 DOI: https://doi.org/10.26549/bdai.v4i2.13130

Discussion on Cloud Storage Data Security in the Big Data Environment

Wei Xia

Taiji Computer Co., Ltd., Beijing, 100102, China

Abstract

With the continuous development of Internet technology, the era of big data has also begun to come. As a new storage mode, cloud storage is the inevitable product of the development of the Internet, and also the latest application of computer technology in network storage. Cloud storage uses distributed storage to collect, manage and distribute user data to different servers, which can effectively improve the efficiency of data management and storage, provide a good user experience, have strong security and stability, and ensure data security against malicious attacks. However, as cloud storage technology is still in the development stage, it has certain limitations. If cloud storage technology cannot be used correctly, it will have a certain impact on data security. Therefore, the paper conducts in-depth analysis and research on cloud storage data security under the big data environment, and proposes corresponding solutions.

Keywords

Internet technology; cloud storage; data security; problem; solutions

大数据环境下云存储数据安全探讨

夏玮

太极计算机股份有限公司，中国·北京 100102

摘　要

随着互联网技术的不断发展，大数据时代也开始来临。云存储作为一种新型的存储模式，是互联网发展的必然产物，也是计算机技术在网络存储方面的最新应用。云存储采用分布式存储的方式，将用户的数据统一收集、管理、并分发到不同的服务器中，可以有效提高数据管理和存储的效率，能够提供良好的用户体验，具有较强的安全性和稳定性，保证数据安全不会受到恶意攻击。然而，由于云存储技术还处于发展阶段，其自身存在一定的局限性，如果不能正确运用云存储技术，就会对数据安全造成一定影响。因此，论文对大数据环境下云存储数据安全进行深入分析和研究，并提出相应的解决对策。

关键词

互联网技术；云存储；数据安全；问题；解决对策

1 引言

随着信息技术的不断发展，云存储已经成为大数据时代背景下的重要信息处理模式，它具有广泛的应用前景，能够为人们带来诸多便利。然而，在大数据环境下，云存储技术也存在一定的安全隐患，如果不能及时解决这些问题，就会对数据安全造成一定影响。因此，必须采取有效措施解决数据安全问题。

2 云存储数据安全

2.1 云存储数据安全技术

云存储数据安全技术主要包括以下方面，包括数据加密、数据防泄漏、数据备份、数据恢复和数据销毁 [1]。

①数据加密。数据加密是指通过加密算法对数据进行加密，使得用户无法获取到原始数据，从而保证数据的安全。数据加密技术主要有两种：对称加密和非对称加密。其中对称加密是使用两个密钥对数据进行加解密，非对称加密则是使用一个密钥对整个数据加密，这样在解密时只需使用其中一个密钥即可完成解密。

②数据防泄漏。数据防泄漏是指通过对数据加密，使得用户无法获取到原始数据，从而保证数据的安全。数据加密技术主要有两种：对称加密和非对称加密。其中对称加密是使用两个密钥对数据进行加解密，非对称加密则是使用一个密钥对整个数据加密，这样在解密时只需使用其中一个密钥即可完成解密。

③数据备份。数据备份是指将数据从本地计算机中复制到其他计算机上，或者将数据从其他计算机中复制到本地

【作者简介】夏玮（1978–），女，中国湖北黄冈人，高级工程师，从事计算机软件技术及应用、云原生、大数据方向研究。

计算机中。当数据发生丢失或损坏时，可以将其从其他计算机中恢复过来。数据备份技术主要有三种：本地备份、远程备份和网络备份。其中本地备份是指将本地计算机中的数据复制到网络上的另一台计算机上，远程备份是将网络上某一台服务器或计算机的硬盘的数据恢复到该服务器的硬盘上，而网络级就是将网络上所有计算机的硬盘的数据都复制一份。

④数据限制。在云平台运行过程中，需要设置相应的安全机制来保护用户的个人隐私。这些措施包括但不限于限制访问权限，防止非法访问等。例如对于敏感文件，需要限制只允许特定的人员（如管理员等）才能查看，同时还要禁止无关人员随意修改这些文件的内容等。

⑤数据销毁。对于已经不再使用的，或者是已经过期的信息，可以通过删除的方式进行处理。例如，可以将一些不常用的软件卸载掉，也可以将这些过期信息清除掉，避免其影响后续的使用。

2.2 保护云存储数据安全的对策

随着网络的发展，云储存已经逐渐成了我们日常生活中的一个重要组成部分，它能够让我们随时随地地访问自己的信息资料。但是，在云存储过程中，由于一些人为或者非人为的因素，导致我们的一些数据丢失。如何保证我们的数据安全存在有以下几点：

首先，使用第三方服务。目前，市场上有很多第三方的服务，这些服务都是专门针对企业用户而设计的，它们具有非常专业的技术团队，可以为我们提供各种安全防护。

其次，做好数据的备份。对于一些重要的文件，我们在进行操作之前一定要先对文件进行备份。因为一旦发生意外，我们的文件被损坏，我们可以通过之前的备份，恢复出相应的文件 [2]。

最后，做好容灾准备。为了保证我们的业务不出现中断的情况，我们需要提前做好容灾的准备。例如，我们可以提前购买好相关的硬件设备，并且将它们放在同一个地点。这样，当其中一台设备出现故障时，另一台设备仍然可以正常工作。

3 云存储数据安全与云原生的关系

3.1 云原生的概念

云原生是一种新的计算模式，是云计算、大数据和人工智能的融合，以用户为中心，通过互联网提供各种服务，实现按需使用，随时获取。云原生的核心思想是，把传统 IT 基础设施（服务器、数据库等）虚拟化后，在云端部署应用和服务，从而降低企业成本。同时将大量非关键性业务从线下搬到线上，提升企业的效率。因此，“云原生”可以简单理解为一种新的计算模式 [3]。

3.2 云原生的优势

随着企业对数据安全的重视程度越来越高，越来越多的公司开始考虑采用云存储，但随之带来的问题是：如何保证数据的隐私性和安全性，以及如何避免被第三方窃取。在这种情况下，如果能够解决以上两个问题的话，那么就可以帮助企业更好地管理其内部资源。而要做到这一点就需要对整个系统进行改造升级。

3.3 区块链 + 云计算

通俗地讲，它是一个分布式的共享数据库。在过去几年中，这种技术已经从比特币和其他加密货币，转移到金融交易领域。目前，许多大型银行正在使用这项新技术，以帮助它们处理复杂的交易。区块链本质上是一个分散式账本。所有记录都是公开透明的。任何人都能够看到或更改其中包含的所有信息（包括数字资产）。由于每个节点都有相同的账本，所以无法改变或删除。因为区块链具有去中心化、不可篡改等特性，而“云端 + 本地”的数据传输模式，存在一定的风险。因此，需要将区块链技术融入到企业的业务场景中，从而确保企业数据的安全。“区块链 + 云计算”的优势是，它解决了传统“云计算”无法解决的问题并帮助企业节省大量的时间。此外，由于该方案采用了先进的加密技术和智能合约技术。它不仅提高了系统的安全性，而且大大简化了操作流程 [4]。

4 云存储数据安全解决方案

4.1 云存储数据安全解决方案总体思路

云存储是互联网数据存储的最新应用，是一种新型的数据存储模式，能够有效提高数据管理和存储的效率。在大数据环境下，云存储数据安全解决方案需要结合大数据的特点和云存储技术的应用优势，设计出一套完整的解决方案。在大数据环境下，云存储数据安全解决方案需要包括云存储、数据安全、备份恢复和灾备四个部分。其中，云存储是整个方案中最为重要的部分，也是确保数据安全的关键环节。因此，设计人员必须要重视云存储中数据安全问题，采取有效措施保证数据安全。在设计过程中，首先要制定完善的保护策略和管理措施，其次要注重云计算平台的安全性和可靠性，最后要采用合理的技术手段加强对云计算平台的保护 [5]。

4.2 云存储数据安全解决方案具体流程

云存储数据安全解决方案主要由以下几个方面组成：首先，对用户的访问权限进行控制，通过授权机制的设置，保证用户的身份和访问权限处于动态变化状态，以此来保护数据信息不会被非法获取。其次，对数据信息的备份进行保护。由于云存储平台中有大量的数据信息，一旦出现了安全漏洞就会造成严重影响，因此要采取措施来防止数据信息出现丢失的情况。再次，谨慎选择第三方平台。如今，越来越多的企业开始使用第三方平台来管理自己的数据，比如微信、钉钉等。但是，在选择此类工具时，应该尽量选择正规可靠的平台，并严格遵循相关协议，这样才能有效保障企业的利益。最后，对云存储平台进行定期维护和管理。定期对

云存储平台中的硬件和软件进行维护和管理，保证云存储平台处于正常运行状态[6]。

4.3 云存储操作

在云存储模式中，用户的数据一般都是在网络环境中传输的，而这种传输是不需要用户参与的，也就是用户可以通过浏览器进行访问。这样，如果发生数据丢失或损坏情况，就可以直接从云端进行查找。同时，在云存储模式中，用户并不需要建立自己的服务器，这也就意味着服务器并不会直接为用户提供服务。因此，为了提高数据管理的安全性，还需要对云存储中的服务器进行科学管理。其中包括对云存储系统进行维护、对云存储服务器进行升级等。此外，在对数据进行访问时，用户还可以通过浏览器、客户端软件等多种途径来实现对数据的访问。

5 结论

云存储作为一种新型的存储技术，在应用过程中虽然会遇到一些问题，但仍然具有良好的发展前景。在云存储的应用过程中，需要对数据安全进行保护，只有保证了数据的安全性，才能为用户提供良好的使用体验。由于云存储本身具有较强的灵活性和开放性，其本身并不能完全保证数据安全，所以在使用过程中，需要对用户数据进行加密处理，并提高存储系统的安全性和稳定性。同时，在云存储环境中也会出现一些安全隐患问题，如服务器被恶意攻击、病毒入侵等。为了保证用户数据安全和服务质量，需要对云存储系统进行优化和完善。云存储系统需要不断提高自身的安全性和稳定性，并且需要对网络环境进行优化和管理。此外，需要对用户数据进行加密处理，并加大对用户数据的保护力度。此外，还应加强对云存储安全系统的管理和维护工作。只有不断提高云存储技术水平，才能保证云存储数据的安全性和稳定性。因此，需要从多个方面加强对云存储数据安全的保护工作。

参考文献

[1] 宿琼.大数据环境下云存储数据安全探析[J].中国新技术新产品,2016(4):2.

[2] 颜学祥.关于大数据环境下云存储数据安全的探究[J].中国新通信,2018,20(6):2.

[3] 杨子宇.大数据环境下云存储数据安全的相关探究[J].中国科技信息,2017(10):2.

[4] 李鸿雁.大数据云计算环境下的数据安全探讨[J].信息与电脑,2017(3):3.

[5] 朱登发.大数据云计算环境下的数据安全及防范对策探讨[J].电脑知识与技术:学术版,2018,14(2):2.

[6] 尚永强.云计算与大数据环境下全方位多角度信息安全技术探讨[J].科技传播,2018(23):2.