等新型技术，多维度、多层面技术的相关探索也需要引起重视。

参考文献：

[1] 刘志强.云存储推动云安防落地[J].中国公共安全,2014(09):62-64.

[2] 杜瑞祥,鲜明,谷俊,陈恬.公有云安全风险分析及应对技术[J].网络空间安全,2016,7(07):67-72+79.

[3] 岳光.基于虚拟化环境下的网络安全监控技术应用研究[J].数字技术与应用,2020,38(06):176-177.

[4] 郑旭. 数字化校园视频监控系统组网设计及应用[D].沈阳建筑大学,2017.

[5] 赵波.基于虚拟化环境下的网络安全监控技术应用研究[J].数码世界,2018(08):199.

[6] 黄欣.大数据云计算环境下的数据安全研究[J].信息通信,2019(01):194-195.