网络安全视角下医院信息管理计算机数据库技术分析

高景峰[1] 施健琛[2]
1. 中国人民武装警察部队黑龙江省总队医院 黑龙江 哈尔滨 150010
2. 中国人民武装警察部队福建总队机动支队 福建 福州 350500

摘 要：随着信息技术在医疗领域的广泛应用，医院信息管理系统中的计算机数据库承载着大量敏感的患者信息、医疗数据等重要资源。本论文从网络安全的视角出发，深入分析医院信息管理中的计算机数据库技术，然后详细探讨保障数据库安全的计算机数据库技术，通过实际案例分析这些技术在医院信息管理中的应用效果，并针对现存问题提出优化建议，主要提高医院信息管理计算机数据库的安全性，确保医疗信息资源的可靠存储与合法使用，促进医疗信息化的健康发展。

关键词：网络安全；医院信息；信息管理；数据库分析

1 医院信息管理数据库的重要性

1.1 医疗服务角度

从医疗服务的角度来看，数据库存储着海量的患者医疗信息，这些信息涵盖患者的基本信息，如姓名、年龄、性别、过敏史等，以及详细的诊疗记录，包括病史、症状、诊断结果、治疗方案、用药情况等。医生在接诊患者时，能够快速从数据库中获取这些信息，从而做出更加准确、全面的诊断。例如，对于患有多种慢性疾病的患者，医生可以通过查询数据库，了解其过往的用药反应和治疗效果，避免重复用药或采取不恰当的治疗手段。这大大提高了医疗服务的质量和效率，减少了误诊和漏诊的可能性。

1.2 医院管理运营方面

在医院的管理运营方面，数据库具有举足轻重的地位，其包含了医院的人力资源信息，如医护人员的资质、排班情况、工作量统计等，通过这些数据，医院管理者可以合理安排人员，优化工作流程，提高人力资源的利用效率，同时数据库还存储着医院的财务信息，包括医疗收费标准、医保报销情况、成本核算等。这些数据有助于医院进行财务管理，确保医院的经济稳定和可持续发展。

1.3 医院信息管理方面

医院信息管理数据库对于医疗研究也意义非凡，大量的临床数据是医学研究的宝贵资源。研究人员可以从数据库中筛选出符合研究条件的病例，进行流行病学研究、疾病发病机制探索以及新药研发等工作。例如，通过分析特定疾病患者的大量数据，研究人员发现新的疾病相关因素或治疗靶点，为医学的进步提供有力支持。

2 网络环境下医院信息管理数据库面临的安全威胁

2.1 外部威胁

2.1.1 网络攻击

黑客入侵是医院信息管理数据库面临的严重外部威胁之一，黑客出于获取患者隐私数据以进行非法售卖、破坏医院正常运营或者进行恶意勒索等目的，试图突破医院数据库的安全防护系统。他们利用系统漏洞，如操作系统、数据库管理系统或者网络应用程序中的安全缺陷，通过植入恶意软件、发动拒绝服务攻击（DoS）等手段来入侵数据库。例如，黑客发动DDoS攻击，使医院的网络服务瘫痪，导致医护人员无法正常访问数据库获取患者信息，严重影响医院的日常医疗服务。

2.1.2 恶意软件

病毒、蠕虫和特洛伊木马等恶意软件通过多种途径入侵医院网络并感染数据库系统。例如，医院员工在不经意间从互联网上下载了被感染的文件，或者点击了包含恶意软件的广告链接，这些恶意软件一旦进入医院网络，就会搜索数据库中的敏感信息，进行数据篡改或者将数据发送给外部的恶意攻击者。它们还破坏数据库的正常运行机制，导致数据丢失或者系统崩溃。

2.1.3 云服务风险

随着越来越多的医院将部分或全部信息存储在云端，云服务提供商的安全漏洞也成为了医院数据库面临的外部威胁。如果云服务提供商的安全措施不到位，如数据加密算法被破解、身份认证系统被绕过等，那么医

作者简介：高景峰（1995年6月— ），本科，信息科助理工程师，主要研究方向为计算机科学与技术、可与医疗方面结合。

施健琛（1995年9月— ），男，福清市人，本科，计算机助理工程师，主要研究方向为计算机技术。

院存储在云端的数据库信息就面临泄露的风险。此外，云服务提供商的员工也存在违规操作的风险，从而危及医院数据库的安全。

2.2 内部威胁

2.2.1 员工误操作

医院员工在日常使用数据库过程中，由于缺乏足够的培训或者疏忽大意而发生误操作，例如，在数据录入时输入错误的患者信息，会影响后续的诊断和治疗。或者在进行数据库维护操作时，误删除重要的数据表或文件，导致数据丢失。这种误操作虽然大多是无意的，但却对数据库的完整性和可用性造成严重的损害。

2.2.2 内部人员恶意行为

尽管这是一种相对较少但危害极大的内部威胁，个别内部员工出于私利，如为了获取患者的隐私数据进行贩卖或者为了报复医院而对数据库进行恶意破坏。他们由于熟悉医院的内部网络环境和数据库结构，能够更容易地绕过一些常规的安全防护措施。例如，内部员工利用自己的权限修改数据库中的财务数据，或者删除患者的关键诊疗记录，从而给医院的运营、患者的权益以及医疗安全带来严重的危害。

3 保障医院信息管理数据库安全的计算机数据库技术

3.1 访问控制技术

首先，访问控制技术能够对用户的身份进行精确识别。在医院环境中，存在着多种类型的用户，包括医生、护士、行政人员、技术维护人员等。通过用户名、密码以及身份验证机制，系统可以区分不同用户的身份。例如，医生需要访问患者的病历以进行诊断和治疗，而行政人员则更多地关注医院资源管理等方面的数据，访问控制技术确保只有被授权的医生才能查看特定患者的医疗信息，防止信息的不当获取；其次，基于角色的访问控制（RBAC）在医院数据库管理中有着广泛的应用。不同的角色被赋予不同的权限集。以护士为例，她们可以查看患者的基本护理信息、生命体征记录等，但无法修改某些关键的诊断结果。这种基于角色的权限分配方式既方便了管理，又增强了安全性，当有人员岗位变动时，只需调整其角色对应的权限，而无需对每个单独的用户权限进行繁琐的修改；再者，访问控制技术还能够限制用户对数据库的操作类型。一些用户只有读取数据的权限，而另一些被允许进行数据的写入、更新或删除操作。比如，实习医生只能查看病例资料进行学习，而主治医生则能够对病例中的治疗方案进行更新和完善。这有效地防止了数据被恶意或无意地篡改，维护了医院信息的完整性和准确性。

3.2 数据加密技术

一方面，对称加密算法在医院数据库安全中有其独特的应用。这种加密方式使用相同的密钥进行加密和解密操作。例如，在医院内部网络传输患者的敏感数据时，如患者的身份证号码、家庭住址等，通过对称加密算法将这些数据加密成一串看似无规律的字符。只有拥有正确密钥的接收方才能将其还原为原始数据，对称加密算法具有加密速度快的优点，能够满足医院大量数据传输和存储时的实时加密需求；另一方面，非对称加密算法也不可或缺。它使用一对密钥，即公钥和私钥。公钥可以公开，用于加密数据，而私钥则只有特定的接收者持有，用于解密数据。在医院与外部机构（如医保部门、科研机构等）进行数据交互时，非对称加密算法就发挥了重要作用。当医院向医保部门发送患者的医疗费用结算信息时，使用医保部门提供的公钥进行加密，医保部门收到后再用自己的私钥解密。这样即使数据在传输过程中被截取，没有私钥的第三方也无法获取其中的内容，保障了数据的保密性。

3.3 备份与恢复技术

在日常运营中，医院数据库面临着各种各样的威胁，如硬件故障、软件错误、人为误操作以及自然灾害等。定期的数据备份能够确保在这些意外情况发生时，数据不会永久丢失。医院可以根据自身的数据量大小和重要性，制定不同的备份策略。例如，对于患者的病历数据，需要每天进行全量备份或者增量备份，全量备份是对整个数据库进行备份，而增量备份则只备份自上次备份以来发生变化的数据，这样既能够保证数据的完整性，又能够节省存储空间和备份时间。当灾难发生时，恢复技术就开始发挥作用。恢复过程需要精心设计和严格执行。从备份介质（如磁带、磁盘阵列等）中提取数据，并将其还原到数据库系统中。这一过程需要确保数据的一致性和完整性。例如，如果在备份后数据库中有部分数据已经更新，在恢复时需要按照正确的顺序和逻辑将这些更新合并到恢复的数据中。

4 优化医院信息管理数据库网络安全的建议

4.1 技术层面

4.1.1 强化加密技术

对医院信息管理数据库中的敏感数据，如患者的医疗记录、财务信息等，采用高级加密标准（AES）等强加密算法进行加密。在数据传输过程中，确保数据以密文形式传输，防止数据在网络传输过程中被窃取或篡改。例如，在医院的远程医疗数据传输场景中，医生与患者之间传输的诊断图像和病历信息都应经过加密处理，只

有接收端使用正确的密钥才能解密查看。

4.1.2 防火墙升级与优化

建立多层次的防火墙体系，不仅要在医院网络的边界设置防火墙，还要在内部网络的关键区域设置内部防火墙。定期更新防火墙规则，阻挡外部恶意网络流量的入侵，同时对内部网络的异常流量进行监测和限制。比如，根据医院不同部门的网络访问需求，设置精确的访问控制规则，允许医疗部门正常访问医疗影像数据库，而限制行政部门不必要的访问权限。

4.1.3 入侵检测与预防系统（IDPS）

部署先进的IDPS系统，它能够实时监控网络活动，识别潜在的入侵行为，如恶意软件攻击、端口扫描等，并及时发出警报。同时，IDPS还可以采取主动防御措施，如阻断可疑的网络连接。以医院数据库遭受暴力破解密码攻击为例，IDPS能够迅速检测到异常的登录尝试频率，并在短时间内阻止攻击源的进一步访问。

4.2 管理层面

4.2.1 人员安全意识培训

对医院全体员工开展网络安全意识培训，包括医护人员、行政人员和信息技术人员等。培训内容涵盖网络安全基础知识、密码安全、防范网络钓鱼攻击等。例如，通过模拟网络钓鱼邮件攻击的方式，让员工亲身体验网络攻击的手段，提高他们的防范意识。同时，定期进行网络安全知识考核，确保员工对安全知识的掌握程度。

4.2.2 安全管理制度完善

制定全面的医院信息管理数据库安全管理制度，明确各部门和人员在网络安全中的职责。例如，规定信息技术部门负责数据库的日常维护和安全技术措施的实施，医疗部门负责确保医护人员在使用医疗信息系统时遵守安全规定。制度还应涵盖对数据访问权限的严格管理，根据员工的工作职能分配最小化的访问权限，防止数据泄露风险。

4.2.3 应急响应预案

建立完善的网络安全应急响应预案，明确在数据库遭受网络攻击、数据泄露等安全事件时应采取的措施。应急响应团队应包括信息技术专家、医院管理人员和相关业务部门代表等。当发生安全事件时，能够迅速启动预案，进行事件评估、遏制、恢复和总结等工作。例如，若发现医院数据库存在数据泄露风险，应急响应团队应立即采取措施，隔离受影响的系统，调查事件原因，并及时通知相关监管部门和受影响的患者。

4.3 合作层面

4.3.1 与网络安全厂商合作

医院与专业的网络安全厂商建立长期合作关系，借助其专业的技术和研发力量，对医院信息管理数据库进行安全评估、漏洞检测和安全防护方案定制，网络安全厂商可以提供最新的安全技术产品和服务，如安全漏洞扫描工具、威胁情报共享等。例如，网络安全厂商定期对医院数据库系统进行全面的漏洞扫描，及时发现并修复潜在的安全漏洞，提高数据库的整体安全性。

4.3.2 行业内信息共享

医院之间应加强网络安全信息共享，成立行业网络安全联盟或参与相关的信息共享平台，通过共享网络安全威胁情报，如新型网络攻击手段、恶意软件样本等，各医院可以提前做好防范措施。例如，当一家医院遭受某种新型勒索病毒攻击时，及时将病毒的特征和攻击方式共享给其他医院，其他医院可以迅速采取防护措施，防止同样的攻击事件发生。

4.3.3 与高校及科研机构合作

医院与高校及科研机构开展合作，共同开展医院信息管理数据库网络安全方面的研究项目，高校和科研机构可以为医院提供理论支持和创新技术解决方案，医院则为研究提供实际的应用场景和数据支持。例如，共同研究基于人工智能的网络安全威胁检测技术，将其应用于医院数据库的安全防护中，提高医院应对复杂网络安全威胁的能力。

结语

医院信息管理计算机数据库的安全管理是一项复杂而重要的任务。我们必须从多个方面入手，采取综合措施，确保数据库的安全性和稳定性。只有这样，才能为医院的正常运行和患者的信息保护提供有力保障。同时，随着技术的不断发展和管理经验的不断积累，我们相信医院信息管理计算机数据库的安全管理将不断完善和提高。

参考文献

[1]郑文明,李浩.医院信息安全防护体系建设和实践[J].网络安全技术与应用,2024,(11): 103-105.

[2]戴智超,周燕,陈伟清.全流量分析技术在医院信息网络安全中的运用实践[J].电子产品世界,2024,31(11):50-53.

[3]袁稷梁.基于GPON的全光网络在智慧医院的应用[J].现代信息科技,2024,8(20): 5-9+14.

[4]孟晓阳,杨巍,张楠,等.医院近源网络攻击风险分析及对策建议[J].医学信息学杂志, 2024,45(09):87-90.

[5]郭兆瑞,石福汇.医院管理中计算机网络信息技术的应用探讨[J].中国设备工程,2024, (18):66-68.