第 8 卷◆第 1 期◆版本 1.0◆2026 年
文章类型：论文丨刊号（ISSN）：2705-1102(P) / 2705-1110(O)

智慧诊疗导航眼镜中的隐私计算与数据安全治理框架研究

韦朝楷　谢雨鑫　刘烊　李梅　陆紫光*
广西职业师范学院
DOI:10.32629/bmtr.v8i1.18558

[摘　要] 增强现实(AR)、人工智能(AI)与物联网(IoT)技术的深度融合,推动智慧诊疗导航眼镜成为医疗领域的重要智能穿戴设备。该设备能够实现术中实时导航、患者信息叠加及远程协同操作,显著提高诊疗精准度与效率,契合以患者为中心的整合医疗服务趋势。然而,设备持续采集并处理患者生理数据、医学影像及实时视频流等高敏感信息,面临严峻的隐私泄露与数据安全威胁。此类风险与5G+智慧医疗急救平台中暴露的“数据安全”与“责任归属”问题高度一致,凸显智能医疗设备共有的治理短板。传统安全机制难以在“端—边—云”协同架构中平衡数据可用性、隐私保护与实时性需求。为此,本文提出一种融合区块链与隐私计算的数据安全治理框架,在保障数据隐私的前提下支持诊疗业务连续高效运行,并从技术、管理、伦理与标准多维度提出实施路径,为可信、合规、实用的智慧医疗系统构建提供理论支撑与实践参考。
[关键词] 智慧诊疗导航眼镜；隐私计算；数据安全治理；联邦学习
中图分类号：R197.7　文献标识码：A

Research on Privacy Computing and Data Security Governance Framework in Smart Diagnostic Navigation Glasses

Chaokai Wei　Yuxin Xie　Yang Liu　Mei Li　Ziguang Lu*
Guangxi Vocational Normal University

[Abstract] The deep integration of augmented reality (AR), artificial intelligence (AI), and the Internet of Things (IoT) technologies has propelled smart diagnostic and navigation glasses into a crucial wearable device in the medical field. These devices enable real-time intraoperative navigation, patient information overlay, and remote collaborative operations, significantly enhancing diagnostic accuracy and efficiency while aligning with the trend of patient-centered integrated medical services. However, as the devices continuously collect and process highly sensitive information such as physiological data, medical imaging, and real-time video streams, they face severe risks of privacy breaches and data security threats. These risks closely mirror the "data security" and "responsibility attribution" issues exposed in 5G+ smart medical emergency platforms, highlighting common governance shortcomings in intelligent medical devices. Traditional security mechanisms struggle to balance data availability, privacy protection, and real-time requirements within the "device-edge-cloud" collaborative architecture. To address this, this paper proposes a data security governance framework integrating blockchain and privacy computing, which supports continuous and efficient diagnostic operations while safeguarding data privacy. Additionally, it outlines implementation pathways from technical, managerial, ethical, and standardization dimensions, providing theoretical support and practical reference for building trustworthy, compliant, and practical smart healthcare systems.
[Key words] Smart Diagnostics Navigation Glasses; Privacy-Preserving Computing; Data Security Governance; Federated Learning

引言

党的二十大报告明确提出推进健康中国建设,将人民健康置于优先发展的战略地位。数字技术与医疗健康的深度融合成为提升诊疗质量与服务可及性的关键路径。智慧诊疗导航眼镜作为增强现实技术在医疗场景中的典型应用,能够将医学影像、手术路径等虚拟信息实时叠加至医师真实视野,实现“所见即所

得”的精准导航与决策支持,代表了智慧医疗的前沿发展方向。据《2024年中国智慧医疗发展报告》预测,至2025年,我国智能医疗硬件市场规模将突破千亿元,辅助诊疗类可穿戴设备年复合增长率尤为显著。在这一背景下,医疗设备的智能化与网络化对技术档案管理提出更高要求,智慧运营一体化理念成为保障设备全生命周期可靠运行的重要基础[1]。然而,技术发展伴随风险。智慧诊疗导航眼镜在运行过程中持续生成并处理包括患者生命体征、术野视频、三维器官模型、电子病历等在内的多模态敏感数据。一旦发生泄露、篡改或滥用,不仅侵犯患者隐私,还可能引发医疗事故与法律争议。类似风险在浙江省5G+智慧医疗急救平台中同样存在,表现为黑客攻击、内部泄露与责任认定模糊等问题,反映出智慧医疗系统面临的共性安全挑战。现有医疗信息系统安全标准与通用数据保护条例难以覆盖此类新型设备在移动、动态环境中对实时性、轻量化与强隐私保护的需求。

当前,区块链与隐私计算的融合被视为实现医疗数据安全共享的有效路径,其通过分层协同与智能合约实现“数据不出域”的受控流通,为智慧诊疗导航眼镜的数据治理提供了技术借鉴。然而,现有研究多将隐私计算视为独立工具,缺乏在具体业务场景与“端—边—云”架构下的系统性整合。本文旨在弥补该研究空白,构建一个融合隐私计算与数据治理理念的层次化框架,系统应对数据在全生命周期中所面临的安全与隐私挑战,为相关设备研发、部署与监管提供完整解决方案。

1 数据特性与安全风险分析

智慧诊疗导航眼镜通过将虚拟诊断信息与真实术野实时融合,为医生提供精准的术中导航。这一过程的实现依赖于对多源数据流的高效处理,使其数据生态呈现出区别于传统医疗信息系统的复杂特性,并由此衍生出独特的安全挑战[2]。

1.1数据核心特征分析

智慧诊疗导航眼镜处理的数据具有四个显著特征。首先是多模态与高敏感性。设备同步处理术野视频流、三维重建器官模型、实时生命体征波形及历史电子健康记录等多类数据,均属最高级别的个人敏感信息。这类数据的泄露不仅侵犯患者隐私,更可能引发医疗欺诈等严重后果。其次是极致的实时性要求。手术导航需要虚拟标记与医生操作保持毫秒级同步,任何由安全机制引入的延迟都可能影响手术精度,甚至危及患者安全。这对安全技术的性能提出了极高要求。此外,系统采用端-边-云协同架构以平衡计算负载。数据在终端、边缘节点与云平台间动态调度,虽然优化了系统性能,但也显著扩大了攻击面,使数据在多个实体间面临潜在威胁。最后,系统具有强上下文感知能力。数据处理策略需根据手术阶段、医生操作意图等动态调整,这就要求安全机制必须具备相应的情境感知能力,实现保护强度与诊疗效率的自适应平衡。

1.2全生命周期安全风险

基于上述特性,安全风险贯穿于数据的全生命周期。在采集阶段,终端设备面临恶意软件窃取传感器控制权的风险,设备丢失也可能导致本地存储的原始数据直接泄露。传输过程中,数据在终端、边缘与云端间的无线传输易遭受窃听、中间人攻击等威胁,在远程协作场景下风险尤为突出。计算与存储环节的风险最为集中[3]。边缘节点与云端平台一旦遭受网络攻击,可能导致批量数据泄露。内部人员的越权访问与数据滥用同样构成重大威胁,而静态数据加密不足则进一步加剧了这一风险。共享与销毁阶段的风险主要体现在治理层面。与第三方数据共享时,粗放的权限控制可能导致数据超范围使用；数据到期后若未彻底销毁,残留信息可能被恢复利用。综上所述,传统以边界防护和静态加密为核心的安全方案,难以应对智慧诊疗导航眼镜动态、强实时的应用场景。构建深度融合业务、兼顾安全与效率的系统性治理框架,已成为该技术落地应用的关键前提。

2 隐私计算与安全治理的核心挑战

在智慧诊疗导航眼镜中构建有效的隐私保护与数据安全体系,面临着一系列复杂且相互关联的挑战。这些挑战根植于技术瓶颈、法律合规、临床实践与系统集成的多重维度,共同构成了该技术规模化应用前必须克服的核心困境。深入剖析这些困境,是设计具有可行性治理框架的逻辑前提。

2.1技术性能与业务实时性的根本矛盾

首要的挑战来自于隐私增强技术本身固有的性能开销与医疗业务对极致实时性要求之间的尖锐矛盾。智慧诊疗导航眼镜在术中辅助场景下,要求系统响应延迟严格控制在毫秒级别,以确保虚拟信息与真实术野的精准同步[4]。然而,旨在实现“数据可用不可见”的先进隐私计算技术,如安全多方计算(MPC)和全同态加密(FHE),通常伴随着巨大的计算复杂度和频繁的通信交互。

2.2多主体架构下的权责界定与合规困境

智慧诊疗导航眼镜依托的“端-边-云”协同架构,引入了多元化的参与主体,包括设备制造商、应用软件开发方、医疗机构(数据控制者)、云服务/边缘节点提供商(数据处理者)以及临床操作人员。这种复杂的多主体生态使得数据在全生命周期中的权责边界变得异常模糊。

2.3临床工作流中安全与效率的平衡难题

医疗实践,尤其是急诊和手术,具有高压力、高时效性的特点。任何安全措施如若显著干扰既定的临床工作流程,都将在实践中遭遇强烈的抵触,从而难以落地。传统的安全手段,如频繁的强身份认证(例如,每次访问患者数据都需进行多因素验证)、冗长的访问审批流程,在争分夺秒的抢救场景下显得格格不入。

2.4资源受限环境下的技术适配性与内生脆弱性

作为一款可穿戴设备,智慧诊疗导航眼镜在计算能力、电池续航、散热和物理尺寸方面存在严格的限制。这决定了其无法直接部署为服务器环境设计的高复杂度加密算法或安全协议。尽管轻量级密码学和硬件安全模块(如TEE,可信执行环境)被视作可行的解决方案,但它们各自引入了新的脆弱性。

3 隐私计算与数据安全治理框架构建

面对智慧诊疗导航眼镜在数据安全与隐私保护方面面临的多重挑战,亟需构建一个系统化、多层次且可落地的治理框架。

该框架不应局限于单一技术方案的堆砌,而应通过技术、管理、运营与标准四个维度的协同作用,形成贯穿数据全生命周期的综合防护体系[5]。基于此,本文提出以下构建路径。

3.1技术层：构建融合隐私计算的纵深防御体系

在技术层面,核心目标是建立一套轻量级、高效率且具有韧性的纵深防御技术体系。首要任务是实施精细化的数据分级分类与加密策略。依据《信息安全技术 个人信息安全规范》及医疗行业标准,对眼镜采集的视频、图像、生理参数等多模态数据,基于其敏感度及业务需求进行分级,并为之匹配差异化的加密算法与保护强度。例如,对实时视频流采用低延迟的轻量级加密,而对存档的电子病历则使用更高强度的国密算法。

3.2管理与合规层：健全权责明晰的制度规范

先进的技术需要健全的管理制度作为支撑,以明确各方权责,确保合规性。首要工作是制定专门面向智慧医疗设备的数据安全管理办法。该办法须清晰界定在“端-边-云”复杂架构中,设备商、软件提供商、医院、云服务商等各方在数据采集、存储、处理、共享等环节的法律角色(控制者、处理者或共同控制者)及相应责任,形成权责对等的契约链条。此外,必须完善数据加密与安全销毁的全流程规程。明确规定数据在传输、存储及缓存状态下所使用的加密算法、密钥长度、密钥生命周期管理策略(如采用密钥管理系统KMS)。同时,制定严谨的数据销毁标准,确保在数据达到保存期限或患者行使删除权后,能够通过多次覆写等物理或逻辑手段实现数据的不可恢复性清除。

3.3运营与伦理层：培育安全文化与伦理共识

治理框架的长期有效运行,依赖于持续性的运营管理和深厚的伦理共识。应开展体系化的全员安全与隐私培训,培训对象不仅涵盖IT技术人员,更应重点包括使用设备的临床医生与护士。培训内容需结合真实医疗场景,提升其数据安全意识与应急操作技能,使之成为安全防线中主动的参与者。建立高效协同的安全事件应急响应机制是运营层的核心。制定详尽的应急预案,明确在发生数据泄露等安全事件时的报告流程、处置步骤、沟通策略及法律责任,并定期组织跨部门的应急演练,确保事发时能快速响应、有效遏制并降低损失。更为根本的是,在产品研发全周期中贯彻“设计即安全”与伦理遵循原则。确保技术方案的设计与应用始终以患者福祉为中心,符合“有益、不伤害、公正、尊重自主”的医学伦理基本原则,在追求技术先进性的同时,警惕和防范技术可能带来的偏见与不公。

4 结论与展望

智慧诊疗导航眼镜作为医疗数字化进程中的颠覆性技术,其健康发展依赖于稳健、高效且可信的数据安全与隐私保护体系。本文所提出的隐私计算与数据安全治理框架,通过技术、管理、伦理与标准的协同作用,系统应对数据在全生命周期中面临的各类安全挑战,致力于在保障隐私的前提下支持诊疗业务的实时性与连续性,实现安全与效能的有效统一。

展望未来,随着隐私计算技术的持续成熟、硬件安全能力的增强,以及医疗AI与AR技术的进一步融合,智慧诊疗导航眼镜的数据治理框架将向更自动化、自适应与无缝化的方向发展。通过构建可信数据环境,该设备有望在提升医疗质量、保障患者安全与隐私权益方面发挥更大作用,成为“健康中国”战略实施中不可或缺的技术支撑。

[项目信息]

本项目由国家级大学生创新创业训练计划项目资助,项目名称：广西职业师范学院2025年大学生创新创业训练计划项目《医路瞳行-基于AI和AR的老年智慧诊疗导航眼镜》,项目级别：国家级,项目类别：一般项目,项目编号：202514684022X。

[参考文献]

[1]任静,Nancy R Reynolds,张婧珺,等.患者导航的概念分析[J].护理学杂志,2023,38(16):82-86.

[2]邱小清.医院室内定位导航系统的应用与实现研究[J].中国新通信,2022,24(10):78-80.

[3]陈勰,钟誉豪,赵灿灿,等.浙江省5G+智慧医疗急救平台应用的伦理风险与治理路径[J].温州医科大学学报,2013.

[4]王钰涵,孙燕杰.区块链隐私计算赋能智慧医疗数据共享[J].中国科技信息,2025,(21):131-134.

[5]薛阳.基于智慧运营一体化的医疗设备技术档案管理:优化流程、提升效率与保障安全[J].办公室业务,2025,(20):190-192.

作者简介：

韦朝楷(2002--),男,汉族,广西灵山人,本科,广西职业师范学院,研究方向：物联网工程。

谢雨鑫(2002--),女,汉族,广西博白人,本科,广西职业师范学院,研究方向：物联网工程。

刘烊(2002--),女,汉族,广西河池人,本科,广西职业师范学院,研究方向：物联网工程。

李梅(2003--),女,汉族,广西玉林人,本科,广西职业师范学院,研究方向：物联网工程。

*通讯作者：

陆紫光(1992--),男,壮族,广西桂林人,研究生,广西职业师范学院,研究方向：人工智能。