云计算技术在计算机网络安全存储中的应用研究

董贵晨[1] 孙云豪[2]
1. 青岛能源集团有限公司 山东 青岛 266001
2. 青岛能源华润燃气有限公司 山东 青岛 266001

摘 要：云计算技术有诸多优点，能提升数据存储的安全性。互联网技术多元发展为数据存储提供了多样方式，基于云计算等技术的支持，可以为用户提供更大的数据存储容量，基于分布式存储、数据恢复等技术降低数据丢失的可能性及后果，可见，在计算机数据存储中合理应用云计算技术，对于提升计算机安全存储具有重要现实意义。

关键词：云计算技术；计算机网络；安全存储；应用研究

引言

在互联网时代背景下，国家的发展、社会的进步和个人的发展都需要网络安全技术保障信息的安全储存和传输。因此，网络信息安全的重要性已提升到一个全新高度。信息安全技术应建立在防御系统强硬，网络安全保护体系完善的基础上，提高安全防护技术手段，防止不良因素入侵网络。对此，科研人员应不断进行探索，紧跟时代发展的步伐，开发出安全性较高的防御系统，保障网络信息技术的安全。

1 云计算技术概述

云计算是一种即用即付的模式，可为用户提供方便的按需网络访问，对网络、存储空间，以及一些应用程序、服务器的资源能实现最优的可配置共享。云计算具有很强的灵活性和可用性，允许互联网服务供应商对云中心的功能进行的调整和根据自身的特点进行资源的计算和分配，以满足用户的需求，对提升云中心的计算和服务能力有很大的促进作用。在云计算的应用上，云计算可以通过不断扩大区域用户的数量，增强互联网和计算机之间使用关联[1]。云计算技术是信息发展的产物，是人类智慧的结晶，拥有较高的网络技术手段，可以避免计算机发生硬件问题的故障，以及计算机的程序错误、计算机使用被篡改等问题的发生。目前对云计算的应用较为普遍，各个领域开展工作都离不开云计算的支持，云计算技术优势之多，为人们利用大数据开展生产生活提供有力支撑。

2 计算机网络安全存储常见问题

2.1 网络攻击问题

网络攻击是计算机网络安全存储中需要格外关注的问题，一般指不法分子对数据库或系统发动攻击，从而窃取数据或者破坏数据的情况[2]。网络攻击可以分为内部攻击和外部攻击两类，内部攻击多为信息的越权使用或者内部恶意损毁等，外部攻击则主要是利用黑客程序或者DDos攻击等方式进行恶意攻击。比较常见的网络攻击方式包括：冒充或伪造合法用户身份进入系统窃取数据的冒充行为；通过植入木马程序窃取用户储存数据；利用流量分析方式对数据进行分析与研究，并窃取有价值信息。网络攻击是网络安全存储中比较严重的问题，对信息数据安全具有不良影响，需要引起足够的关注[3]。

2.2 信息泄露问题

信息泄露问题指在计算机网络安全存储中，在未经过用户授权和许可情况下，通过非法手段监听、搭线等方式获得相应数据信息并将其外泄。在早期的网络存储过程中，由于缺乏相应的网络安全经验和安全防护技术，网络安全存储中信息泄露问题的发生比较普遍，而现阶段由于非法窃取技术的提高，信息泄露问题屡有发生。信息泄露问题不仅会使内部敏感信息外泄，同时也会衍生出一系列由于信息泄露造成的严重后果，威胁用户的信息安全甚至财产安全[4]。

3 云计算技术在计算机网络安全存储中的应用

3.1 分布式存储

分布数据存储是将分布于不同位置的所有数据进行集中化的管理，并对其进行记录、传输、保存。分布式数据存储主要有以下几种存储形式：①依照网络拓扑结构，进行数据的分类，然后选择相应合适的节点及合适的存储设备，基于信息加密等技术处理数据，最后将相应数据传输至对应的分布式存储文件中。②利用优化后的存储结构，保存和管理数据，在数据存储中应用分布式存储技术，建立相应的完善的数据库，在对信息进行基本的分类等处理后，再将数据存储于不同位置中，在此基础上通过某种记录来实现检索、阅览等操作，这种存储形式中数据库是存储系统的一个重要部分，能为用户提供强大、可靠、高效的信息服务，且该存储形式应

用灵活，能够较好应对大数据存储环境，满足用户对数据处理速度、存储容量等方面的要求。③基于数据加密等技术存储数据，但无法较好应对大量数据的存储要求，主要体现在无法满足数据安全性、传输速度、数据完整性等要求，因此该存储形式一般应用在少量数据的存储中。

3.2 数据备份

传统备份需要为每台主机配备专用的备份磁盘，主机内数据必须全部备份存储于本地的专用磁盘阵列内。主流数据备份应用以下几种技术：

3.2.1 LAN备份

传统备份时需要为每台主机安装磁盘设备，若数据总量不大，一般应用LAN备份技术进行集中的备份。使用一台中心备份计算机，基于LAN备份方式，将应用服务器、工作站配置为相应的备份客户端。而中心备份服务器在运行中接收到客户端的备份代理请求后，将相关数据基于LAN方式传递至其所管理的、连接的相关备份磁盘资源上。LAN备份方式提供了集中化的、管理便捷的备份方案，且通过网络共享磁盘资源提升了备份效率。

3.2.2 LAN-Free备份

基于SAN环境，可应用不经局域网存储的LAN-Free备份技术，需要首先利用SAN将备份的服务器于备份磁盘进行连接，LAN-Free备份方式中，在客户端软件触发备份请求后，磁盘读取所需备份的相关数据，基于SAN备份到网络共享的备份磁盘中。这一独立网络能够保证LAN流量被合理地转移，相比LAN方式，其运转所占用的处理器资源更少，因为通信通道不需经过服务器TCP/IP栈，要实现某些应用层的错误检查，则可通过光纤通道硬件完成。实际应用中，需要一台计算机来管理网络共享的存储磁盘，并在该台主机上建设具有查阅数据、恢复数据等功能的备份数据库。

3.2.3 SANServer-Free备份

由于LANFree备份方式需要占用主机一定的CPU资源，若备份过程中能在SAN内部进行，则大量数据流不必通过服务器，即不会占用备份主机的资源，避免对生产系统产生不良影响。而SANServer-Free备份方式，结合阵列快照等技术，由服务器挂载快照，备份至相关的磁盘中，从而大大减轻了主服务器的运行负担，但仍需要使用主机来运行相关的备份软件，存储备份相关的源数据。

3.3 备份步骤

进行数据备份时，一般需要根据企业数据存储的实际需求，分析其各类数据的备份危险等级，基于不同等级的备份分类确定相应等级数据备份的资金投入，以节约建设成本，切词应确定适合企业使用的数据备份方式及策略，根据企业所定的存储目标合理选择备份技术，尽可能对高等级数据进行多机备份，从而提升备份的安全等级，提高其被攻击后被完全恢复的可能性。

3.4 数据恢复

根据底层技术，可将数据丢失问题分为逻辑问题、硬件问题两种，相应的数据恢复技术为逻辑恢复与硬件恢复。数据恢复涉及复杂的计算机知识及综合性很强的计算机维修技术，这就要求技术人员了解计算机数据记录、存储的方式及硬盘基础结构，熟练使用各种计算机故障检测、维修工具，如计算机数据记录方式包括数据表示方式、数据存储字节顺序及位序、数据存储逻辑、记录运算、数据结构等方面的知识，硬盘基础结构包括物理结构、逻辑结构两大方面，物理结构包括硬盘外壳、磁头定位驱动系统、盘标信息、主轴系统、数控系统、电路结构、接口技术及相关性能指标等知识，逻辑结构包括硬盘逻辑磁道、逻辑扇区、柱面及逻辑C/H/S、LBA等知识。数据恢复需要用磁盘编辑等工具分析、编辑磁盘底层数据，如使用WinHex、DiskEdit、HexEdit、HxD等工具，根据具体环境结合相关知识完成不同操作环境下的数据恢复工作。

4 云计算技术在计算机网络安全的管理策略

4.1 构建完善的网络信息安全框架体系

云计算视角下网络信息安全问题的解决首先需要从构建完善的网络信息安全框架体系入手。在云平台安全建设的基础上，从技术、管理和服务三个体系进行安全框架的构建。在云计算平台建设初期，从平台、访问和数据三个方面完善平台自身的网络信息安全体系。在技术层面，建立安全管理中心、安全计算环境、完善安全区域边界[5]。在管理方面，根据云计算平台的变化，定时完善和更新安全管理制度，加强安全运维、安全流程和安全建设的管理力度。在服务体系中，定期开展安全评估、安全加固以及应急响应的理念，同时加强自动化运维体系的建设，减少人工的干预。在身份层面，需要将身份视为主要的安全边界，并将身份系统，以及管理员和凭据作为首要优先事项加以保护[6]。

4.2 改进数据加密技术

在计算机内部的网络系统中，通过加密技术，数据信息即使被黑客窃取，得到的也会是没有意义的乱码，要对经过加密的信息进行读取，需要接收方和发送方使用密钥进行识别，这样才能最大程度上保证数据传输的质量和安全，避免数据在传输中途丢失。当前国内研发出的加密技术主要有2种，一是对称加密，二是非对称

加密。对称加密在对文件进行加密和解密的时候，需要运用到对称密码编码技术，这种只有通过密钥才能对数据进行读取和处理的渠道，能够有效保证各类数据的处理形式都符合系统加密处理的诉求[7]。非对称加密主要针对密钥交换协议而制定，是基于公开密钥系统而建立的一种加密系统，这也是与对称加密不同的地方，通过公开密钥和私有密钥相结合，才能成功将整个数据信息进行加密和解密的处理，通过这种方式，可以有效保证计算机网络数据系统在运行时，每一类信息都能过有效传递。另外，还可以通过运用密码机对程序进行简单设定，从多个角度对计算机网络内部数据信息进行解析，从而确保在实际操作中，数据的传输符合计算机网络安全的规范，提高计算机网络的适应能力和可靠性。

4.3 提高运维管理和风险管理的能力

云计算视角下网络信息安全问题的解决，除技术因素外，更需要提高运维管理和风险管理的能力，真正变被动防御转为主动预防。在运维管理方面，需要根据制度划分各类人员的管理权限，如云计算平台系统管理员、网络管理员、主机管理员、数据库管理员和应用管理员等，采用最小权限的原则给予赋权，并在岗位变化时，及时进行人员权限的调整。采用堡垒主机实现对云计算资源的身份认证、访问控制和行为审计。做好云计算资源的变更管理，定期展开渗透测试和应急演练。特别要对重要节点的云计算网络信息安全问题做好应急预案，要求相关人员对处理、上报和恢复流程烂熟于心。定期开展相关理论、制度和流程的宣贯工作，对于应急演练做好记录工作，并认真找出其中的不足，做好应该演练方案的更新工作。让人员从思想上认识到网络信息安全的重要性，从行动上全面掌握解决问题的技能。

4.4 改进身份认证技术

身份认证技术建立在对面部、语音和密码识别的基础上，通过多层次化的身份认证模式，保证人们在处理各类数据的时候，通过系统智能查辨，检查出用户在当前使用的计算机网络系统中，具有的访问权限，根据识别出的权限，再根据用户角色进行授权处理，拥有相应访问权限的用户，在具体的操作过程中，就能根据自身具有的权限功能，支配相应的数据信息，满足用户自身对操作和信息获取的需求。在云计算的大环境下，如果网络信息安全风险等级逐步提升，那么云计算网络安全防护系统对数据信息的监管力度也会随之增加。而通过身份认证技术，就可以将数据认证模式有效地作用于用户。身份认证技术实际上是丰富了数据信息的认证模式，使得认证形式不仅仅局限于传统的密码式认证。例如，使用指纹和虹膜识别，就能保证信息的传输是经过用户允许的。此外，还可以让口令认证和密钥认证相互关联，使传统的认证模式不完全来自第三方系统认证，而是直接让用户和服务器对接，通过这种方式，使得用户在对计算机进行操作时，计算机服务器就可通过相关口令产生密钥，从而顺利进行身份认证，等到此类操作被判定为合法模式之后，用户便可在系统内执行权限范围内的所有操作。

结束语

综上所述，随着信息技术在各行各业的应用，人们逐渐摆脱空间和时间上的束缚，生活和工作由此变得更加便利和高效。同时，各个新行业也随着信息技术的发展而诞生。信息技术的发展，为云计算的应用提供可靠保证，大量数据经过云计算的处理，以一种虚拟的形式存在于计算机中，满足用户的需求。云计算技术基于分布式存储等技术，将整体数据安全地存储于若干个程序、服务器中。因此，重视网络信息安全，积极开发强硬的防御系统十分有必要。

参考文献

[1]袁梓涵.计算机大数据分析与云计算机网络技术应用研究[J].网络安全技术与应用,2022(05):81-82.

[2]刘文君.云计算环境下网络信息安全技术发展研究[J].中国新通信，2020，22（17）：33-36.

[3]谢培璇.云计算背景下网络信息安全技术发展探究[J].网络安全技术与应用，2020（4）：91-92.

[4]崔斌.计算机大数据分析与云计算机网络技术探讨[J].无线互联科技,2022,19(02):67-68.

[5]王侃.人工智能、大数据和云计算的融合发展[J].信息记录材料，2022,23(2):170-172.

[6]李震.计算机大数据分析与云计算机网络技术研究[J].科技创新与应用,2020(02):150-151.

[7]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.