医疗信息化系统架构优化与安全防护研究

常　刚
郑州大学第五附属医院　河南郑州　450052

摘　要：随着医疗信息化的发展，医疗系统面临着数据处理、系统性能和安全性等多方面挑战。本文提出了医疗信息化系统架构优化的相关内容及关键技术，并提出了对医疗信息化系统采用分布式设计、微架构和云等技术实施结构优化来改进效能和响应速度，满足大数据存储、大数据智能解析等大数据系统的要求。为了应对医疗信息化系统面临的安全问题，还提出了安全加密、网络安全、权限控制等安全防护解决方案，从而实现医疗信息化系统架构的优化，提高医疗服务运行效率、强化数据安全保障，以适应我国医疗技术快速发展与相关政策需求。文章旨在对医疗信息化系统结构的优化、安全防范提供指导与启发。

关键词：医疗信息化；系统架构优化；云计算；安全防护

引言

医疗信息化系统是现代化医疗服务的基础性建设，伴随着信息科学技术的不断进化和医疗市场需求的不断增长，医疗体系面临着愈益加大的压力。安全有效的医疗信息化系统可以提升医疗服务质量和效率，推动医疗行业的进一步发展。然而，当大量数据层出不穷时，传统的系统框架无法满足海量数据的高带宽、高速传输的数据处理和智能化数据挖掘的需求。同时，由于医疗信息网络安全的重要性日益显现，数据泄露、黑客攻击等安全风险正在侵害病人隐私以及系统安全性。因此，加强医疗信息系统的架构建设是提高医疗信息工作效率的重要发展方向，其中网络安全也成为一项至关重要的措施。

一、医疗信息化系统架构优化的必要性

1.提升系统性能与响应速度

在医疗信息化的发展过程中，医疗机构承担的数据量也在不断上升，系统性能提升对医疗机构工作服务效率与质量产生了关键因素。高效的系统能够根据客户的需求，及时地进行响应，对患者、医生及其他相关者的行为进行实时响应，减少因系统延时而导致的医疗差错概率。通过修改系统架构，采取更加新颖先进的系统方法，如压力缓冲平衡法、缓冲技术以及分层结构，可以显著提升系统的处理能力以及相应的响应速度，确保系统能够在高并行下持续高效地完成日常工作。优化过的系统既加快了数据的传输与处理的速度，也确保了系统和处理核心数据的有效共享，避免出现由于就诊时间过长的医疗系统给就诊患者带来的差旅时间拖延的问题，提升整个医疗服务质量和服务对象的就医感受。

2.支持大规模数据处理与智能分析

医疗信息化系统需要应对来自各个渠道纷繁复杂的各类数据，如患者历史数据、影像数据及检查检验数据等。数据不断增长将使传统的数据架构面临存储和处理能力的瓶颈。由此可以运用分布式架构、云计算和大数据分析处理的技术构建新的智慧医院数据架构，以更好地管理和处理大量的结构化和非结构性数据并及时获取数据以及智能化分析数据，从而使数据的存储与管理更方便且为智能学习和人工智能等技术的开发提供基础，以便实现医学的精准诊断和对未来情况的数据预测，从而全面提升医疗服务质量和科学性。

3.适应快速发展的医疗技术与政策需求

随着医学技术的发展和相关法律法规的日益健全，医疗信息系统应具备一定的可塑性及扩展性，以适应其中出现的各项变化。新工具、新技术的应用往往产生新的输入方式和数据结构需求，原有方案无法适应快速变化的需求，因此优化系统设计需要加强其可塑性，使其能够更加有效地整合不同医疗手段及政策。医疗信息管理系统应能够快速地应对新设备与系统的连接请求，保持其兼容性和稳定性。此外由于保密法规及医疗资料分享法令的常变性，医疗信息管理系统必须能够符合各项相关法令。对系统设计进行改进后，可以坚信医疗信息

作者信息：常刚，男（1983.11－），汉族，河南南阳人，硕士，无职称，研究方向：医疗信息化建设或网络与信息安全。

管理系统能够在快速发展的医疗产业环境下在面对政策及技术上产生更大的适应力及执行力，进而提升医疗服务成效及精细度。

二、医疗信息化系统架构优化的关键技术与方法

1. 分布式架构与云计算技术

分布式架构和云计算技术是医疗信息化系统架构优化的核心组成部分。因为医疗信息化系统数据正在日益庞大，单机集中式的架构已经不足以应付大规模并发和大数据量。使用分布式的架构方式，可以将系统各模块部署到不同的服务器节点上，实现数据、计算资源的集中管理，大幅增强系统并行性及扩展性，在此基础上，医疗信息化系统就能平均承担工作，在防止故障单点的前提下，保持高效率、稳定运行。云计算技术提供了变化性计算和存储资源，协助高效地管理与自动化、智能化的方式处理医疗信息数据。云平台可以在需要时自动扩展计算资源，医疗信息化系统会因为数据量增长或者处理数据的需要随时进行调整，以保证系统的稳定运行。同时云计算平台也保证很高的可用性和安全性，减少数据丢失或被盗取的风险，分布式架构和云计算结合，医疗信息化系统抵御海量并发和高负载量，提高了数据处理结果，增强了灵敏性和稳定性。

2. 微服务架构的应用与优化

微服务架构是一种新兴的信息系统设计模式，现已演变为提高医疗信息系统架构的主要技术手段。其将大型单体程序划分为诸多松散的、松散耦合的服务单元，每个单元执行单一的工作，并通过轻量级通信进行交互。与传统架构的整体现象相比，微服务架构更具弹性及扩展性，可适应医疗信息系统各科室及工作部分的自主研究、安装、维护需求。每一个服务单元可单独采用其技术方案且可按需求拓展或缩减。这种架构模型能进一步减弱系统的耦合性，提高开发和维护效率，同时强化系统的可扩展性和可容错性。此外，微服务架构的优化还涉及服务精细划小、对服务进行自动装配、容器管控和实时监控等工作，以确保系统能在高度并行、高负荷状态下顺利运行。微服务架构的应用赋予了医疗信息系统功能扩充、性能优化及安全性保护的优势，契合当前医疗服务复杂化的趋势要求。

3. 数据库管理与数据架构优化

在医疗信息化系统中，数据库管理与数据架构的优化是重要的影响因素，可提高数据储存有效性与搜索质量。面对信息量持续增多，而传统的数据库架构已不能满足数据的有效性操作。因此，运用分布式数据库、数据分割技术、改善搜索方式，可以有效提升数据库的容量存储与搜索速度。数据库架构的优化也包括了容纳各种形式的数据（如结构化的数据、非结构化的数据）并与之有效控制，在大数据量多用户等条件下，也可以使系统保持高效运行。同时合理的资料备份与灾难预防工作，也可以提高数据的安全性与可靠性，防止数据损失或损坏。

下表1对比了不同类型的数据库在医疗信息化系统中的应用及优劣。

表1　不同数据库类型对比

数据库类型	优点	缺点	适用场景
关系型数据库	结构化数据管理、强一致性、事务支持	扩展性差、处理大数据性能不足	结构化数据存储、事务管理
NoSQL数据库	高扩展性、适应非结构化数据	不支持复杂查询、缺乏事务管理	大数据处理、实时数据分析、日志记录
分布式数据库	高可扩展性、容错性强	实现复杂、成本较高	高并发访问、大数据量处理、跨区域数据管理

通过合理选择数据库类型和优化数据架构，医疗信息化系统能够更好地应对数据存储、处理和安全需求，提高整体系统的效率与稳定性。

4. 高可用性与容错技术

在医疗信息化系统中，高可用性与容错技术是保持系统稳定性和持续性的重要保证。由于医疗信息化系统要处理很多实时信息和做出必要的决定，如果服务停止或系统崩溃可能会导致病人治疗结果发生改变，因此系统的高可用性非常重要。高可用性技术通过冗余设计、负载均衡和容灾转移防止单个节点出错引起整个系统崩溃。容错技术主要是通过当硬件故障、网络中断等问题发生时保持系统的连续性运行，以最小化医疗服务中断的可能性。这些方法包括备份、自我修复和服务器端的即时监控等。采用分散的结构化容错技术，每个数据节点的服务单元之间可以做到故障隔离并且自动恢复，以保证医疗信息管理的长久性。在医疗信息管理系统结构中引入高可用性和容错技术，不仅可以增强系统的容错能力，还可给医院一个稳定的工作环境，免去病人信息内容更改不及时或者医疗过程不正常的尴尬局面。

三、医疗信息化系统的安全防护策略

1. 数据加密与隐私保护措施

数据加密和隐私保护是医疗信息化系统安全防护的核心内容。医疗数据中包含着许多敏感数据，如病人个

人信息、病人病例、就医历程等，如果这些数据外泄后将带来严重后果，不仅涉及病人本身，还会引发相关的法律和伦理问题。因此，要采用信息加密方式防止信息泄露。医院可采用最新的数据加密技术，如对称加密、非对称加密、哈希加密等确保数据在存储或者传输过程中不被泄露。不仅要对静态数据（存储在数据中的病人病历信息）进行加密，同时还要保护动态数据（储存在医院网络中流动作业的图像数据）。此外，为保障病人隐私，可以构建严格的数据访问控制策略和多层次的访问认证流程，只有具有权限的人员才能访问敏感数据，同时对数据做脱敏处理，对于在网上传播的数据，利用数据脱敏的方法对发表的数据进行处理，防止病人私人信息泄露，以此使医疗信息化系统避免数据被泄露、篡改或者非法使用，有效保护了病人隐私。

2.网络安全防护与防攻击技术

由于医疗系统中信息化的广泛运用，网络安全逐渐成为系统设计与优化的重要考量之一。为了防止被黑客攻击并保护安全信息的隐私性，医疗信息系统必须具备安全防御措施，并且采取网络安全的防御措施来保护系统的安全，包括防火墙、入侵检测系统（IDS）和密码通信协议等。防止恶意行为的工具技术也包括阻止大多数形式的常规网络攻击行为，如分布式拒绝服务攻击（DDoS攻击）等。为了衡量防护效果，可以使用以下公式来估算系统的安全性增强程度：

$$S=\frac{R\times(1-F)}{C} \quad (1)$$

其中，S表示系统的安全增强度，R为防护措施的覆盖率，F为系统的漏洞频率，C为修复漏洞的成本。通过该公式，可以评价不同安全防护措施对系统安全的影响，同时可以帮助医疗机构合理分配有限资源，提升网络安全防御能力。医疗信息系统要不断更新网络安全防范技术以防范新的安全风险，确保数据在传输以及存储过程中的安全。

3.访问控制与身份认证机制

身份认证、访问控制是医疗信息化系统最主要的保护机制，用以保护患者的隐私和其他关键数据信息。该机制能确保只有得到授权的用户才能访问特定的系统模块或者敏感数据。访问控制的常见模式包括基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC），通过根据使用者角色和地位来动态变化权限。关于身份验证方式，主要是对使用者进行身份验证并防止未经批准的使用者访问某个系统。使用多重认证（MFA）能提高认证的强度，防止密码被破解。同时，生物特征识别方法（指纹、面部识别等）也可以在身份验证阶段使用，以提高系统的安全性和灵活性。通过提高访问控制和认证措施，医疗信息化系统能够有效抵御数据泄露和非授权访问。

4.安全审计与合规性管理

在医疗信息化系统中，安全审查和合法化管理构成了保证数据机密性和系统合法性之基石，通过运用安全审查技术可以及时监测、分析系统发生的各项操作如用户注册、数据访问、数据修改等，以定位可能存在的风险因素，及时发现异常行为。建立完善的审计日志可使医院追踪、追溯整个过程，为其后期的探索和处理工作提供帮助。合法化管理要求医疗信息化系统需按照《个人信息保护法》《医疗信息安全管理办法》等相关法律法规运行，确保其操作符合国家和社会规范。医疗机构需要定期进行合法性审核并借助内外部审计评价，确保持有数据的管理、私有化、数据安全符合相关法规要求。安全审查和合法化管理不仅能提升医疗机构的信息安全水平，还能避免因不合规操作引发的法律纠纷和信誉损失。

结语

随着医疗信息化广泛应用以及技术水平的提升，改善系统架构、加强系统安全防护变得越来越关键。应用新技术与策略将使医疗信息化系统发挥更高的效能、提高处理能力，保障数据信息的安全性和隐私保护。随着医疗技术的发展以及信息数据的增长，医疗信息化系统必须不断进行创新和升级，以应对新的需求以及解决当前存在的各种问题。强化系统安全防护，不仅可以抵御外来攻击、防止内在的风险，还可以提升患者对医院的信心与满意度，从而推动医疗行业取得新的突破与进步。

参考文献

[1]荆芳，葛创杰.水电站监控系统安全防护体系研究[J].水利信息化，2023（6）：75-79.

[2]张宇辰.浅析数据库系统安全架构研究与实践[J].数码设计（上），2022（14）：99-101.

[3]王代军.医疗信息安全体系架构设计研究[J].数字化用户，2021（2）：80-81.

[4]龙智勇，陈姣，阳赣萍，等.医院信息化建设网络安全与防护问题研究[J].医学教育管理，2021，7（6）：675-679.

[5]陈忠，莫然，胡阳.地铁信息系统架构设计及安全方案研究[J].网络安全技术与应用，2023（4）：115-117.