 DOI: https://doi.org/10.26549/bdai.v4i5.14760

Analysis of Security Management Techniques for Computer Networks and Databases

Ning Kang

China Telecom Fuzhou Branch, Fuzhou, Fujian, 350005, China

Abstract

The paper deeply analyzes various security issues faced by computer networks and databases, and explores a series of corresponding security management technologies. By understanding and mastering these technologies, computer networks and databases can be better protected and secure, ensuring the confidentiality, integrity and availability of data. This paper discusses key areas such as computer network and database security management construction, virus protection technology, access control technology, recovery and backup technology, data encryption technology, audit tracking and attack determination technology, and identity authentication technology, it is hoped to provide readers with a comprehensive and effective security management strategy to ensure the safe operation of computer networks and databases.

Keywords

computer networks; database; security management

计算机网络与数据库的安全管理技术分析

康宁

中国电信福州分公司，中国·福建 福州 350005

摘　要

论文深入分析计算机网络和数据库面临的各种安全问题，并探讨一系列相应的安全管理技术。通过了解和掌握这些技术，可以更好地保护计算机网络和数据库的安全，确保数据的机密性、完整性和可用性。论文讨论计算机网络和数据库的安全管理建设、病毒防护技术、控制访问技术、恢复与备份技术、数据加密技术、审计追踪与攻击测定技术以及身份认证技术等关键领域，希望能为读者提供一套全面而有效的安全管理策略，以保障计算机网络和数据库的安全运行。

关键词

计算机网络；数据库；安全管理

1 计算机网络数据库发展趋势

随着信息技术的不断发展和进步，计算机网络数据库已成为各个领域中重要的信息存储和处理工具。计算机网络数据库将面临诸多挑战和机遇，其发展趋势将更加明显。论文从数据隐私化和数据商业化两个方面，详细探讨计算机网络数据库的未来发展趋势。

1.1 数据隐私化

随着互联网的普及和信息技术的不断发展，个人和企业信息泄露事件频繁发生，人们对数据隐私保护的重视程度越来越高。因此，计算机网络数据库在未来的发展中，将更加注重数据隐私保护，采取更加安全的数据加密和隐私保护技术，以确保数据的安全性和保密性。

1.2 数据加密技术

数据加密技术是保护数据隐私的重要手段之一。未来几年，计算机网络数据库将采用更加先进的数据加密技术，如全同态加密、属性基加密等，以实现数据的加密存储和传输，防止数据被非法获取和利用。

1.3 隐私保护技术

隐私保护技术是保护个人隐私的重要手段之一。未来几年，计算机网络数据库将采用更加先进的隐私保护技术，如差分隐私、联邦学习等，以实现数据的隐私保护和数据分析，避免个人信息被泄露和滥用。

2 数据商业化

随着大数据时代的到来，数据已经成为一种重要的资产和资源。因此，计算机网络数据库将更加注重数据的商业化和价值挖掘，以实现数据的最大化和最大化。

2.1 数据资产化

数据资产化是指将数据作为一种资产进行管理和利用。另外，计算机网络数据库将采用更加先进的数据资产化管理方法，如数据湖、数据仓库等，以实现数据的集中管理和利

【作者简介】康宁（1973–），男，中国湖南涟源人，本科，工程师，从事信息安全与数据库管理研究。

用，提高数据的商业价值和竞争力。

2.2 数据服务化

数据服务化是指将数据作为一种服务进行提供和使用。因此，计算机网络数据库将采用更加先进的数据服务化技术，如云计算、大数据分析等，以实现数据的快速响应和高效利用，提高数据的商业价值和竞争力。

2.3 数据驱动决策

数据驱动决策是指以数据为基础进行决策和管理。此外，计算机网络数据库将采用更加先进的数据驱动决策方法，如数据挖掘、人工智能等，以实现数据的深度分析和智能决策，提高企业的商业价值和竞争力。

未来几年，计算机网络数据库的发展趋势将更加注重数据隐私化和商业化。通过采用先进的数据加密技术和隐私保护技术，确保数据的安全性和保密性；同时通过采用先进的数据资产化、数据服务化和数据驱动决策等技术，实现数据的最大化和最大化。随着信息技术的不断发展和进步，计算机网络数据库将在各个领域中发挥更加重要的作用，将成为推动经济社会发展的重要力量 [1]。

3 计算机网络数据库面临的各类安全问题分析

随着信息技术的迅速发展和广泛应用，计算机网络数据库已成为企业和个人日常信息管理的重要工具。然而，随着网络环境的复杂性和数据量的增加，计算机网络数据库面临着越来越多的安全问题。论文将深入分析计算机网络数据库所面临的硬件性能问题、黑客攻击问题、计算机漏洞和病毒入侵等安全问题。

3.1 硬件性能问题

①数据存储和处理能力不足。随着数据的快速增长，原有的硬件设备可能无法满足数据存储和处理的需求，导致数据丢失或处理延迟。例如，当数据库服务器无法承受大量数据的读写操作时，可能会出现性能瓶颈，从而影响到数据库的稳定性和可用性 [2]。

②网络设备性能瓶颈。网络设备的性能不足，如路由器、交换机等，可能会造成数据传输的瓶颈，影响数据的安全性和完整性。例如，在数据传输过程中，如果网络设备出现性能问题，可能会导致数据丢失或损坏，给企业和个人带来不可预测的损失。

3.2 黑客攻击问题

①恶意攻击。黑客可能会利用网络漏洞，侵入计算机网络数据库，窃取、篡改或删除数据，给企业和个人带来严重的损失。这种攻击行为通常具有隐蔽性，难以被用户及时发现和防范。

②钓鱼攻击。黑客通过伪造合法网站或邮件，诱骗用户输入敏感信息，如用户名、密码等，进而获取非法访问权限。这种攻击方式常常导致用户信息泄露和系统被非法入侵。

③勒索软件攻击。黑客利用恶意软件感染计算机网络数据库，对数据进行加密或锁定，然后向用户索取赎金以获取解密或解锁密钥。这种攻击方式不仅会对数据库造成严重破坏，还会给企业和个人带来经济和声誉上的损失。

3.3 计算机漏洞

①软件漏洞。操作系统、数据库管理系统等软件中的漏洞，可能会被黑客利用，导致数据泄露或系统崩溃。这些漏洞可能源于软件设计缺陷、编程错误或者恶意软件植入等。

②配置漏洞。网络设备的配置错误，如防火墙规则、路由器设置等，可能会让黑客有机可乘，入侵计算机网络数据库。这些配置漏洞可能源于管理人员的安全意识不足或者操作失误。

③物理环境漏洞。例如，门禁系统漏洞、监控设备缺失等，可能让未经授权的人员进入数据中心，对计算机网络数据库造成威胁。这些物理环境漏洞可能给黑客提供入侵机会或者直接导致数据泄露 [3]。

3.4 病毒入侵

①恶意软件感染。病毒、木马等恶意软件可能会感染计算机网络数据库，窃取、篡改或删除数据，甚至破坏系统运行。这些恶意软件可以通过各种途径传播，如网络下载、移动设备等。

②文件传输病毒。病毒可以通过文件传输进入计算机网络数据库，造成数据泄露或系统损坏。当用户在不知情的情况下下载了带有病毒的文件时，病毒可能会自动传播并感染数据库。

③网络传播病毒。病毒可以通过网络传播，感染其他计算机和设备，进一步扩大对计算机网络数据库的威胁。这种病毒可能会在短时间内迅速传播，给整个网络环境带来严重威胁。

计算机网络数据库面临着来自硬件性能、黑客攻击、计算机漏洞和病毒入侵等多方面的安全问题。为了应对这些威胁，需要建立完善的安全管理制度，增强安全防范意识，采用先进的安全技术手段这些安全问题不仅会威胁到企业和个人的信息安全和财产安全，还会对整个社会的稳定和发展产生负面影响。因此必须采取有效的措施来保护计算机网络数据库的安全性和可靠性以确保数据的机密性、完整性和可用性。

4 安全管理技术在计算机网络数据库中的应用策略

随着信息技术的快速发展，计算机网络数据库已成为企业和个人信息存储和处理的重要工具。然而，网络环境的复杂性和数据的重要性决定了计算机网络数据库面临诸多安全问题。为了保障计算机网络数据库的安全性和可靠性，需要采用一系列安全管理技术。

4.1 计算机网络数据库安全管理建设

计算机网络数据库安全管理建设是保障数据库安全的

基础，包括以下几个方面：

建立完善的安全管理制度：制定并执行一系列安全操作规程，包括用户管理、密码策略、数据备份等，确保数据库的安全运行。

定期进行安全审计和风险评估：通过对数据库系统的安全审计和风险评估，发现潜在的安全隐患，及时采取措施进行修复和防范。

强化物理环境安全：确保数据中心的安全设施完善，如门禁系统、监控设备等，防止未经授权的人员进入。

建立灾备中心：为防止意外事故导致的数据丢失或损坏，建立灾备中心进行数据备份和恢复。

4.2 计算机网络数据库病毒防护技术

病毒防护技术是防止病毒入侵计算机网络数据库的关键。以下是几点建议：

安装杀毒软件：为所有计算机和服务器安装杀毒软件，并及时更新病毒库，以便在第一时间检测和清除病毒。

定期进行安全检查：定期对计算机系统和网络设备进行安全检查，发现并修复潜在的安全漏洞。

加强文件传输管理：限制文件传输权限，避免用户随意下载和打开未知来源的文件，防止病毒通过文件传播。

实施访问控制策略：根据用户的角色和权限，限制其对特定文件和资源的访问，降低感染病毒的风险。

4.3 计算机网络数据库控制访问技术

控制访问技术是防止非法访问计算机网络数据库的重要手段。以下是几点建议：

实施严格的身份认证：要求用户进行身份认证才能访问数据库，确保只有授权用户能够访问敏感数据。

划分用户权限：根据用户角色和需求，为其分配适当的权限，限制其对数据库的访问和操作。

审计和监控：对用户的访问行为进行审计和监控，发现并记录异常操作，及时采取措施进行防范。

加密敏感数据：对敏感数据进行加密存储，防止未经授权的用户获取和利用这些数据 [4]。

4.4 计算机网络数据库恢复与备份

恢复与备份技术是保障计算机网络数据库安全的重要措施。以下是几点建议：

定期备份数据：按照一定的周期性策略，对数据进行备份，确保数据的完整性和可恢复性。

异地备份：将备份数据存储在异地安全位置，防止意外事故导致的数据丢失或损坏。

恢复策略制定：制定完善的数据恢复策略，包括应急响应计划和恢复步骤，以便在发生故障或灾难时快速恢复数据。

数据归档：将不再使用的数据进行归档处理，以释放存储空间并确保数据的可访问性。

4.5 计算机网络数据库数据加密技术

数据加密技术是保护计算机网络数据库中数据隐私的关键。以下是几点建议：

使用加密算法：选择合适的加密算法对数据进行加密存储和传输，如对称加密算法或非对称加密算法。

加密敏感数据：对敏感数据进行加密处理，确保只有授权用户能够解密和访问这些数据。

保护密钥安全：采用安全的密钥管理策略，确保密钥的生成、存储和使用过程都受到保护 [5]。

4.6 计算机网络数据库审计追踪与攻击测定

审计追踪与攻击测定技术可以有效地检测和防止计算机网络数据库被攻击和篡改。以下是几点建议：

开启审计功能：在计算机网络数据库中开启审计功能，记录所有用户的访问和操作行为，形成审计日志。

定期审计：定期对审计日志进行审计和分析，发现异常操作和潜在的安全威胁。

攻击测定：采用攻击测定技术，实时监测网络流量和数据库活动，及时发现并阻止潜在的攻击行为。

安全事件响应：制定安全事件响应计划，一旦发现安全威胁，立即采取措施进行响应和处理，确保数据库的安全性和完整性。

4.7 计算机网络数据库身份认证技术

身份认证技术可以确保计算机网络数据库中数据的机密性和完整性。以下是几点建议：

使用强密码策略：要求用户设置复杂且不易被猜测的密码，避免使用弱密码或默认密码。

多重身份认证：采用多重身份认证方式，如密码加短信验证、指纹识别等，提高身份认证的安全性。

定期更换密码：要求用户定期更换密码，防止密码被破解或泄露。

加密传输数据：在数据传输过程中使用加密技术，确保数据在传输过程中的机密性和完整性。

综上所述，安全管理技术在计算机网络数据库中的应用策略是保障数据库安全的重要手段。通过建立完善的安全管理体系、采用病毒防护技术、控制访问技术、恢复与备份技术、数据加密技术、审计追踪与攻击测定技术以及身份认证技术等措施，可以有效提高计算机网络数据库的安全性和可靠性，确保数据的安全存储和处理。

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(1):23.

[2] 苏华.计算机网络数据库安全管理技术的优化[J].计算机与网络,2021(2).

[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(1):3.

[4] 陈建锋.计算机网络数据库的安全管理技术[J].电子技术与软件工程,2019(1).

[5] 宋俊苏.计算机网络数据库的安全管理技术分析[J].信息技术与信息化,2019(5).