 DOI: https://doi.org/10.12349/iser.v5i10.3485

Research on Hospital Network Architecture Optimization and Security Enhancement Scheme

Jinyuan Zhang

The Second Hospital of Tianjin Medical University, Tianjin, 300000, China

Abstract

With the rapid development of information technology, hospital network system as a key medical information service platform, its security and optimization problems have attracted much attention. Based on the in-depth study of the existing hospital network architecture, this paper puts forward a set of hospital network architecture optimization and security enhancement scheme. The scheme uses advanced firewall technology, VPN technology, powerful intrusion detection and defense system as means to optimize the hospital network architecture to enhance its security. At the same time, this study also improved the data backup and recovery system and strengthened the disaster recovery capability of the network to ensure that the hospital can maintain the stable operation of the network in the face of emergencies in view of the large amount of data and multiple types of data in the hospital network. The research results are helpful to solve the current problems of hospital network security, stability and data protection, and improve the integration level of hospital information technology and medical services.

Keywords

hospital network architecture; firewall technology; disaster recovery capability; network maintenance; data protection

医院网络架构优化与安全性增强方案研究

张津源

天津医科大学第二医院，中国 · 天津 300000

摘　要

随着信息技术的快速发展，医院网络系统作为关键的医疗信息服务平台，其安全性和优化问题备受关注。本研究在深入研究现有医院网络架构的基础上，提出了一套医院网络架构优化与安全性增强方案。该方案以高级防火墙技术、VPN技术、强大的入侵检测及防御系统等为手段，优化医院网络架构，以增强其安全性。同时，本研究还针对医院网络数据量大、数据类型多等特点，完善了数据备份及恢复系统，强化了网络的容灾能力，以确保医院在面对突发事件时，仍能保持网络的稳定运行。研究成果有助于解决当前医院网络安全、稳定性和数据保护等方面的问题，提升医院信息技术与医疗服务的整合水平。

关键词

医院网络架构；防火墙技术；容灾能力；网络维护；数据保护

1 引言

随着社会的不断进步和发展，信息技术的快速扩展正在改变我们生活的各个方面，而医疗行业也不例外。医院这个特殊的组织结构，每天都会产生大量的医疗数据，这些数据不仅有助于医生更好地诊断和治疗疾病，也有助于医院管理人员对医院运行情况进行持续改进。因此，医院网络系统作为存储和传输这些数据的平台，其安全性和稳定性至关重要。然而，随着网络攻击手段的不断升级和变化，医院网络系统也面临着严峻的安全挑战。怎样通过优化网络架构，增强安全性，以及应对大数据等问题，已经成为当前医院网络技术发展的重要课题。本研究基于深入剖析现有医院网络架构和挑战的基础上，提出了一套医院网络架构优化与安全性增强的方案，旨在解决医院网络系统在面临信息技术发展和网络攻击挑战时，如何保持稳定运行，能及时进行排查和修复，从而确保医疗服务的高效运行，并向读者展示如何通过优化网络架构和增强网络安全性，以进一步提高医院信息技术的整合水平，从而促进医疗服务质量的提升。

【作者简介】张津源（1990–），男，回族，中国天津人，本科，助理工程师，从事网络工程研究。

2 当前医院网络架构的挑战与分析

2.1 网络架构面临的安全威胁

医院网络架构面临众多安全威胁，直接影响了医疗服务的稳定性和数据保护的可靠性 [1]。恶意软件和病毒攻击是最为常见的安全威胁，它们可以通过电子邮件、下载文件等途径入侵医院网络，进而导致系统瘫痪、数据泄露。另一个

主要威胁是社会工程学攻击，黑客通过假冒合法人员或者利用社交媒体信息，骗取医院员工的敏感信息，从而获取网络系统的访问权限。分布式拒绝服务（DDoS）攻击也在不断增加，这类攻击通过从多个源向医院网络发送大量请求，导致网络瘫痪，严重影响医疗服务的正常运行。

网络内部威胁同样不容忽视。内部人员因操作失误或故意窃取数据，造成数据泄露甚至系统毁损。许多医院在网络架构设计时，缺乏充分的安全考虑，设备的默认密码未改、系统更新不及时等问题，使得网络漏洞频发。近年来，移动设备及物联网设备在医院中的应用日益广泛，这些设备的安全性普遍较低，一旦被黑客利用，将进一步扩大医院网络的攻击面 [2]。网络协议的安全漏洞如传输层安全协议（TLS）和互联网协议（IP）层的潜在缺陷，也为网络攻击提供了途径。医院网络必须时刻面临外部和内部的多重安全威胁，迫切需要优化网络架构和提升安全防护能力。

2.2 数据管理的复杂性及其风险

医院网络系统处理大量的患者信息、医疗记录和管理数据，面临数据管理的复杂性和风险。医疗数据不仅包括结构化数据如电子病历，也涵盖非结构化数据如影像数据和诊断记录。不同数据类型的多样性增加了数据管理的难度，也对存储、传输和处理提出了高要求。患者隐私和数据保密是医疗机构必须关注的核心问题，但由于数据量大且复杂，数据泄露和未经授权访问的风险显著增加。

大规模的数据管理带来不少技术难题，包括数据的完整性、可用性和一致性保证。在分布式网络架构下，数据传输过程容易受到攻击，导致数据丢失或篡改。数据的冗余备份系统也必须具备足够的灵活性和可靠性，以应对数据恢复的需求。由于涉及多部门协作和跨平台应用，数据共享和实时访问均需要良好的授权管理，任何管理不善都可能制造安全漏洞。医院网络架构中数据管理的复杂性和多样性直接影响网络的安全性和整体服务质量。

2.3 医院网络现有防护措施的不足

医院网络现有防护措施普遍存在一些不足之处。传统的防火墙技术往往只在网络边界实施，对内部网络交通的监控和防护能力较弱，难以应对复杂的内外部威胁。多数医院网络缺乏全面部署的入侵检测系统，导致在面对高级持续性威胁时难以做到及时发现和应对。医院网络数据备份机制不够完善，一旦发生突发事件，数据恢复的速度和完整性得不到保证，进而影响到医疗服务的连续性。由于医疗环境的特殊性和数据敏感性，现有网络防护措施在响应速度和精度上仍然有待提高。

3 医院网络架构优化方案设计

3.1 应用高级防火墙技术的策略

在医院网络架构优化过程中，应用高级防火墙技术的策略是提高医疗信息系统安全性的关键环节。高级防火墙技术能够提供更加精细的访问控制和深度数据包检测，防止恶意攻击和数据泄露 [3]。具体策略包括以下几个方面：

部署基于状态检测的防火墙，通过对网络流量的状态进行实时跟踪和分析，确保仅合法的连接能够通过防火墙。该技术能够识别和阻断非正常流量，从而有效地防范如 DoS 攻击等恶意行为。

应用具有应用层网关功能的下一代防火墙（NGFW），对网络流量进行深度包检测（DPI）。这使得防火墙不仅能够检测到传输层上的威胁，还能够识别和控制应用层上的恶意活动，增强防火墙对复杂攻击的防护能力。

为了进一步提升网络安全性，建议启用基于黑白名单的访问控制策略。通过建立和维护详细的黑白名单，防止外部恶意 IP 地址访问医院网络，确保内部网络的安全访问。这种策略可以灵活适应医院网络的动态变化，提供持续的保护 [4]。

防火墙策略应与医院的安全信息及事件管理系统（SIEM）集成，实时监测和分析安全事件，确保防火墙策略的有效性和及时性。通过这种集成，可以迅速检测和响应潜在的网络威胁，进一步增强网络防护能力。

高级防火墙技术的策略包括状态检测、下一代防火墙、黑白名单访问控制及与 SIEM 系统的集成。这些策略共同作用，有效提升了医院网络的安全性和稳定性 [5]。

3.2 VPN 技术在医院网络架构中的集成与应用

虚拟专用网络（VPN）技术在医院网络优化中发挥关键作用，其主要功能在于通过加密隧道保护数据传输，从而提升网络安全性。在医院网络架构中，VPN 技术可用于连接不同医院分支机构，实现信息共享和远程医疗服务。医院人员在外部访问内部网络时，VPN 可以提供安全的访问途径，确保敏感数据不被窃取或篡改。

实施 VPN 技术时，应选择高强度加密算法，如 AES-256，以确保数据传输的安全性。需配置多因素身份验证（MFA）来加强用户认证，降低未经授权访问的风险。网络管理员需要对 VPN 连接进行实时监控，及时发现异常流量和潜在威胁。

为了最大化 VPN 的效益，医院应定期进行安全评估和漏洞扫描，确保 VPN 设置符合最新安全标准。培训医院工作人员正确使用 VPN，是保障网络安全的重要环节。通过优化 VPN 技术的应用，医院网络在数据传输的安全性和管理便捷性方面将得到显著提升。

3.3 入侵检测及防御系统的实施细节

实施入侵检测及防御系统（IDPS）是提升医院网络安全性的关键步骤。IDPS 应集成基于签名和行为的检测技术，以便全面监控网络流量及系统活动。实时告警和自动化响应功能需确保在网络遭受攻击时迅速采取行动，阻止威胁扩散。系统应定期更新威胁数据库，并进行安全策略调整。IDPS 需与防火墙、VPN 等安全措施紧密联动，构建多层次的协同防御体系，提高整体网络防护能力。

4 网络安全能力的增强与网络维护

4.1 数据备份及恢复系统的完善

医院网络中数据备份及恢复系统的完善至关重要。高效的数据备份策略包括完整备份和增量备份相结合，以减轻系统负担并确保数据的完整性。应用异地备份技术，将重要数据存储在地理位置不同的服务器上，防止因单点故障导致的数据丢失问题。进一步优化数据备份系统时应引入智能化备份管理平台，实现自动化和可视化的备份流程监控，确保备份任务的高效执行。

为了保障数据恢复的及时性，制定详细的数据恢复计划至关重要。应对各种可能的突发事件进行风险评估和恢复演练，保持恢复方案的实用性和可靠性。冷备份和热备份相结合，使系统在数据恢复时既能确保数据的完整性，又能保障业务的连续性。通过部署高可用性的存储系统，减少数据恢复所需的时间，提高医院网络应对突发事件时的反应速度。

在整个数据备份及恢复系统的管理中，还需加强对备份数据的安全保护，应用加密技术防止备份数据在存储和传输过程中的泄漏。对备份数据的访问权限进行严格控制，避免因人为操作导致的数据泄漏和破坏。通过建立健全的数据存取审计机制，确保整个备份及恢复过程的安全可控。这样不仅提高了医院网络系统的安全性和可靠性，也为医院提供稳定的运营环境奠定了基础。

4.2 医院网络容灾能力的强化方案

医院网络的容灾能力尤为重要，以应对可能的突发事件，保障医疗服务的连续性。为此，医院网络可采用多层次的容灾设计方案。启用多地点的数据备份机制，可以定期将重要数据复制到异地服务器，确保在发生灾难时能迅速进行数据恢复。实施双活数据中心技术，通过在不同地理位置设置两个实时同步的数据中心，在任一数据中心出现故障时，另一个数据中心能够无缝接管业务，从而减少业务中断的风险。可以引入数据冗余与镜像机制，使关键数据在本地和云端存储，增强数据的可靠性和可恢复性。网络基础设施方面，可通过冗余线路设计和智能路由技术，确保网络故障时流量自动切换到备用线路，维持网络的畅通无阻。应制定详细的容灾演练计划，定期进行模拟演练，以验证和优化容灾方案的有效性，确保所有系统和人员在紧急情况下能够迅速响应和恢复。通过以上多层次的容灾能力建设，能够显著提升医院网络的稳定性和抵御突发事件的能力。

4.3 网络维护及应急响应策略

网络维护与应急响应策略在提升医院网络安全性和稳定性方面具有关键作用。定期检查和更新网络硬件与软件，确保其处于最佳运行状态，是有效维护网络的基础。制定系统化的巡检计划，及时发现并修复潜在漏洞，以预防网络攻击；针对突发网络故障，建立健全的应急响应机制，确保在出现问题时能够迅速定位并解决。配备专业的网络管理团队，提供 24 小时监控与技术支持，保障网络的持续稳定运行。开展定期的网络安全培训，增强员工的安全意识和操作技能，有效减少人为因素对网络安全的威胁。

5 结语

这个研究提出了一个改善医院网络的方案，可以让网络更安全，更稳定。研究者用新的技术，包括高级防火墙、VPN 技术和强大的保护系统，提升了网络的安全。他们还因为医院网络需要处理大量的数据，因此也改进了数据备份和恢复系统，让网络在遇到突发情况时还能正常运行。研究者还提出了维护网络的方案，帮助医院解决网络问题，保证医疗服务的顺利进行。这个方案虽然有着先见之明，但面对新的网络威胁，可能还需要更深入地研究。在未来，研究者希望能进一步改进这个方案，提高网络的安全和稳定，为医疗服务提供更好的支持。这个研究对解决医院网络问题，提高医院信息技术和医疗服务的整合能力是有帮助的。

参考文献

[1] 冯雁辉,陆华英,蒋彭.基于Netfilter架构的网络防火墙设计与实现[J].电子技术与软件工程,2022(14):31-34.

[2] 徐皓,李超凡,张梦娜,等.医院网络架构仿真研究[J].医学信息学杂志,2021,42(1):64-67.

[3] 虞宏达.对医院网络基础架构的维护研究[J].计算机产品与流通,2020(5):115-117.

[4] 龚雨雄.网络信息安全与防火墙技术研究[J].电子测试,2021,32(16):127-128.

[5] 史亚香.防火墙技术在医院网络中的应用[J].健康之友,2021(16):296-298.