

计算机数据库系统在信息管理中应用 面临的挑战与对策

耿国钊

北京理工大学，北京 海淀 100080

摘要：在数字化时代，计算机数据库系统面临着严峻的网络安全威胁，这些威胁对数据库系统的安全构成了重大挑战，可能导致严重的后果。网络病毒是常见的安全威胁之一，它们具有极强的传播能力和破坏性。例如，勒索病毒通过网络传播，感染计算机系统后，对数据库中的数据进行加密，使其无法正常访问，并向用户索要赎金。一旦数据库感染勒索病毒，企业或组织可能会面临数据丢失、业务中断等严重后果。

关键词：计算机；数据库；信息管理

1 网络安全威胁

黑客攻击也是数据库系统安全的重要威胁。黑客通过各种技术手段，如 SQL 注入、漏洞利用等，试图获取数据库中的敏感信息、篡改数据或破坏数据库系统的正常运行。SQL 注入攻击利用应用程序对用户输入数据验证不足的漏洞，将恶意的 SQL 语句插入到应用程序的输入参数中，从而获取数据库的访问权限，执行非法操作。据统计，SQL 注入攻击是导致数据库安全事件的主要原因之一，许多知名企业都曾遭受过 SQL 注入攻击，导致用户信息泄露、财务数据被篡改等严重后果。

数据泄露同样不容忽视，它可能由内部人员的不当操作、外部攻击或系统漏洞等原因引起。一旦数据泄露，个人隐私信息、商业秘密等敏感数据可能被非法获取和利用，给个人和企业带来极大的损失。例如，2018 年，美国社交平台 Facebook 发生数据泄露事件，涉及约 8700 万用户的个人信息被泄露，这一事件引发了全球范围内的关注和担忧，对 Facebook 的声誉和业务造成了严重影响。数据泄露不仅会损害企业的商业信誉，还可能引发法律纠

纷，使企业面临巨额的赔偿责任。

网络安全威胁对数据库系统的稳定性和可靠性也会产生负面影响，导致系统性能下降、服务中断等问题。当数据库系统遭受攻击时，可能会出现数据丢失、数据损坏等情况，影响信息管理的准确性和完整性。频繁的安全威胁还会增加企业和组织在安全防护方面的投入，包括安全设备的购置、安全技术的研发、安全人员的培训等，增加了运营成本。

2 数据模型局限性

随着信息技术的快速发展，数据的复杂性和多样性不断增加，现有数据模型在处理复杂数据和满足多样化需求时逐渐暴露出一些局限性。在处理复杂数据方面，传统的数据模型如关系模型，主要适用于结构化数据的存储和处理，对于非结构化数据（如文本、图像、音频、视频等）和半结构化数据（如 XML、JSON 格式的数据）的处理能力相对有限。关系模型以二维表格的形式组织数据，要求数据具有严格的结构和模式，而大量的非结构化和半结构化数据难以按照这种模式进行存储和管理。在社交媒体平台上，用户发布的文本内容、上

传的图片和视频等数据，具有高度的灵活性和多样性，难以用关系模型进行有效的组织和分析。

对于复杂的业务场景，现有数据模型在表达数据之间的复杂关系时也存在不足。例如，在物联网应用中，设备之间存在着复杂的交互关系和实时动态数据，传统的数据模型难以准确描述这些关系和处理实时数据。物联网中的传感器设备会实时产生大量的数据，这些数据之间存在着时间序列关系、因果关系等复杂关系，关系模型在处理这些关系时效率较低，无法满足物联网应用对实时性和数据处理能力的要求。

在满足多样化需求方面，不同的应用场景对数据模型有着不同的要求，单一的数据模型往往难以满足所有需求。在大数据分析领域，需要数据模型能够支持海量数据的高效存储和快速查询；在人工智能应用中，需要数据模型能够支持数据的深度学习和智能分析。目前的数据库系统通常采用单一的数据模型，难以在不同的应用场景中都达到最佳性能。关系数据库在处理结构化数据的事务处理方面表现出色，但在处理海量非结构化数据的分析任务时，性能会受到限制；而 NoSQL 数据库虽然在处理非结构化数据和高并发读写方面具有优势，但在事务处理和数据一致性方面存在不足。

3 用户安全意识薄弱

用户安全意识薄弱是计算机数据库系统在信息管理中面临的一个重要问题，它可能导致一系列安全隐患，给数据库系统的安全带来风险。许多用户在使用数据库系统时，存在操作失误的情况，如误删除重要数据、误修改数据结构等。这些操作失误可能是由于用户对数据库系统的操作不熟悉、粗心大意或缺乏相关的培训和指导引起的。在企业的数据库系统中，员工可能因为不了解数据库的操作规范，误删除了关键业务数据，导致业务无法正常进

行，给企业带来经济损失。

用户在设置密码时，往往存在密码强度不足的问题，如使用简单的数字、字母组合，或者使用与个人信息相关的密码，这些密码容易被破解，从而导致账号被盗用，数据库中的数据面临泄露风险。据统计，许多数据泄露事件是由于用户密码被破解引起的。用户还存在密码保管不当的情况，如将密码写在纸上、在不安全的网络环境中输入密码等，这些行为都增加了密码被窃取的可能性。

用户对网络安全风险的认识不足，容易受到钓鱼邮件、社交工程攻击等威胁。钓鱼邮件通常伪装成合法的邮件，诱使用户点击链接或下载附件，从而获取用户的账号密码等敏感信息。社交工程攻击则通过欺骗用户，获取用户的信任，从而获取数据库系统的访问权限。一些用户在收到钓鱼邮件时，由于缺乏警惕性，点击了邮件中的链接，导致账号被盗用，数据库中的数据被泄露。用户在使用公共网络时，也容易忽视网络安全问题，如在公共 WiFi 环境中进行敏感数据的传输，这可能导致数据被窃取或篡改。

4 加强网络安全防护

为有效应对网络安全威胁，应采取一系列综合性的网络安全防护措施，构建多层次、全方位的安全防护体系，确保计算机数据库系统的安全稳定运行。

在技术层面，防火墙和入侵检测系统（IDS）/入侵防御系统（IPS）是网络安全防护的重要防线。防火墙作为网络访问的控制设备，应合理配置其规则，严格限制对数据库系统的访问权限，只允许合法的网络流量通过，阻止未经授权的访问和恶意攻击。例如，在企业网络中，应将防火墙部署在数据库服务器与外部网络之间，根据企业的业务需求和安全策略，设置访问规则，禁止外部网络直接访问数据库服务器的敏感端口，如数据库默认端口等。同时，应定期更新防火墙的规则库，以应

对不断变化的网络安全威胁。

IDS/IPS 能够实时监测网络流量，及时发现并防范入侵行为。应确保 IDS/IPS 的正常运行，定期更新其特征库，以识别最新的攻击模式。当 IDS 检测到异常流量或攻击行为时，应及时发出警报，通知管理员采取相应的措施；IPS 则应具备自动阻断攻击源的能力，防止攻击进一步扩散。例如，当 IDS 检测到有大量来自某个 IP 地址的异常数据库查询请求，可能是遭受了 SQL 注入攻击时，应立即发出警报，并通知管理员进行调查；IPS 则应自动阻断该 IP 地址的访问，保护数据库系统免受攻击。

加密技术在保障数据安全方面发挥着关键作用。对于数据库中的敏感数据，如用户账号密码、财务数据、个人隐私信息等，应采用先进的加密算法进行加密存储，确保数据在存储过程中的安全性。在数据传输过程中，应使用安全的传输协议，如 SSL/TLS 协议，对数据进行加密传输，防止数据被窃取或篡改。例如，在电商平台中，用户的登录信息和交易数据在传输过程中应通过 SSL/TLS 协议进行加密，确保数据的机密性和完整性。同时，应妥善管理加密密钥，采用密钥管理系统（KMS）对密钥进行生成、存储、分发和更新，确保密钥的安全性和可用性。

除了技术措施，还应建立健全网络安全管理制度，加强对网络安全的管理和监督。制定详细的网络安全策略和操作规程，明确各部门和人员在网络安全方面的职责和权限，确保网络安全措施的有效实施。定期对网络安全进行评估和审计，及时发现并整改安全隐患。例如，企业应制定网络安全管理制度，规定员工在使用数据库系统时的安全要求，如定期更换密码、不随意点击可疑链接等；定期对网络安全进行评估，检查防火墙、IDS/IPS 等安全设备的运行状态，以及数据加密、访问控制等安全措施的执行情况，发现问题及时整改。同时，应加强对网络安全事件的应急响应能力，制定

应急预案，定期进行演练，确保在发生安全事件时能够迅速、有效地进行处理，减少损失。

5 创新数据模型

为突破现有数据模型的局限性，满足日益复杂的数据管理需求，需要积极创新数据模型，探索新的数据组织和处理方式，提高数据库系统对复杂数据和多样化业务场景的适应性。

一方面，可以结合多种数据模型的优势，构建融合数据模型。例如，将关系模型的结构化和查询优势与图模型的关系表达能力相结合，形成一种新的数据模型，以处理具有复杂关系的数据。在社交网络分析中，图模型能够清晰地表达用户之间的关系，但在处理结构化数据和事务处理方面相对较弱；而关系模型在处理结构化数据和事务处理方面具有优势，但在表达复杂关系时较为繁琐。通过将两者结合，可以更好地满足社交网络分析的需求，既能高效地存储和查询用户的基本信息等结构化数据，又能准确地表达用户之间的关系，进行社交网络分析和挖掘。

另一方面，积极开发新的数据模型，以适应特定的应用场景和数据特点。随着大数据和人工智能技术的发展，出现了一些新的数据模型，如面向列的数据模型、文档型数据模型等。面向列的数据模型适用于大数据分析场景，它将数据按列存储，能够提高数据的压缩率和查询效率，特别是在处理大规模数据的聚合和分析操作时具有明显优势。文档型数据模型则适合存储和处理半结构化的文档数据，如 JSON 格式的数据，它具有灵活的数据结构和快速的读写性能，在内容管理、日志分析等领域得到了广泛应用。在实际应用中，应根据具体的业务需求和数据特点，选择合适的数据模型或开发定制化的数据模型，以提高数据管理的效率和质量。例如，在物联网应用中，由于设备产生的数据具有实时性、多样性和海量性的特点，可以开发一种基于时间序列的数据模

型,专门用于存储和处理物联网设备产生的时间序列数据,以满足物联网应用对数据实时处理和分析的需求。同时,应不断探索新的数据模型和技术,如基于区块链的数据模型,利用区块链的去中心化、不可篡改等特性,提高数据的安全性和可信度,为数据管理带来新的思路和方法。

6 提高用户安全意识

提高用户安全意识是保障计算机数据库系统安全的重要环节,需要通过多种方式加强用户培训和宣传教育,使用户充分认识到数据安全的重要性,掌握正确的操作方法和安全防范措施,减少因用户安全意识薄弱而导致的安全风险。

开展定期的数据库安全培训是提高用户安全意识的有效途径。培训内容应涵盖数据库系统的基本操作规范、安全注意事项、常见安全威胁及应对方法等。例如,培训用户正确设置和保管密码,强调密码强度的重要性,建议用户使用包含字母、数字和特殊字符的复杂密码,并定期更换密码;教导用户如何识别钓鱼邮件,避免点击可疑链接或下载附件,防止账号被盗用;培训用户在使用数据库系统时,遵循最小权限原则,只获取完成工作所需的最小权限,减少因权限滥用导致的数据泄露风险。培训方式可以多样化,包括线上培训课程、线

下讲座、实际操作演练等,以提高培训的效果和用户的参与度。

利用宣传海报、内部邮件、安全提示等方式进行广泛的宣传教育,营造良好的数据安全文化氛围,也是提高用户安全意识的重要手段。在办公区域张贴数据安全宣传海报,展示数据安全的重要性和常见的安全风险,提醒用户时刻注意数据安全;通过内部邮件定期向用户发送数据安全提示,如最新的安全漏洞信息、安全防范措施等,让用户及时了解数据安全动态;在数据库系统登录界面或操作界面设置安全提示信息,如密码强度要求、防止钓鱼邮件的提醒等,时刻提醒用户注意安全操作。通过这些宣传教育方式,不断强化用户的数据安全意识,使数据安全成为用户的自觉行为。

建立有效的监督和激励机制,对用户的安全行为进行监督和评估,对遵守安全规定的用户给予奖励,对违反安全规定的用户进行惩罚,也有助于提高用户的安全意识。例如,定期对用户的密码强度、操作行为等进行检查,对密码强度符合要求、操作规范的用户给予一定的奖励,如奖金、荣誉证书等;对使用弱密码、违规操作的用户进行警告或处罚,如扣除绩效分数、暂停使用数据库系统等。通过这种监督和激励机制,引导用户养成良好的安全习惯,提高用户对数据安全的重视程度。

参考文献

- [1] 王亮,张新建,杨春,等. 计算机数据库系统在信息管理中的运用探究[J]. 中国新通信,2023,25(7):104~106
- [2] 付强,王建霄. 农村信用信息管理中的计算机数据库技术探讨[J]. 信息技术时代,2023,16:45~47
- [3] 宋家鹏. 医院信息管理中的计算机数据库技术探讨[J]. 计算机产品与流通,2023,5:207~209
- [4] 罗晓璐. 计算机数据库系统在信息管理中的实践思考[J]. 电脑采购,2023,2:7~9
- [5] 汤琳燕. 计算机数据库系统在信息管理中的应用[J]. 无线互联科技,2022,19(7):113~115