基于区块链技术的医院计算机通信网络安全防护体系构建

王欢　刘晓冬*
河北医科大学第二医院
DOI:10.12238/acair.v3i3.15547

[摘　要] 医疗信息技术持续迭代,医院计算机通信系统逐渐成为现代医疗体系的核心架构,承担着患者诊疗信息、电子病历、临床决策方案等敏感数据的存储与传输。网络环境的复杂特性与黑客攻击手段持续升级,导致医疗通信网络安全风险日益凸显,数据泄露或篡改直接威胁患者隐私安全,诊疗信息异常可能破坏医疗服务连续性,极端情况下将引发生命安全风险。区块链技术具备去中心化与不可篡改特性,其分布式账本结构实现全程可追溯,这种技术架构为解决医疗通信网络安全缺陷开辟了创新路径。基于此,本文对区块链技术支撑下的医院计算机通信网络安全防护体系构建做出研究,以供参考。
[关键词] 区块链技术；医院计算机通信网络；安全防护体系
中图分类号：G633.67　文献标识码：A

Construction of hospital computer communication network security protection system based on blockchain technology

Huan Wang　Xiaodong Liu*
The Second Hospital of Hebei Medical University

[Abstract] With the continuous iteration of medical information technology, hospital computer communication system has gradually become the core architecture of modern medical system, which is responsible for the storage and transmission of sensitive data such as patient diagnosis and treatment information, electronic medical records, and clinical decision plans. The complex characteristics of the network environment and the continuous upgrading of hacker attack methods have led to increasingly prominent medical communication network security risks. Data leakage or tampering directly threatens the privacy and security of patients. Abnormal diagnosis and treatment information may damage the continuity of medical services, and in extreme cases will lead to life safety risks. Blockchain technology has the characteristics of decentralization and immutable, and its distributed ledger structure can be traced throughout the process, which opens up an innovative path for solving the security defects of medical communication networks. Based on this, this paper studies the construction of hospital computer communication network security protection system supported by blockchain technology for reference.
[Key words] Blockchain technology; Hospital computer communication network; Safety protection system

引言

数字化医疗领域,医院计算机通信网络安全防护成为关键议题。网络攻击事件层出不穷——数据泄露与勒索软件侵袭持续威胁医疗机构运营秩序,患者隐私信息面临严重风险。区块链技术依托去中心化架构与加密机制,开辟数据安全新路径,该技术确保数据不可篡改——实现透明追溯,有效防范外部攻击与内部恶意操作。建立区块链技术的医院通信网络安全体系,对医疗数据保全具有核心价值,这种防护架构既推动医疗信息共享应用,又能优化服务质量,为诊疗效率提升创建良好基础。

1 区块链技术介绍

区块链技术最初作为比特币底层架构获得认知,其本质是去中心化分布式账本系统。数据存储机制突破传统模式,信息并非集中于独立服务器,网络节点共同承担存储职能。每个节点维护完整账本副本,数据变更需多数节点共识验证,信息不可篡改特性得以实现。区块链系统运用密码学手段处理交易信息,数据机密性获得保障。每笔交易附带时间戳标识,时序排列形成链式结构,完整溯源体系由此建立。技术特征赋予区块链多维应用潜力,涵盖数据防护、身份核验、智能协议执行等场景。医疗领域信息安全防护迎来革新方案,区块链技术支撑诊疗数据全生命周期管理——安全存储、高效传输、合规处理均获技术保障。

2 基于区块链技术的医院计算机通信网络安全防护体系构建价值

2.1确保医疗数据的完整性

医疗数据完整性与可靠性构成医疗服务体系的根基，传统中心化存储模式存在安全隐患，黑客攻击、人为篡改、设备故障可能引发数据损毁或遗失；区块链技术凭借分布式存储架构与链式加密机制，构筑起防篡改屏障——医疗信息真实性得以维护，数据全周期可追溯特征得以保留。这种技术特性重塑临床诊疗路径：医生诊疗决策依赖更精确的病史资料，科研机构获取更完整的病案样本，患者隐私权利得到更严密的数字防护。涉医法律争议场景中，基于区块链的诊疗轨迹形成铁证，司法判定过程获得可信数字凭证。医疗信息连续性直接影响诊疗质量层级，跨机构转诊场景下，区块链医疗档案消除信息孤岛效应；接诊医师能即时调阅患者过敏史、影像资料、用药记录等核心数据，制定个性化治疗方案的时间成本大幅降低。分布式账本技术正在重构医疗协作网络：不同医院检验报告互认效率提升，远程会诊数据同步延迟缩短，区域医疗资源利用效率呈现指数级增长——这标志着从数据确权到价值流转的医疗信息化新生态。

2.2保护患者隐私，促进数据安全

医疗隐私构成医疗服务领域的关键议题，在电子化存储与传输患者信息的过程中，隐私泄露风险显著上升——区块链技术凭借加密机制与数据分布式存储特性，为解决这一问题开辟新路径。医疗数据经加密后存储于区块链网络，仅持有对应私钥的用户可解密访问内容；即便传输链路遭非法截取，攻击者亦无法破译敏感信息。传统中心化存储模式下，单一服务器被攻破即导致全局数据泄露；区块链采用分布式节点架构，数据集中化风险得以降低。医疗信息分散存储于不同节点，局部节点受攻击不会危及整体网络安全；这种架构同时提升数据可用性与抗攻击能力，隐私保护体系获得多维度支撑。

2.3抵御网络攻击恶意行为

网络攻击可能导致数据泄露或篡改，甚至会影响医疗设备的正常运行，严重还会危及患者的生命安全。区块链技术的去中心化架构和共识机制，为抵御网络攻击提供了有效手段，这是因为在区块链网络中，任何数据的添加或修改都需要经过网络中多数节点的共识，这种机制使得攻击者难以通过控制单个节点或少数节点来篡改数据或发动攻击，即使攻击者成功入侵了部分节点，也无法改变整个网络的数据状态。区块链技术还可以结合智能合约等机制，实现对网络行为的自动监控和管理，其实智能合约是一种自动执行的合约条款，当满足特定条件时，合约将自动执行相应的操作。在医院计算机通信网络中，可利用智能合约来监控网络流量、检测异常行为，并及时采取措施阻止攻击行为的发生，这种自动化的管理方式提高了网络的安全性，降低了人为干预的成本和风险。

2.4促进医疗信息的实时共享

医疗信息的共享与协同是现代医疗体系发展的重要方向，但由于数据安全和隐私保护等问题，医疗信息的共享一直面临着诸多挑战，随着区块链技术的出现，彻底为医疗信息的共享提供了新的可能，在区块链上医疗数据被加密存储，并且只有经过授权的用户才能访问数据，这种机制确保了数据的保密性和安全性，使得医疗机构之间可以更加放心地共享医疗信息。在医疗协作过程中，各参与方能通过区块链网络共享患者的医疗记录、检查结果等信息，这些信息都是经过验证和不可篡改的，这有助于提高医疗协作的效率和准确性，降低因信息不一致或错误而导致的医疗风险。区块链技术还可以结合人工智能等技术，实现医疗信息的智能分析和挖掘，为医疗决策提供更加精准和个性化的支持。

2.5提高医疗设备的安全可信度

医疗设备是医院计算机通信网络中的重要组成部分，其安全性和可信度直接关系到患者的生命安全和医疗服务的正常运行，传统的医疗设备管理方式往往存在诸多安全隐患，如设备身份伪造、数据篡改等。区块链技术的去中心化和不可篡改特性为医疗设备的安全管理提供了新的解决思路，比如通过将医疗设备的身份信息、运行数据等存储在区块链上，可实现设备的身份认证和数据溯源，当医疗设备接入医院计算机通信网络时，系统通过区块链验证设备的身份和数据的真实性，防止设备身份伪造和数据篡改等安全隐患。区块链的透明公开特性也使得设备的运行状态和维护记录更加可追溯和可控，提高医疗设备的可信度。

3 基于区块链技术的医院计算机通信网络安全防护体系构建对策

3.1加强基于区块链的医疗设备安全管理

区块链医疗设备安全管理体系强化方案聚焦安全性能与信任机制优化，覆盖设备身份认证、数据溯源验证、远程监控维护三大核心环节。借助区块链技术为每台医疗设备分配唯一地址及数字身份证书，确保设备身份真实可靠；运行数据与维护记录完整存储于区块链，建立可追溯验证的数据链条，便于后续故障诊断与维护支持。搭建区块链医疗设备管理平台实时监控运行状态与维护情况，设备故障或安全隐患触发即时响应机制，平台自动推送预警信息至运维终端——这种分布式监管模式打破传统中心化系统响应延迟的局限。实施该综合方案，医疗设备安全性实现系统性提高，故障率与安全隐患风险同步下降，运维人员可通过链上证书核验模块快速比对设备授权信息，数据追踪功能则完整记录设备全生命周期中的参数波动曲线、固件更新日志等关键信息。

3.2设计去中心化的网络架构，增强系统抗攻击性

医院为了构建基于区块链技术的医院计算机通信网络安全防护体系，首先需要设计一种去中心化的网络架构，这种架构将摒弃传统的中心化服务器模式，而是将数据和服务分散到网络中的多个节点上，每个节点都承担着数据存储、处理和传输的功能，共同维护整个网络的安全和运行。这种去中心化的设计使得网络不再依赖于单一的服务器或数据中心，即使部分节点受到攻击或发生故障，也不会影响整个网络的正常运行，在去中心化

网络架构的基础上,还可引入区块链的共识机制来进一步增强系统的抗攻击性,共识机制是区块链网络中的核心机制之一,它确保了网络中所有节点对数据状态的一致性认知,当有新数据需要添加到区块链上时,网络中的节点会通过共识算法来验证数据的合法性和正确性,只有经过多数节点验证通过的数据才能被添加到区块链上,从而确保了数据的不可篡改性和可靠性。这种机制使得攻击者难以通过控制少数节点来篡改数据或发动攻击,有效提高了网络的安全性。

3.3利用加密技术保障数据传输存储的安全性

医院应该保证医疗机构的通讯系统的安全性,其实密码学是一项非常有意义的工作,在传送的时候,可使用对称和不对称的方法来实现对资料的加密,这样就会保证在传送的时候,不被人截取或者篡改。利用同一密钥加密与加密,加密速度快,效率高；而不对称密码体制采用一对公开密钥和私有密钥分别实现加、解密,因而更加安全。就资料储存而言,区块链的本质是加密储存,在区块链中,每一块都含有前面一块的散列值和自己的事务等相关的信息,而且经过了加密。这样的方法保证信息的隐私性和完整性,并且在未经授权的情况下,不容易被黑客破解或者修改,也会与存取控制等相关技术相配合,对资料的存取进行更严格的限制,保证资料只能由合法的使用者存取与利用。

3.4建立智能合约机制,实现自动化安全管理

智能合约是区块链技术中的另一个重要概念,它是一种自动执行的合约条款,当满足特定条件时,合约将自动执行相应的操作。在此基础上,医院提出了一种基于智能合同的医疗信息系统的设计方案,并对其进行了详细的分析。比如,我们可以在智能合同中设置一定的约束条款或者政策,使其在特定的情况下,能在特定的情况下采取相应的防范和预警行动。在此基础上,医院还提出了一种基于智能合同的新型医疗设备系统,一方面对用户进行在线监测与报警,从而能及时地检测和应对可能存在的安全隐患,而且该系统还能自动完成访问控制、数据备份等相关的安全管理工作,减少了人工介入的代价与风险,由于其透明、可追溯的特性,使得该系统的运行更加公平、更加可追溯。

3.5强化身份认证,确保用户权限的合理性

在医疗设备的通讯系统中,用户的身份验证与权限管理是一个非常关键的问题,在此基础上,医院提出一种基于增强的身份鉴别机制,以保证使用者的授权合理,它包含了多因子认证,生物识别等多种方法,保证了互联网上仅允许合法的使用者能够访问并利用互联网上的资源。在存取控制中,医院使用RBAC(Role-basedAccessControl)或ABAC(Property-basedAccessControl)等模式对使用者的授权进行管理。RBAC模式对用户进行了功能分区,并对其进行了授权;ABAC模式通过对不同类型的使用者(职位、部门等)进行动态决策。该模式能够根据医院的具体需要进行动态的设置与调节,保证了使用者使用权限的合理性与正确性。

3.6推动基于区块链的医疗数据共享操作

医院需制定出一套统一的数据标准以及接口规范,以此来确保不同医疗机构之间的数据能够顺畅地进行互操作,采纳如HL7等国际公认的医疗数据标准,这样的做法能够有效保障医疗数据的可交换性和可读性,为数据的跨机构流通打下坚实基础。医院也要充分利用区块链技术的特性,来实现数据在共享过程中的隐私保护,比如采用零知识证明等先进技术,既能确保数据的加密传输,又能满足共享验证的需求,从而全方位保障数据在共享过程中的安全性,消除数据泄露的风险。医院必须明确规定,只有经过授权的医疗人员才能访问这些共享的医疗数据,为了后续审计和追踪的需要,每次数据访问的日志信息都应被详细记录下来,这样一来既能有效防止数据被非法访问,又能为数据的安全使用提供有力保障。

4 结束语

总体而言,区块链技术伴随比特币问世引发广泛关注,其核心架构为去中心化分布式账本,依托密码学原理实现数据防篡改与可追溯特性。医院计算机通信网络安全领域,区块链技术借助特有属性——为数据隐私防护、网络攻击抵御等复杂问题开辟解决路径。本研究聚焦区块链技术赋能的医院通信网络安全架构设计,引入区块链技术打造安全可靠防护机制,维护医疗数据完整性,守护患者隐私安全。数字医疗环境中的分布式存储机制与智能合约技术形成互补,区块链结构有效阻隔非法数据篡改行为,以及建立全流程追溯能力,这些技术特征构成医疗信息安全防护的底层逻辑。

[参考文献]

[1]胡栋鹏,汤紫雄,曾坚毅.基于区块链技术的光通信网络数据加密方法设计[J].激光杂志,2023,44(10):128-132.

[2]王彦华,赵延磊,王顺晔,等.基于区块链技术的光通信系统安全风险评价研究[J].激光杂志,2022,43(10):197-201.

[3]朱宝亮.医院计算机网络的层次化设计方案[J].信息与电脑(理论版),2021,33(23):225-227.

[4]袁红团.通信技术与计算机技术融合发展——评《安全通论:刷新网络空间安全观》[J].科技管理研究,2021,41(20):I0012.

[5]赵欣.医院网络安全管理与态势感知平台的建设[J].网络安全技术与应用,2025,(03):124-126.

作者简介：

王欢(1988--),男,汉族,黑龙江绥化人,本科,工程师,从事信息、大数据、远程医疗、互联网诊疗和人工智能相关工作。

*通讯作者：

刘晓冬(1988--),男,汉族,河北石家庄人,硕士,工程师,从事数据中心工作。