探析计算机网络数据库的安全管理技术

廉志文
江西省乐平市大数据中心

摘　要：随着信息技术的创新与发展，数据信息所蕴藏的经济价值也被不断扩大，很多企业开始注重数据信息的发掘与探索工作，而计算机网络数据库也得到很好的推广与应用。计算机网络数据库具有存储量大、信息处理便捷等多种优势。随着时代的进步与发展，计算机网络数据库安全管理暴露出很多不足和缺陷，这对用户信息安全造成严重威胁。基于此，文章对计算机网络数据库安全管理存在的问题展开详细论述，有针对性的提出科学实用的计算机网络数据库安全管理方法，力求为计算机网络数据库安全管理水平提升和管理实效增加指明方向。

关键词：计算机网络数据库；安全管理；关键技术
【DOI】10.12252/j.issn.2096-6288.2023.01.073

引言

随着社会经济的发展与繁荣，计算机网络数据库的安全问题也越来越明显，为了保证用户安全上网和健康浏览各种数据信息，有关领域需要进一步提高计算机网络数据库的管理水平和保护实效。计算机网络数据库是重要的信息储藏区域，用户可以将文件资料以数据形式保存下来，这样在网上搜索、查阅的时候，就能快速找到想要的信息，可以说数据库给用户查找、处理信息带来很大方便。但是受网络环境的影响和安全问题干扰，网络数据库安全管理一直存在很多不足和缺陷，如果某些重要信息被遗漏或者窃取，用户工作生活也会受到很大影响，所以有关领域要深化数据库安全管理工作，持续提高计算机网络数据库的安全等级，确保信息数据能够安全存储和健康查阅，这对计算机网络技术的发展起到明显推动作用。

一、加强计算机网络数据库安全管理的实际意义

在信息技术发展升级过程中，计算机网络数据库的作用价值十分显著。利用计算机网络数据库，可以实现对海量信息的存储以及使用。与此同时，通过各种科技手段对数据库展开安全管理和健康维护工作，借助完善的信息存储技术，可以实现对各种数据的管理控制目标。只有在安全保护技术的参与支撑下，数据库安全等级才能得到有效提升，信息数据运行速率也能大幅增强。特别是随着网络技术的推广与应用，大数据、云计算等先进手段迅速崛起，数据信息的种类也更加复杂，数据存储量逐渐增多。在信息社会的背景条件下，数据信息作用价值得到有效扩展和明显延伸。在网络环境下，许多企业的生产经营活动都要借助信息手段来完成，而计算机网络数据库管理一旦出现问题，将会给企业带来巨大的经济损失。对于普通网络使用人员来说，一旦遇到网络故障、信息泄漏问题，他们的隐私权益就会大打折扣。如果网络数据库管理不科学，数据信息很容易发生泄漏和篡改风险，无论是对企业还是对个人，都会造成巨大的经济损失。所以在信息技术高速发展的背景条件下，加强计算机网络数据库安全质量显得尤为重要。如今计算机网络技术使用人数逐年递增，计算机网络技术涉及的信息数据也异常繁多，为了保证计算机网络技术处理数据信息的时效性和准确性，有关领域要持续优化网络数据库存储结构，这也使得计算机网络技术管理难度进一步增大，这种情况很容易造成数据信息丢失或者泄漏问题发生[1]。众所周知，数据信息具有更新速度快、处理量大、处理时间短等明显特征，为了保证信息处理的质量和水平，有关部门需要加强对数据库中的信息管理和保护工作。随着云计算和5G技术的推广与覆盖，数据信息的复杂性、准确性和高效性都明显提升，如果网络数据库安全管理工作不能发展或者更新，无法与新技术互相融合甚至匹配，那么信息数据的安全性就很难得到保障。因此，对计算机网络数据库进行安全管理显得十分必要。

二、计算机网络数据库安全管理需求

（一）确保数据安全质量

计算机网络数据库是一个庞大的数据存储区间，它的数据量会随着时间的流逝逐渐增多，并且会有源源不断的新数据加入存储库当中。相对于已经存储的数据信息，新流入的数据信息安全管理风险更高，容易引发严重的安全问题。在这种情况下，如何保证新输入数据的质量与性能，以及如何提升数据信息的安全等级成为有关领域不得不思考的实际问题。在具体操作过程中，管理人员要加强新输入数据的安全管理工作，防止数据信息混淆、丢失或者病毒入侵；与此同时，还要注意对新输入的数据信息进行正确归类和存储操作，将新输入的数据信息和原来的信息资料有机融合起来[2]。

（二）确保数据传输安全

数据传输是计算机网络技术发挥作用价值的必要条件，数据传输可能遇到的安全问题数不胜数，所以保证数据传输安全质量十分重要，同时也是计算机网络数据

库安全管理的必然要求。一般情况下，计算机网络数据库的数据信息处于灵活多变的发展状态，数据信息传输量十分巨大，在此过程中如果遇到数据信息丢失和泄漏等问题，用户隐私权益就得不到有效保障。因此，在计算机网络数据库安全管理当中，必须加大对数据信息传输问题的保障和维护，确保数据信息安全稳定输送，增强数据信息完整性和可靠程度。

（三）确保数据使用安全

计算机网络技术产生的信息数据应该保持科学完整的发展状态，只有这样才能提高数据信息使用价值。在实际管理过程中，计算机网络数据库安全管理人员要保证信息数据完整性和可靠程度不受损伤，为数据信息提供相应的管理控制意见[3]。因此相关管理人员要持续深化数据库安全管理技术和保护手段，为计算机网络数据库平稳高效运行奠定深厚基础。

三、计算机网络数据库安全管理存在的问题

（一）数据库网络安全问题

实践研究表明，数据库网络安全问题产生的一大根源与系统安全性不强有很大关系，通常情况下，技术人员在管理保护数据信息资料时，会采用防火墙等网络手段提高系统安全等级，如果网络环境比较危险，很容易受到不法分子的侵害与威胁，稍有不慎就会产生数据信息泄漏和窃取等问题，在这种条件下，网络数据库中的重要信息会全部流失，如果病毒和其他危害信息趁虚而入，网络数据库的完整性和可靠程度就会大幅下降。

（二）数据库管理安全问题

数据库安全问题产生的原因有很多，其中包括网络监管制度的匮乏和缺失，这是造成数据库安全等级不够高的主要根源，在这种条件下，有关部门要通过合理的控制管理措施来增强数据库管理工作的安全性和可靠程度，确保数据信息能够保持高效、平稳的储存状态。技术人员在管理数据库的同时需要把网络环境适当优化，同时还要对数据信息进行整理和汇总，借助人力资源管理优势增强数据信息的安全性和可靠程度，大幅提升数据库管理安全等级与质量。值得注意的是，当前我国很多数据库管理人员能力水平有限，在数据库安全管理过程中表现出不同形式的缺陷和弊病，无论是管理方法还是技术手段都存在很大的改进上升空间，这些问题也是导致数据库安全管理不到位的主要根源[4]。

（三）系统硬件安全问题

计算机网络技术需要依靠系统硬件和软件两大部分发挥效用，软件部分属于计算机网络技术的核心与中枢，系统硬件是计算机网络技术平稳高效运行的基础和前提所在，脱离系统硬件的计算机网络技术是不完整也是不科学的。如果计算机网络技术存在系统硬件问题，那么后续工作就无法正常开展，很多数据信息也会出现缺失情况。现阶段，很多组织与个人在使用计算机网络技术的时候，为了节省成本和扩大效益，经常选择不符合预期要求的系统硬件，在后续安装管理过程中计算机网络技术的安全性和可靠性得不到有效保障，网络数据库也会受到不同程度的损伤与破坏，更有甚者会引发严重的干扰问题。

（四）系统漏洞问题

由系统漏洞引发的安全问题十分严重，在实际应用当中，系统一旦出现漏洞和缺陷，其安全性就会大幅下降，并且很容易被外界因素干扰和破坏。人们把系统漏洞称作计算机的bug，不法分子就是利用这些 bug入侵用户的数据库和网络平台，给计算机安全防护造成极大损伤，与此同时，里面的数据信息也会被盗取和复制，个人或组织都会遭受不小的经济损失。因此，技术人员在进行计算系统的设计与规划时，应该加强自我审查功能，确保漏洞和缺陷得到有效弥补，增强计算机网络数据库管理运行的安全程度。

四、计算机网络数据库的安全管理技术

在实际应用当中，对网络数据库进行安全管理，不但能保证数据库内数据信息的完整性和安全程度，而且能准确防止网络失效问题的产生，确保计算机网络系统稳定高效运行。在计算机网络数据库安全管理过程中，有关工作人员需要对实践经验进行归纳总结，并且对存在的问题进行准确探索，从不同角度对这项工作的可行性展开有效验证，进而制定出周密详细的管理计划。为了确保网络数据库的安全管理质量，首先要做的就是选择合适的安全管理技术；此时，数据库安全管理人员应从网络安全、管理安全、硬件安全等方面进行深入思考。

（一）网络安全技术

在计算机网络数据库管理当中，需要加大对网络安全技术的管理重视程度。在实际操作过程中，有关人员要保证网络安全技术作用价值最大化展现。在这种情况下，计算机网络数据库的安全管理人员就必须选择合适的安全管理技术，解决黑客攻击和病毒入侵等一系列干扰问题，把工作重心放在数据存储和传输管理当中。

1.防火墙技术

目前网络上的黑客和病毒比较猖獗，防火墙技术也成为防御病毒入侵行为的有效手段。在计算机网络和数据库安全管理当中，防火墙是最主要的安全屏障。采用防火墙技术，可以有效地抵御来自网络与外界的损害或者威胁，使内部系统维持稳定高效的运行状态；不管是防御黑客攻击，还是阻止信息泄漏防火墙都起到不可或缺的作用。一般而言，在使用防火墙技术的时候，要确

保防火墙的包过滤技术、加密技术、和代理服务器等不受损伤。在这种条件下，提出一种高可靠度设计的防火墙结构，并给出实现该体系的具体方法；还可以根据实际需要选择合适的防火墙技术等。

2.数据加密技术

数据加密技术是一种简单有效的保护数据库信息安全的方法和手段。在实际应用当中，数据加密技术可以为计算机网络数据库的安全管理打下坚实基础，能够最大限度地保障数据信息的安全性和完整程度[5]。在这种情况下，可以根据多种密钥对数据信息进行加密处置。在通讯方面计算机网络数据库的资料，必须采用极端的链路加密、节点加密及端对端加密传送方式。

3.数据备份技术

当计算机网络数据库遭到损害和攻击时，很可能会造成大量信息损失或者失效，这给计算机使用人员造成严重干扰和明显困惑。为了提高信息数据的安全性和可靠程度，有关部门必须对数据备份与恢复展开有效防护。计算机网络数据库在运行的过程中应具有实时备份和一键恢复的功能，这样在数据库被攻击后，可通过直接恢复技术，迅速、完整地恢复有关数据，避免数据遗漏缺失情况发生。

（二）管理安全技术

1.身份识别技术

数据不正当查阅和使用是造成数据信息丢失的主要原因，因此，在实际使用当中，必须重视对数据访问者的身份验证。目前，可供计算机网络数据库使用的身份认证技术主要有静态口令、数据签名、动态口令、生物特征识别等多种类型，而计算机使用人员在进入数据库时，首先要进行身份验证，否则将被当成非法入侵。当然，在数据库安全管理当中，除了数据库的存储和查阅，还应在数据使用过程中增加身份验证技术。一般情况下，计算机网络数据库中的数据都是分类存储的，在不同数据之间有相应的访问标准，很多数据只有通过系统许可验证才可以使用，因此，在进行数据上传、下载、复制等操作之前，还需要进行身份验证，做好操作权限的检验审核工作，保证数据库的安全性和完整程度都不受影响[6]。

2.病毒查杀技术

病毒查杀是清除数据库安全隐患和风险因素的主要手段，病毒查杀一般分为两种形式。在实际应用当中，计算机网络数据库安全管理人员需要安装病毒查杀软件，通过不同形式的查杀操作，寻找计算机网络数据库存在的不足和缺陷，避免网络数据库遭到不法分子侵害和窃取，同时需要做好系统安全维护与病毒追踪工作。此时需要及时更新病毒库、数据库的病毒查杀技术，确保计算机网络数据库安全目标有效落实。

（三）硬件安全技术

计算机网络数据库安全管理人员在选择硬件加密技术时，需要考虑以下几方面的问题。首先要加强对数据库安全管理的验证和防护，提高其安全等级；在此基础上，提出一种新的解决方法，把提高硬件系统的安全性和可靠性作为根本目标。目前，在计算机网络当中存在三种不同的安全管理方式：一种是分散式管理方式；第二是集中式管理；第三是静态管理模式[7]。在具体操作过程中，计算机网络数据库的安全管理人员要结合实际情况，选择合适的安全管理模式，以确保数据库安全管理质量达到预期成效。为了更好地保证数据信息的完整性和健康程度，必须加强对不同类别数据信息的差异化管理操作。在硬件维修过程中，有关人员应熟悉硬件设备的稳定运行标准，并且实行定期更换、定期维护等管理操作，确保硬件设备稳定高效运行。

结语

综上所述，随着信息技术的推广和使用，计算机网络数据库所包含的信息资料逐渐增多，在这种条件下，网络数据库的压力和负担也在明显增加，网络数据库管理难度和安全问题也逐渐上升，这对计算机网络技术的发展和推广起到明显干扰作用。因此，如何对数据库进行安全管理，已成为有关领域不得不思考的问题。管理人员要全面提高自己的运行维护能力。在实际管理当中，要加强对数据库安全防护的重视与关注，做好数据信息加密、身份认证和病毒预防控制等管理工作，提高病毒查杀和追踪技术的实用程度，采用各种方法来保证网络数据库平稳高效运行。

参考文献

[1]乔泽华.基于计算机网络数据库的安全管理技术研究[J].信息记录材料，2022，23（01）：83-85.

[2]郭海燕.计算机网络数据库的安全管理技术策略研究[J].江西电力职业技术学院学报，2020，33（7）：23-24.

[3]赵鑫.试论计算机网络数据库的安全管理技术[J].现代信息科技，2019，3（01）：97-99.

[4]肖楠.计算机网络数据库的安全管理技术研究[J].科学技术创新，2020，14（20）：95-96.

[5]程力.计算机网络数据库的安全管理技术分析[J].网络安全技术与应用，2022，9（12）：46-48.

[6]张驰，李策，王华.计算机网络数据库安全管理技术的优化分析[J].中国新技术新产品，2020，10（22）：143-145.

[7]郭轶卓.计算机网络数据库的安全管理技术分析[J].产业与科技论坛，2020，19（12）：63-64.