云计算技术在计算机网络安全存储中的应用研究

刘金涛
潍坊职业学院　山东　潍坊　262737

摘　要：随着云计算技术的不断发展，其在网络安全存储领域的应用日益广泛。本文主要针对云计算技术在计算机网络安全存储中的应用进行研究。首先对云计算技术和计算机网络安全存储技术进行概述；接着针对云计算技术在计算机网络安全存储领域中的应用进行了详细分析；最后，针对云计算技术在计算机网络安全存储中的应用进行了实验设计和数据分析。本文的研究结果将有助于进一步推广和应用云计算技术，在网络安全存储领域发挥更大的作用。

关键词：云计算技术；计算机；网络安全存储；应用

引言：随着互联网和计算机网络的迅速发展，计算机网络安全存储已经成为了一个备受关注的领域。计算机网络安全存储不仅涉及网络数据的安全存储，还包括了数据的备份、恢复、加密、解密等技术。而云计算技术由于其高可靠性、高可扩展性、高效性、灵活性等特点，已经被广泛应用于计算机网络存储领域。因此，对云计算技术在计算机网络安全存储方面的应用进行研究，将不仅能提升网络安全存储技术的可靠性和安全性，而且还能够在实践中为云计算技术的发展和应用提供支持。

1 云计算技术和计算机网络安全存储技术概述

1.1 云计算技术

云计算（Cloud Computing）是一种基于互联网的计算方式，它利用远程服务器和虚拟化技术来提供可扩展的IT资源服务，包括计算、储存和网络等资源。云计算的发展带来了计算模式和技术的革命。它提供了强大的计算和存储能力，对于企业和个人用户都有很多好处，如成本更低、服务更快速、更高效、更灵活和更具安全性等。

云计算模式主要包括公有云、私有云和混合云。公有云是由云服务提供商建设和提供服务，用户可以按需使用，这些资源通常由多个用户共享。私有云是一种在企业内部建设的云，用于仅限于企业内部的应用，访问仅限于企业内部员工。混合云是由私有云、公有云和本地IT资源构成的，允许企业在不同的云环境中部署其资源和应用程序。

云计算架构主要包括应用层、平台层和基础设施层。应用层包括软件即服务（SaaS）和网络即服务（NaaS）。平台层包括平台即服务（PaaS）和存储即服务（SaaS）。基础设施层包括基础设施即服务（IaaS）、网络即服务（NaaS）和虚拟化技术等。云计算安全问题是使用云计算技术时需要面对的一个重要问题。云安全主要包括数据安全、应用程序安全、身份认证和访问控制、网络安全和物理安全等。为了提高云计算的安全性，需要采取一系列措施，如完整性验证、数据加密、多重身份认证、审计、访问控制和容错等[1]。

1.2 计算机网络安全存储技术

计算机网络安全存储技术是指通过各种技术手段，保护计算机网络中的存储设备和数据资源，防止各种恶意攻击和数据泄露等问题的技术。这些技术涉及到硬件设备的安全和数据的保护两个方面。

在硬件设备方面，计算机网络安全存储技术主要包括：存储加密技术、存储虚拟化技术、安全存储管理技术等。存储加密技术是指对存储设备或存储系统进行加密，以保护数据的安全性。存储虚拟化技术是指将多个存储设备虚拟化成一个统一管理的存储池，提高存储资源的灵活性和可管理性。安全存储管理技术是指通过权限控制、安全审计等手段，保护存储设备的安全性。

在数据保护方面，计算机网络安全存储技术主要包括：访问控制技术、数据备份技术、数据完整性保护技术等。访问控制技术是指通过对存储设备进行规范访问控制，限制访问权限，防止非法用户获取存储设备中的敏感数据。数据备份技术是指对数据进行备份，以保证数据的可靠性和恢复性。数据完整性保护技术是指通过数据签名、数据加密等技术手段，保证数据在传输和存储过程中的完整性。

2 计算机网络安全存储的现状和问题

计算机网络安全存储的现状和问题有些许复杂，需要在技术、政策、管理等多方面进行综合考虑。未来的研究重点可能会更加关注机器学习和人工智能技术在存储安全中的应用，以提高存储数据的安全性和可靠性。计算机网络安全存储的现状和问题主要涉及以下几个方面：

2.1 存储数据的加密性问题

为保护存储在计算机系统中的数据不被窃取或破坏，需要采用加密存储技术对这些数据进行保护。但是当前加密算法的安全性面临不确定性，比如量子计算崛起可能会破解当前的加密算法。

2.2 存储数据的备份和恢复问题

针对数据在存储中的备份和恢复，需要采用可靠的备份和恢复机制，以确保数据的安全和可靠性。但是这种机制往往会占用大量的硬盘空间，增加存储成本。

2.3 存储数据的访问控制问题

存储需要严格的访问控制机制，以避免未授权访问和数据泄露。当前的访问控制技术主要基于身份验证和权限控制，但是这种技术虚拟机或云环境中很难实施[2]。

2.4 存储数据的物理安全问题

对存储设备的物理安全进行管理，以避免因硬件故障、灾难、劫持等原因导致数据的永久性丢失。

3 计算机网络安全存储的应用

计算机网络安全存储技术将在各个领域得到广泛的应用。在实践中，应该采用可靠的安全机制和手段，确保数据的保密性、完整性和可用性，更好地发挥存储技术在提高业务效率和安全性方面的作用。计算机网络安全存储的应用主要包括以下几个方面：

3.1 企业业务数据存储

越来越多的企业开始采用云存储、网络存储等技术进行数据存储，以便合理地备份、管理和共享业务数据。如何保证存储的安全和有效性成为了企业选型和实施的重点。

3.2 金融数据存储

随着金融业务的数字化，金融数据存储和安全也成为了金融机构亟需解决的问题。需要采用可靠的存储设备和安全机制，以确保数据的保密性、完整性和可用性。

3.3 政府信息存储

随着政府信息化的进一步推进，安全存储政府机构的各类敏感数据，如公民信息、税收数据、安全防控等备受重视。需要采用有力的数据加密和身份认证技术，以减少数据泄露的风险。

3.4 私人信息存储

如今越来越多个人使用云存储将重要数据备份，如照片、文件和联系人等。随着互联网的普及，隐私数据的保护和存储安全成为用户非常关心的问题[3]。

4 云计算技术在计算机网络安全存储中的应用分析

4.1 云计算技术在数据加密和解密中的应用

4.1.1 数据加密

云计算技术可用于加密数据，保护敏感信息免受未授权的访问和恶意攻击。最常用的加密方法是对称和非对称加密。

对称加密是一种相对较快速、安全的加密技术，其中发送方和接收方使用同一个密钥进行加密和解密数据。云计算技术使得对称加密变得更加容易，减少了加密、解密过程中数据的操作量。对称加密在保护大量数据时通常更有效。非对称加密采用公钥和私钥进行加密和解密，提供更强大的安全性能，但加密速度比对称加密慢。云计算技术可以通过提供高性能的处理能力，加速非对称加密的过程。

4.1.2 密钥管理

云计算技术可用于管理加密和解密数据所使用的密钥。密钥管理是一项复杂的过程，包括生成、储存、传输和撤销密钥。云计算技术可以帮助企业和组织高效地管理密钥。

云计算平台提供安全的密钥生命周期管理，包括密钥生成、储存和注销，同时还提供安全的密钥传输，防止中间人攻击。此外，云计算技术还提供了可信计算的技术，该技术可以确保密钥只在安全的环境中使用，以避免恶意攻击和数据泄露[4]。

4.2 云计算技术在数据备份和恢复中的应用

云计算技术在数据备份和恢复中的应用越来越广泛，这是由于云计算拥有高效、安全和经济的特点。以下是云计算技术在数据备份和恢复中的主要应用：

4.2.1 数据备份

云计算技术可以提供可靠的、高效的和经济的数据备份，帮助企业和组织保护数据安全。云备份服务通常提供自动备份功能，可以根据用户的要求定期备份数据，支持增量备份和全量备份。此外，云备份服务还可以提供不同级别的备份，并为用户提供选择备份数据存储区域的授权。

4.2.2 数据恢复

云计算技术可以提供高效的数据恢复服务，帮助企业和组织在数据灾难事件中快速恢复数据。备份的数据可以在云端存储，并能够快速恢复。此外，云计算技术还为用户提供了强大灵活的恢复功能，例如云内数据恢复、对本地磁盘的快速恢复、云和本地恢复之间的同步，以及多版本数据恢复等。

4.2.3 数据管理

云计算技术可以提供有效的数据管理服务，支持数据管理任务（例如数据分类、数据销毁）并可以快速完成，同时还可以提供更强大的分析能力，帮助企业和组织更好地管理备份和恢复的数据。

4.3 云计算技术在数据去重中的应用

云计算技术在数据加密和解密中的应用主要包括在云端对数据进行加密和解密操作，保障数据的安全性。当用户上传数据至云端时，云计算系统可以采用一系列的加密算法对数据进行加密，确保用户的数据在上传和存储的过程中不被非法获取。在数据的下载过程中，云计算系统可以根据用户身份和权限，对数据进行解密操作，使得用户可正常地访问和使用云端数据。同时，云计算技术还可以生成一些密钥管理方案，帮助用户更好地管理密钥，进一步加强数据的安全性。

云计算技术在数据去重中的应用主要从两方面入手。一方面，云计算技术可以利用哈希算法和摘要算法对重复的数据进行去重，降低存储空间的占用，提高存储效率。具体来说，当用户上传数据至云端时，云计算系统会对数据进行哈希操作，得到一个哈希值来判断该数据是否已经存在于云端，如果存在，则不再存储；如果不存在，则将该数据存储到云端。另一方面，云计算技术还可以通过比较不同用户上传的数据来实现去重，从而提高数据的共享和利用效率。

4.4 云计算技术在数据防篡改中的应用

云计算技术在数据防篡改和数据完整性保护方面具有广泛的应用。在云计算环境中，为了保证数据的安全性和完整性，一般采用数字签名技术和哈希校验等手段进行数据防篡改和完整性验证。

数字签名技术可以对数据进行身份认证和鉴别，防止数据被篡改和冒充。在数字签名技术中，云计算环境中的数据被签名，签名后的数据包括原始数据和数字签名。接收方在验证数据的完整性时，可以通过对数字签名进行校验，以确保数据的完整性和真实性。

哈希校验的目的是通过比较数据的哈希值来验证数据的完整性。哈希校验是通过计算数据的哈希值，将这个哈希值与存储的哈希值进行比较，以验证数据是否遭到篡改。如果哈希值一致，则表明数据没有被篡改；如果哈希值不一致，则表明数据被篡改或者传输过程中发生了错误。

5 云计算技术在计算机网络安全存储中的应用实验设计和数据分析

云计算技术在计算机网络安全存储中应用的实验设计和数据分析，可分为以下几个步骤：

5.1 实验设计

首先，需要设计一个能够满足计算机网络安全存储需求的云平台。本实验采用AWS（Amazon Web Services）云计算平台，搭建一个存储及分析安全日志的系统。具体步骤如下：

- 创建EC2实例：选择一个适合自己需求的实例，例如“Amazon Linux 2 AMI”。

- 安装基础软件：依次安装Logstash、Elasticsearch和Kibana。

- 配置Logstash：设置输入端口和输出端口等参数。

- 配置Elasticsearch：设置集群名称、节点名称、端口和索引等参数。

- 配置Kibana：设置端口、访问权限和Elasticsearch主机等参数。

5.2 数据收集

利用上述搭建好的系统，可以收集和存储各种安全日志数据，例如网络流量、入侵检测、系统日志等等。可以通过安装各种安全设备、安全软件等方式，将这些数据发送到Logstash，再由Logstash传输到Elasticsearch进行存储。

5.3 数据分析

通过Kibana提供的各种图表和分析工具，可以对存储在Elasticsearch中的安全日志数据进行分析，并生成有价值的分析结果。例如，可以通过分析安全日志来发现潜在的漏洞和安全威胁，对安全事件进行分类和统计，并及时采取措施进行解决。

5.4 性能测试

为确保系统在高负载的环境下仍然能够正常运行，需要进行一系列的性能测试。例如，可以模拟大量的日志数据并观察系统的稳定性和响应时间，调整系统参数以优化性能。

结束语：综上所述，云计算技术在计算机网络安全存储中的应用具有重要意义。通过云计算的存储方式，可以提高存储效率、可靠性和安全性。同时，云计算还能够支持大规模数据处理和分析，使安全存储的数据更好地被管理和利用。不过，云计算的应用还存在一定的安全风险，如数据泄露、数据损坏等问题。因此，在使用云计算技术时，必须注重数据的安全管理和保护措施，必要时可对数据进行加密等操作，以确保数据的完整性和机密性。

参考文献

[1]刘建康, 吴健锋, 范磊. 基于云计算的数据安全性研究. 计算机与数字工程, 2017(6):100-104.

[2]邱振军, 罗智鹏. 云计算数据安全与管理的研究. 管理科学与工程, 2018, (2):52-59.

[3]王晓晖, 王文超. 云计算安全技术研究现状与展望. 软件学报, 2017(2):383-400.

[4]葛丽萍,张艳.云计算时代网络安全问题分析及对策计算机系统应用2017(10):161-165.