# 云计算的计算机网络安全存储技术探究

吴武斌*
宁波奥克斯进出口有限公司　浙江　宁波　315191

**摘　要：**随着计算机软件技术的快速发展，逐渐形成了云计算技术。在云计算技术的作用下，让传统计算机网络保存和计算形式发生了一定改变，有效地缓解计算机数据保存压力，提高网络数据资源使用效率，让数据保存更加安全和便捷。但是云计算自身展现出较强的开放性特点，在数据保存安全上将会面临一定考验，是当前相关领域重点思考的问题。基于此，本文围绕云计算的计算机网络安全存储技术的科学运用展开讨论，以供参考。

**关键词：**云计算；计算机网络；安全存储；关键技术

**DOI：**https://doi.org/10.37155/2717-5170-0305-26

## 1 云计算和计算机网络安全存储的概述

云计算技术是一种分布式计算技术，简单地说就是将处理体量巨大数据的程序分解成无数个小程序，通过多部服务器组成的系统对这些小程序进行分析、 计算和处理，并在得到处理结果后将其反馈给用户。云计算技术具有可靠性强、拓展性好、规模大等优点，在实际应用中有三种常见的服务模式：第一，IaaS，基础设施即服务不需要用户自行建立数据中心，而是通过租用的方式完成基础设施服务，包括对数据的收集、计算、整理和储存。第二，SaaS，软件即服务利用网络提供软件服务，在软件中设置虚拟化桌面，完成网络储存服务。第三， PaaS，平台即服务。用户可根据需求对软件进行开发。云计算技术在网络储存中的应用为用户增加了储存数据的新方式，有效提高了处理数据的速度，让数据的使用有更强的拓展性[1]。

网络安全存储指的是数据、文件在计算机系统中的存储安全性。网络存储结构通常包括以下几类，即直连式、存储网络与网络存储这三类。其中，直连式是最为常见的，存储网络指的是在计算机系统与网络存储系统之间进行文件、信息、 数据的传递，通过磁盘等多种硬件设备实现文件与信息的传输，而存储网络指的是利用网络实现信息的收集与存储，以数据为核心，断开储存设备与网络的连接， 需要注意的是，这种方式成本较低，但信息运行却有较高的效率，属于一种性价比较高的网络安全存储类型。

## 2 云计算技术在计算机网络存储中的安全隐患

虽然云计算技术的出现给当今社会信息数据储存时代带来了很多便利，但是在计算机网络的储存中仍存在不可忽视的安全隐患问题。主要包括两个方面。第一，黑客盗取网络数据。现在社会中有着很多电脑黑客，面对云计算拥有各个行业的重要数据信息带来的巨大诱惑，黑客凭借高超的计算机应用能力，帮助一些不正当竞争企业，盗取企业信息，谋求个人私利。因此，加强云计算技术在网络安全储存中的作用至关重要。第二，云计算技术有开放储存的便利特点，给客户带来了便利同时也会引起一些不法分子的躁动，因为一些个人或者企业可以借用云计算技术服务形成垄断，这样确实可以提供商业信息，但难以保证云计算技术在数据信息储存中降低损失。

## 3 基于云计算的计算机网络安全存储关键技术

### 3.1 加密存储数据

当前，最常用的加密技术包括对称加密技术和不对称加密技术。对称加密技术使用相同的加密密钥加密和解密加密算法，其速度、效率和加密安全取决于相同的加密算法，因此加密密钥的管理是非常重要的。不对称加密则需要设置一个同时且两两相对的公开密钥和私密密钥。公开密钥用于数据加密，而私密密钥用于解密数据，其特点是算法复杂，安全依赖于算法和密钥，尽管加密和解密并不比类似的加密更快，但这种密钥更安全。这两种数据加密技术的应

*通讯作者：吴武斌，1983.6，汉，男，浙江宁波，宁波奥克斯进出口有限公司，高级工程师，本科，研究方向：计算机及人工智能。

用填补了以往在网络安全存储领域存在的安全漏洞，从而大大增加了云计算应用的安全。

3.2 身份认证

每条信息都需要身份验证才能确保网络存储的安全性。身份确认在防御中起着重要作用，主要依托以下四种技术。第一，核对密钥。用户在开启云计算技术进行数据的传递和分享时，可以提前设置一个口令和密码，只有通过密码才可以使用网络信息。第二，智能IC卡。用户将自己的信息录入到系统中，用户在使用过程中，服务器可以通过身份验证获取使用人员的相关信息，进而判断用户身份。第三，kerberos。用户以密码密钥的形式设置密码，用户必须得到服务器的授权指令，并且网络只能通过相关的身份验证进行身份验证。第四，pkl。使用密码加密网络并更新数据信息，确保网络信息数据的安全。

3.3 备份技术和恢复技术

信息数据的恢复和备份技术在网络存储过程发挥着重要作用，如果没有恢复技术和备份技术，存储在网络中的数据信息就无法得到有效保护。当这些信息数据受到恶意破坏或者无意丢失之时，如果事前没有备份，或者无法有效恢复时， 会给用户造成极大损失[2]。因此，在网络存储的过程中，需要利用先进的恢复技术、存储技术，保护存储在网络中的信息数据。基于云计算的恢复技术和备份技术将这些重要的信息数据可直接存储在计算机硬盘中，也可存储云于服务器，能很好对存储在网络中信息数据进行备份，还可有效恢复意外丢失、删除的信息数据，从而有效保证了信息数据的安全性和完整性。目前在众多云计算存储软件中最常用的数据保护技术是删除保护技术，删除保护技术可将用户已删除的数据信息保存在回收站里一定的时间，在这期间可依照用户的使用需求对信息数据进行恢复。

3.4 密匙管理技术

云计算数据存储的安全性主要取决于密钥，而密钥管理技术是当前计算机网络存储中的重中之重。如何有效地管理密钥也是大型云计算技术公司发展的关键和难点。通过共享合理的计算机网络安全存储是使用的关键，可以有效地提高云计算技术的服务效率和业务水平。当前，许多云计算存储程序都使用CAPTCHA来保护密钥和数据信息，这也有利于云计算网络信息存储安全的发展。

3.5 删除码技术

删除码技术可以有效地应用于对分布在计算机系统网络中的存储错误上代码的解码。当该技术应用于编码技术时，它可以选择诸如码字，分组代码，代码集和监督代码元素之类的信息进行编码。在实际应用中，它可以分为三种：RS纠删码，无速率码和级联的低密度擦除码。这些技术可以保护计算机网络并提高计算机网络存储技术的可靠性[3]。

## 4 基于云计算技术的计算机安全存储中的应用

4.1 MC-R中的应用

使用MC-R技术可以带来不同的安全管理战略，一般可分为客户端MC-R和云端MC-R。第一，客户端MC-R。传统数据库的数据隐藏以及伪装在计算机网络安全存储中处于较差的位置，大量数据以明文的形式储存在数据库中，在这种情况下，可以使用MC-R加密算法来隐藏重要数据，标记重要数据信息，在数据库中储存大量数据以供修改，利用其强大的计算能力，迅速解密数据，在使用数据时及时解密数据， 并确保适当使用。这个技术可以在协同状态下安全地储存电脑网络数据；第二，云端MC-R加密。目前计算机设备具有很高的信息处理能力，特别是在AI技术方面，不需要计算所有数据就能得出最终结果，而且基本数据加密可以防止在云端MC-R中大量消耗。完整的加密和解密程序是：①用户在云端上生成MC-R密钥，并保留唯一的钥匙。②使用MC-R加密算法处理数据，将文档数据与密钥一起并上载到云端。③密文和密钥要同时保存在云端。④用户可以用密钥进入云数据库，在此基础上，可以将密文下载下来并进行修改，当然密钥打开密文之后回就会自动转换为原始数据。⑤数据标签功能允许查找隐藏的数据并将数据的伪装撤除，以便用户能够自然地获取信息。

4.2 M-POR中的应用

M-POR 是“挑战—响应—验证”机制中的重要算法。其通过冗余纠错码验证云计算中用户的数据状态，当用户查询所需数据时，会自动将挑战申请发送给云端，由云端响应该挑战申请，用户验证云端响应信息，信息验证通过后，便可证明归档数据所处的安全状态。若验证不通过，代表归档文件已破损，需采取恢复手段。当破坏值未超出阈值时，可通过编码冗余信息恢复原始数据，还可通过副本冗余安全存储提高恢复数据的成功率。M-POR 可有效验证

云端中数据是否完整，准确定位云中的错误数据，以此开展深层分析。

## 5 结束语

总而言之，现阶段，互联网信息技术为人们带来了极大的便捷，使得人们的生活发生了 翻天覆地的变化，社会生活日新月异。通过运用云计算技术，提高了计算机安全存储水平，希望通过以上分析，能进一步加强实践研究能力。

## 参考文献

[1]萧益民云计算技术在计算机网络安全存储中的应用[J].科技展望，2016， 26(29):6.

[2]阮英勇.计算机网络安全存储系统设计及应用.云计算技术下[J].现代商贸工 业,2016,37(10):186-187.

[3]李海生.计算机网络安全存储中云计算技术运用[J].网络安全技术与应应用，2020(6):96-97.