云计算技术在计算机网络安全存储中的应用研究

杨 雷[1] 李 虹[2]
1. 中国北方发动机研究所 天津 300400
2. 中国电子科技集团公司第十八研究所 天津 300384

摘 要：在计算机网络存储中，假如安全防范措施落实不到位而造成关键内容丢失，就会引起一系列的损害，减少用户的网络存储使用感受。阐述了身份认证技术、加密技术、数据库备份修复技术和删除码等几种计算机网络存储安全核心技术，并制定了根据云计算技术的计算机网络安全存储方案，从设计模型、数据编码结构等环节提升数据存储安全，合乎互联网时代的安全存储规定。

关键词：云计算；安全技术；网络存储

引言

计算机互联网及存放作用在企业和个人发展过程中具有作用支撑点，需具备安全及稳定性特性。但计算机网络安全数据存储结构运作期内，仍存在一定的缺点，比如，安全防范创新方面的不健全，非常容易造成黑客病毒及其计算机系统漏洞的风险难题，增加安全隐患。云计算技术的应用及完成，在计算机安全分布式存储中，根据高安全、高效化性、高检干脆特点，对计算机数据存储结构设安全防范体制，提升设备运行效率。

1 云计算技术的概念

云计算技术是一种创新的互联网技术，具有极强的虚构性、开放性、可扩展性和可靠性。在互联网时代下，云计算技术通过一些计算服务，助力企业获得管理优势，根据创设服务体系和规范化部件助力企业创设最理想的资源与技术。现阶段，90%的公司早已选用多种多样云计算技术协作的计算机互联网服务技术。云计算技术的应用，主要在分布式技术、高性能计算、热备份冗余技术等方式方法的大力支持下，完成各种各样计算机网络功能的融合，将诸多计算机软硬件建设融合成一个统一的指引集群式，进而提升每台计算机的计算效率，从而以手机客户端网络服务器为依托，为用户提供对应的服务项目。云计算技术具有极强的普遍性，这在一定程度上取决于云计算技术的经营规模高效率[1]。

2 发展现状

伴随着云计算技术的诞生，计算机和互联网信息技术有了更多的发展动能，在计算机和互联网信息存放行业，出现了新的词汇：互联网安全。互联网安全被用于避开计算机病毒感染预防黑客入侵，致力于为用户、公司等组织的信息安全保驾护航，互联网安全要以互联网计算和及时性强的信息共享的方式去完成信息存放安全的目的。目前我国在云计算技术领域内的研究和应用赢得了丰厚的造就，但是同时还是有一定的提升空间。

我国在将云计算技术应用于计算机存放层面获得了很不错的造就，以往计算机存放数据信息一般来说主要有两种方式，一是运用U盘和移动终端将它们信息存放下去，二是在计算机设备上运用电脑硬盘把要需文件存储下去。第一种存储方式运用U盘和移动终端，有可能在挪动过程中遇到内容丢失的概率，第二种存储方式运用电脑磁盘，存放的信息会占有很多磁盘空间，甚至贴近电脑硬盘最大容量，导致程序运行受阻的情况出现。除此之外，若是在有计算机病毒电脑插进移动终端，可能会致使移动终端中毒了，导致数据信息遗失，电脑磁盘就会受到病毒侵略，毁坏存放的信息。而应用云计算技术可以提升文件存储方法与存放自然环境，最大程度地减少计算机病毒攻击的概率，云计算技术也有自动化技术备份数据的功效，能够减少用户人为因素错误操作导致内容丢失现象发生[2]。

3 云计算背景下计算机网络安全存储现状

3.1 计算机安全防护存在漏洞

许多计算机互联网的安全防范存有系统漏洞，因而造成内部存储的大规模信息可以轻而易举地从外部搜索系统获取到，可能会导致犯罪分子可以轻而易举地寻找进攻目标开展信息盗取。因而，在日常应用计算机的过程当中，一定要进一步提升互联网的安全防范水平，根据高效的安全防范措施提升安全防护特性，进而保证内部结构文件存储的安全。一般情况下，建立网络防火墙或运载电脑杀毒软件，可以实现对计算机互联网分布式存储的前提维护，需要进一步提高维护实效性，还要对互联网系统稳定性和安全开展更新，比如根据专业化信息防御系统创建，提升信息管理工作的安全，使计算机

互联网文件存储作用获得最大限度充分发挥，促进云计算技术的理论运用。

3.2 系统安全问题

如今在一些终端设备软件系统中，这类互联网最很容易发生VM系统漏洞、RDP系统漏洞，从某种意义上比较严重限制计算机应用软件的安全和企业网络智能终端的安全。计算机网络安全分布式存储的病毒感染较强。毁灭性网络安全问题对计算机系统内部结构涉及到的数据代码等优质有严重危害。一般作为编程设计的基本模型，潜藏在系统终端的系统内部结构，有隐性的特点、潜在性等。计算机病毒感染主要是针对系统终端的信息具备毁灭性的编码实体模型，在其中绝大多数依编程设计设计风格存在系统内部结构。计算机电脑病毒对系统终端的毁坏有一定的造成了巨大危害，绝大多数公司资料都存放在这一终端设备中，在遭遇病毒入侵后，保存在终端设备的相关资料也会受到安全风险[3]。

4 加强计算机网络安全储存中云计算技术的应用方法

4.1 强化信息库和防火墙设备

许多人在正常计算机工作和学习过程中，必须提升对业务信息的安全防范意识，保证数据信息可以存放在的环境里，从而减少被窃取风险。其最为重要的对策，是为了计算机开设安全网络防火墙，维护数据信息不被很多人病毒感染或网络黑客侵犯。防火墙是一个具备学习功能的app，它不仅可以抵御外来的攻击、恶意病毒感染，还可以在管理的过程内进行主动学习，持续提升自身的抵挡水平，进而对计算机进行全面维护。因而，对云计算技术网络防火墙作用开展加强的过程当中，一样可以不断提升数据信息的贮存安全，让用户可以安心的应用云计算技术贮存作用。比如，在一台电脑中设置权限防火墙软件，接着运用云计算技术能将防火墙的作用拷贝到另一台计算机中，而且计算机可以在单独运作状态下，正常启动防火墙的作用，以达到维护数据信息安全的目的，保证每一台计算机既在云计算管控下，又可自由地完成数据信息安全贮存，进而提升数据库的安全。

4.2 安全技术手段

4.2.1 数据加密算法

数据库加密环节中，可以提高数据信息分数安全，防止数据信息于被盗取，用户可采取加密技术，将文档加密后信息进行提交存放，保证信息数据库的安全，与此同时可采取步多加密技术，执行不一样档次的数据加密控制方法，避免信息的泄漏，提升文件存储的安全。比如：可选择256个随机数字对业务信息开展数据加密，使之处在同一引流矩阵之中。云云计算平台下，密钥管理是保障计算机网络安全关键方式，数据库加密可以用随机序列设计方案，将ascii码的编码序列开展升级和辨别，提高数据信息破译难度系数，掩藏数据长度。云计算技术为用户带来了自动化资源服务，云计算部件与整体框架以互联网为核心，由互联网连接在一起向用户提供帮助，云服务器的服务提供者应完成资源透明度、池化，摆脱界限统一调度，每一个网络资源，为用户给予根据需求服务项目。云云计算平台下病毒、安全漏洞、黑客入侵都来自于安全技术攻击，用户要进行网络隔离搞好入侵防御系统，运用入侵检测技术对计算机互联网开展限制访问，操纵相对应管理权限，防止违法用户的进入[4]。

4.2.2 设置访问权限

在时期飞速发展的今日，人工智能的来临让信息更为有效化，但也随之而来各种各样信息也变的愈发透明度，用户信息安全也逐步形成每个人相对高度关注的问题，在云计算机服务项目环节中，因为用户处在开放式的互联网时代当中，作为经销商要重视其用户信息安全隐患，融合用户的实际需求访问限制的有效设定，提高资源安全，合理防止用户信息泄漏事件发生与产生。密码是一种安全保障措施，在用户信息化办公室环节中要注重起数据加密工作中，对一些秘密文件及其关键操作中加强登陆密码的应用，同时注意不要把密码管理的太过于简易，根据高效的安全防护充分保障用户安全。所以在云计算的发展环境下，经销商和用户都需要全方位重视安全技术标准体系的搭建，有效对访问限制开展设定，多方位提高信息安全防护专业技能与水准，为用户的安全服务保障。云计算根本目的是把大量云计算服务器发放给不同类型的用户，适用用户根据自己要求，进行一定的网络资源的应用，在云计算安全身份验证，能够有效确保各类数据库的安全，用户在浏览时需要键入相对应的认证信息，动态口令、IC卡、Kerberos身份验证、PKI身份验证等，进一步促进身份验证的精确性，合理降低用户风险性，减少安全风险，提升企业数据库的安全。

4.3 基于云计算的网络数据安全存储模型

现阶段，互联网数据库主要采用分布式系统架构，存放在分布式系统架构里的意见反馈信息马上发送至信息中，随后信息操纵数据加密和块存储。该分布式系统实体模型在一定程度上确保了数据存放的安全，却也存在许多难题。假如用户想浏览的数据，云服务器将标志用户，通过一系列安全认证，获得用户数据存放的有关信息，并依据该信息测算存储节点。此全过程能控制数据的保存，并

在原有和获取环节中维护信息。为了能精确获得存放数据的数据加密块信息，云服务器创建数据加密方程，根据求得方程获得对应的保密，进一步确保数据信息安全。互联网数据安全存储实体模型与此同时用了多种多样安全生产技术。一是合理认证用户真实身份，选用登陆密码认证、身份核查等形式多样。随后数据加密保护数据，假如用户必须载入数据，则完成破译[5]。

4.4 数据编码构造

数据编号构造展现了计算机应用的便利性，一部分解决目标必须编号。现阶段常见的输电线有归零码、双极码、单级码、更替码翻转码等。编号的目的是为了降低数据量、数据处理准确性高效率。编码技术能够帮助你在短时间内掌握数据的特点，降低电脑硬盘在互联网数据存放里的占有，尤其是在必须快速解决很多数据的情形下。在云技术的运用中，互联网安全存储能够取决于数据编码存放安全。假如用户需要使用数据，能直接从云间获得数据。分类存储系统大大提升了用户数据安全。在数据编码的建立情况下，首先剖析用户对数据存放的需要。在其中，任意多余信息是数据编号构造的关键主要参数。假如x表示任意冗余度，y表明冗余信息，而且k表示编号主要参数，则得到下列关系式：n=k+x+y。用户在存放数据时，能够最先把整个数据分成k块，搭建均匀随机矩阵。随后，可以将事先搭建的随机矩阵组合在一起编号，能够形成信息连接点表。在数据编码的建立情况下，主要是由云计算技术适用，能够实现统一的操作控制操纵，最大程度地确保互联网存放安全，防止存放的数据以密文方式发生。假如在这段时间产生数据泄漏，则只能产生编号数据的泄漏，不会泄漏存放在互联网中最原始的数据。

4.5 身份认证技术

现阶段比较常见的云计算技术认证技术包含登陆密码认证、智能化IC卡用户认证和PKI认证等。运用不一样的运转情景，置入对应的数据认证技术，提升信息协同控制。

（1）安全校验：作为一种比较常见的安全校验方式，用户浏览数据库时应该根据电子计算机页面输入支付密码凭证。电子计算机设备验证信息后，假如恰当则授予用户管理权限，假如不正确就需要全方位认证。这类认证方式较为立即，根据不同类型的用车场景开展认证较为。假如用户数次出现错误，当超过限制时把限制访问。

（2）IC卡认证：IC卡以处理芯片方式键入用户信息。当IC卡内部身份信息与当前操作权限的指令信息存在不符时，则无法驱动计算机系统，防止外部操作对计算机存储环境造成损害。

（3）PKI身份认证：该认证实体模型由公钥实际操作，也可以理解为是硬件配置、手机软件、工作人员、法律法规的结合，确保了公钥密码体系公钥和证书形成、管理与存放的合理化。针对电子计算机安全存储系统而言，该认证根据认证、数据安全保密性、数据可逆性来确定数据信息的时间点和空间节点，在传动系统的过程当中根据多维度认证体制，从而实现计算机软件的总体运作[6]。

5 结束语

总的来说，由于电子信息技术的迅速发展，大众的日常生活出现了很大的变化，生活习惯更为便捷，社会发展面貌焕然一新。但是目前电子计算机安全存储存在一些不够，信息数据存放安全不可以100%确保。在这样的环境下，依据计算机存储的现象，运用云技术协助电子计算机完成安全存储。在日常工作中，仅有运用云技术安全管理信息数据，创建合理的数据安全管理模式，充分运用云技术的优点，电子计算机数据存储安全才能获得想要的效果

参考文献

[1]荣喜丰. 云计算技术在计算机网络安全存储中的应用[J]. 电子技术与软件工程，2020(22):251-252.

[2]杨碧倩. 大数据时代背景下高校档案信息数字化建设研究[J]. 兰台世界，2019(29):40-41.

[3]王红梅.试析云计算技术在计算机安全存储中的应用分析[J].新型工业化,2021,11(5):96-97+111.

[4]乐晓蓉.基于云计算技术的计算机网络安全储存系统设计[J].电子技术与软件工程,2021(4):252-253.

[5]郭文博.云计算技术在计算机安全存储中的应用[J].电声技术,2022,46(1):39-40.

[6]钟思.何国民,袁煜,等.基于大数据和云计算的网络空间安全防御研究[J].科技创新与应用,2022,12(10):45-46.