doi: 10.7690/bgzdh.2024.09.007

基于区块链的医疗数据共享系统

温　煜，潘昌森，陈绍勇，梁　斐
（梅州市人民医院数据中心，广东 梅州 514000）

摘要：为实现医疗数据的安全存储、管理和访问控制，提出一种基于区块链、物联网、云存储和代理重加密算法的医疗数据共享系统。对系统进行结构设计，分为系统管理层、数据收集层、区块链网络层、云服务层、应用程序层；分析系统的工作过程，包括系统初始化、数据采集与上传、数据查询与共享；对所提基于区块链的医疗数据共享系统进行仿真与测试。仿真结果表明，该方案为智能医疗系统数据安全管理及可靠运行提供了一定借鉴。

关键词：医院信息系统；数据共享；区块链；云存储
中图分类号：TP393　　**文献标志码：**A

Medical Data Sharing System Based on Blockchain

Wen Yu, Pan Changsen, Chen Shaoyong, Liang fei
(*Data Center*, *Meizhou People's Hospital*, *Meizhou* 514000, *China*)

Abstract: In order to realize the secure storage, management and access control of medical data, this paper proposes a medical data sharing system based on blockchain, Internet of Things, cloud storage and proxy re-encryption algorithm. The system is divided into system management layer, data collection layer, block chain network layer, cloud service layer and application layer. The working process of the system is analyzed, including system initialization, data collection and upload, data query and sharing. The proposed medical data sharing system based on block chain is simulated and tested. The simulation results show that the scheme provides a reference for data security management and reliable operation of intelligent medical system.

Keywords: hospital information system; data sharing; block chain; cloud storage

0　引言

医院信息系统[1](hospital information system，HIS)是现代医院的基础设施，在患者管理、诊断和治疗决策等诸多方面发挥着至关重要的作用。同时，结合网络、大数据、物联网、通信[2-3]等技术，HIS以现代化、科学化、规范化的手段管理医院，可以有效提高医院的工作效率和医疗质量。

患者的医疗数据包含了患者的历史生理信息，如电子医疗记录(electronic medical records，EMR)、个人健康记录(personal health records，SHR)、电子健康记录(electronic health records，EHR)等数据。这些数据对患者的疾病诊断和治疗以及日常保健具有重要的参考价值。文献[4]对大数据概念进行解释，并对健康医疗大数据应用现状及改进策略探析。文献[5]探讨了医疗机构数据共享关键问题研究与数据治理对策。传统的医疗数据存储与管理存在以下问题：1) 系统安全问题和医疗数据共享困难。传统方法将医疗数据存储在私有或云服务器中，系统面临恶意攻击、数据泄漏和篡改的风险。2) 传统系统通常在医院独立运行，难以满足患者共享医疗数据的基本需求。

为此，大量学者将区块链引入医院信息共享系统，区块链的不变性、分散性和匿名性确保了医疗数据的安全存储。文献[6]使用改进的声誉机制保证在数据共享中筛选数据源的效率，并利用区块链和联邦学习技术，提高共享效率和实现隐私保护。文献[7]提出一种属性基可搜索加密方案。目前，大部分方案中提出的系统仅使用区块链进行安全的医疗数据存储，缺乏系统实现细节和数据共享解决途径。

为改善上述问题，笔者提出一种基于区块链、物联网、云存储和代理重加密算法的医疗数据信息系统模型，从而实现医疗数据的可靠采集、安全存储和共享方案。

1　系统设计

1.1　系统结构

基于区块链的医疗信息共享系统结构如图1所示。

收稿日期：2024-05-24；**修回日期：**2024-06-20
第一作者：温　煜(1985—)，男，广东人。

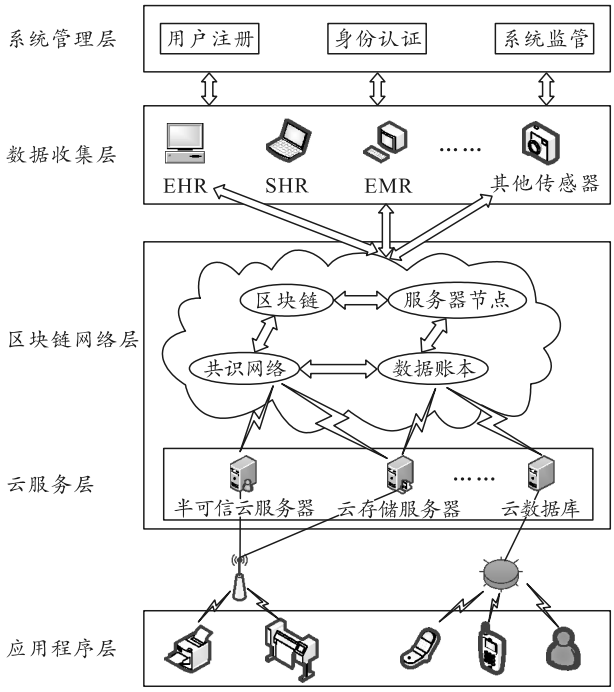

图 1　基于区块链的医疗信息共享系统

系统管理层主要对医疗机构的医生、管理节点等进行管理，包括用户注册、身份认证和系统监管等。数据收集层中的医生和数据采集器可以收集 EMR、SHR、EHR 等数据。同时，收集的医疗数据将发送到数据客户端应用程序进行处理和上传。区块链网络层由共识网络、医院和第三方提供的服务器节点、数据账本和区块链组成。同时，医疗数据索引记录和数据使用记录存储在区块链中。云服务层由半可信云服务器、云存储服务器和云数据库组成。云服务器的接口设计用于数据客户端交互、区块链访问、数据管理和数据共享。应用程序层中，患者可以与各种应用程序的数据消费者共享历史医疗数据。

1.2　系统工作过程

基于区块链的医疗信息共享系统工作过程如图 2 所示，主要包括以下关键步骤：系统初始化、数据采集与上传、数据查询与共享。

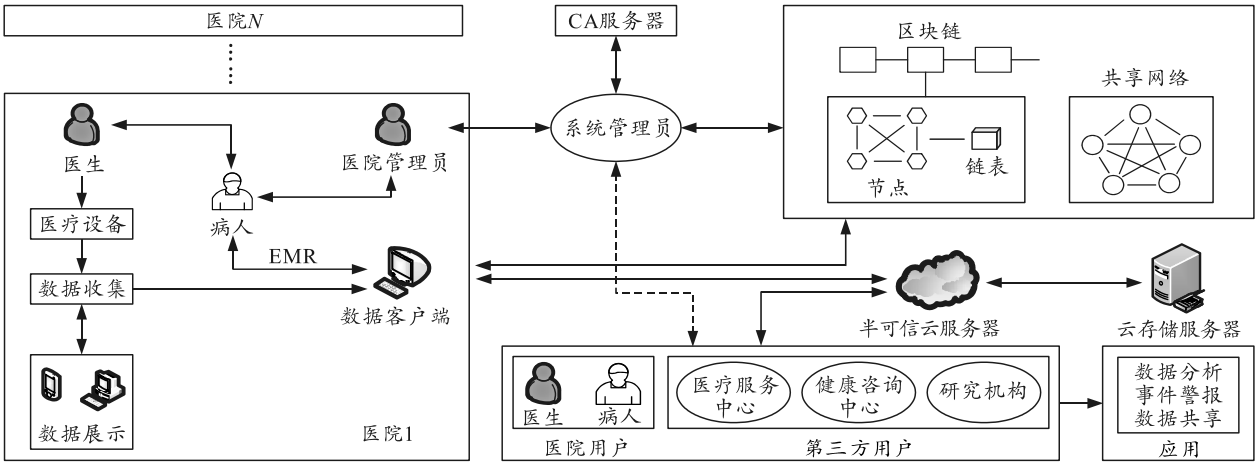

图 2　基于区块链的医疗信息共享系统工作过程

1.2.1　系统初始化

初始化阶段的目标是完成系统网络搭建和用户注册。为实现安全的数据存储和通信，用户需要提供身份信息进行注册并获取安全证书，如安全套接层(secure socket layer，SSL)/传输层安全(transport layer security，TLS)证书和 X509 证书。SSL/TLS 证书使用户能够通过 SSL/TLS 协议在系统中安全通信。X.509 为服务器节点和用户的身份证书，并存储用户的公钥。

1) 系统网络搭建。

系统首要目标是构建基于超级账本(hyperledger)结构的区块链网络。首先，医疗中心机构配置系统的加密参数并启动证书颁发机构(certificate authority，CA)服务器。然后，医疗中心系统管理(system administrator，SA)节点通过配置文件(configuration files，CF)初始化区块链网络中的服务器节点。

当任意医院 H_j 或第三方组织 T_{Hj} 要加入医疗信息共享系统时，需要向 SA 提供身份信息，从而进行资格审核。经 SA 批准后，系统将为 H_j 或 T_{Hj} 生成 SSL/TLS 和 X.509 证书。同时，H_j 或 T_{Hj} 应在区块链网络中提供和设置对等节点服务器。接着，SA 为系统创建通道，然后将对等节点添加到相应的通道，并在每个对等节点上安装和实例化区块。当创建网络后，医院 H_j 需要初始化其管理节点 H_{Mj} 并向 SA 进行注册。最后，SA 将为 H_{Mj} 生成密钥对、

SSL/TLS 和 X.509 证书。

2) 用户注册。

用户注册主要是防止无关人员进入系统，从而确保安全的数据通信。数据传输过程中，医生和患者是数据的生产者和消费者，而第三方机构用户只是数据消费者。为便于用户管理，患者和医生由管理节点注册和管理，而第三方机构由 SA 注册和管理。

首先，用户 U_x 加入系统需要生成密钥对，并在注册前提供其真实身份信息(real identity information，RID)。例如，在医院 H_j 注册的医生 D_{ij} 或患者 P_{ij} 需要提交注册请求，并提供其 RID 和公钥 $P_{Kx}(x\in(D_{i,j}, P_{i,j}))$致医院管理节点 H_{Mj}。接着，H_{Mj} 将该请求转发给 SA 进行验证，而第三方机构的用户应直接向 SA 提供上述信息。进一步，SA 将向通过注册审核的用户授予 X.509 证书和 SSL/TLS 证书。同时，SA 使用用户的公钥加密用户的 RID，并计算其消息摘要从而生成用户的系统伪身份信息(seudo identity information，PID)。SA 将用户的 RID 和 PID 信息存储到私有数据库中，并将 X.509 证书存储到云数据库中。最后，SA 将证书和 PID 返回给成功注册的用户。系统用户可以通过云服务器提供的应用程序接口(application program interface，API)从云数据库获取数字证书。

1.2.2 采集与上传

参照传统医院的医疗流程,数据收集和上传可分为：患者预约、治疗和数据收集、数据上传和存储等 3 个阶段。

1) 患者预约。

在此阶段，注册患者向医院管理节点 H_{Mj} 提供其健康信息，然后 H_{Mj} 将指派医生并为其生成预约信息。当患者 P_{ij} 前往医院 H_j 接受治疗时，需要患者向 H_{Mj} 提交预约请求。该请求携带患者的 PID、数字证书和疾病信息(isease information，DI)。接着，H_{Mj} 生成治疗 ID($T_{\mathrm{ID}}(P_{ij}, D_{ij})$)，其中 D_{ij} 为收到预约证书的患者分配医生。然后，H_{Mj} 使用医生的公钥对伪身份、分配的 $T_{\mathrm{ID}}(P_{ij}, D_{ij})$、疾病信息和患者的数字证书进行加密，从而生成治疗会话密钥 $T_{SK}(P_{ij}, D_{ij})$。最后，H_{Mj} 将向患者返回 $T_{SK}(P_{ij}, D_{ij})$和必要的治疗信息，如时间、地点和医生姓名等。

2) 治疗和数据收集。

此阶段完成医疗数据的生成和收集。当患者携带 $T_{SK}(P_{ij}, D_{ij})$到指定医生处进行治疗，首先 D_{ij} 将使用私钥解密 $T_{SK}(P_{ij}, D_{ij})$并访问其中存储的信息。然后，D_{ij} 根据疾病信息或历史医疗数据对患者进行诊断和治疗，并为患者生成 EMR 数据(M_{EMR})。如果患者需要手术，医生将使用数据采集器提取医疗器械生成的患者 SHR 数据(M_{SHR})。同时，EMR 和 SHR 都将收集到数据客户端应用程序，并由医生和患者确认。确认后，患者使用公钥对数据进行加密，得到医疗数据的密文，应用 SHA384 哈希算法计算加密医疗数据的消息摘要。最后，患者使用私钥对消息摘要进行签名，并使用伪身份获得数字签名 $D_{SP_{ij}}(M_{\mathrm{EMR}}\|M_{\mathrm{SHR}})$；同理，医生执行相同的操作从而获得 $D_{SP_{ij}}(M_{\mathrm{EMR}}\|M_{\mathrm{SHR}})$。至此，数据用户就可以从区块链中查询医疗数据的索引记录并验证数字签名。

3) 数据上传和存储。

经过治疗和数据收集阶段，加密的医疗数据上传到云存储服务器，可以获得数据存储地址 U_{RL_C}。患者可以将在上述过程中获得的数据信息构建到数据结构 P_{DE} 中，从而形成医疗数据的索引记录。P_{DE} 定义如下：

$$P_{DE}:=(T_{\mathrm{ID}}(P_{ij}, D_{ij}), U_{RL_C}, D_{SP_{ij}}(M_{\mathrm{EMR}}\|M_{\mathrm{SHR}}), D_{SD_{ij}}(M_{\mathrm{EMR}}\|M_{\mathrm{SHR}}))。\tag{1}$$

接着，患者使用数据客户端应用程序将数据结构 P_{DE} 转换为 JSON 字符串，并将其上传到代表每个医院的对等节点，同时将数据保存在区块链网络中。

1.2.3 数据查询与共享

通过系统设计一个完整的数据共享方案，从而解决传统 HIS 中数据共享困难和数据使用有限的问题。

1) 数据查询。

与他人共享数据的患者应首先获取其历史医疗数据。患者可以调用区块链中的链码来查询医疗数据索引记录，并根据伪身份和历史治疗信息提取医疗数据结构对象 P_{DE}。之后，患者可以从 P_{DE} 检索加密数据存储地址 U_{RL_C}，并从云存储服务器获取相应的加密医疗数据。接着，患者计算其消息摘要，并验证从区块链获得的索引记录中的数字签名，以检查数据是否被篡改。如果签名得到验证，患者将使用其私钥对加密数据进行解密，从而获得医疗数据的明文。

2) 数据共享。

为解决数据共享过程中云服务器可能存在的数据被盗或篡改问题，笔者基于代理重加密算法对数据进行加密，从而确保数据的安全共享。需注意，半可信云服务器仅为密钥转换提供代理服务，无法获取任何明文数据。

当数据使用者需要使用患者医疗数据时，将生成包含数字证书和伪身份的数据共享请求。患者可以通过 SA 验证申请者证书，从而确定申请者是否是合法的系统用户。假设某个第三方医疗机构(数据接收方)申请使用患者(数据发送方)的医疗数据，则数据共享过程可描述如下：

① 患者基于高级加密标准(advanced encryption standard，AES)[8]算法随机生成对称加密密钥。然后，患者使用该密钥对医疗数据的明文和索引记录中包含的部分信息进行加密，从而获得共享数据密文 $C_s(M_{\mathrm{EMR}}||M_{\mathrm{SHR}})$。当加密完成后，患者应用 RSA 算法及其公钥 $D_{SA}(P)$对原始 AES 密钥进行加密，从而生成加密的共享密钥 $D_{SA}(P^*)$。接着，患者应用 RSA 算法和公钥对其密钥进行加密，以生成代理重加密转换密钥 $R_K(P\rightarrow T_H)$。

② 半可信云服务器通过区块链码验证接收到的证书和用户的伪身份。如果数据发送方和接收方都是合法注册用户，则将使用代理重加密算法转换密钥并生成数据使用者的 AES 密钥。之后，云服务器发送转换后的加密密钥至数据接收器 $T_{Hm,dm}$。同时，半可信云服务器将医疗数据构建到数据结构 D_{UE} 中。D_{UE} 定义如下：

$$D_{UE}:=(T_{\mathrm{ID}}(P_{ij},D_{ij}),T_{Hm,dm})。\tag{2}$$

③ 服务器将 D_{UE} 转换为 JSON 字符串，并将其上载到区块链网络以进行存储。接下来，用户可以通过查询区块链获取数据使用记录，实现数据共享。

3) 数据使用。

数据使用阶段是对传统医院信息系统的功能扩展。系统用户可以处理和使用患者的历史医疗数据来实现各种应用程序。患者可以根据历史医疗数据通过系统进行病情交流，医生可以使用其他医院生成的历史医疗数据，从而实现医院间的数据共享。医疗数据对于第三方组织也具有重要意义。例如，科研机构和医疗服务提供商可以基于医疗数据进行一些数据挖掘，以获得更详尽的信息。医疗器械制造商还可以通过患者的 SHR 评估器械的性能，使用 SHR 指导器械的改进和升级。

2　系统仿真与评估

2.1　仿真环境

对所提基于区块链的医疗数据共享系统进行仿真与测试，从而评估医疗数据处理和共享的效率。按照系统设计方案进行网络建设。测试时总共部署了 7 台虚拟机模拟网络节点。测试硬件图像：服务器 10 块 Intel(R) Xeon(R) 金牌 6136 CPU，3 GHz，内存 64 G，硬盘 2 T；虚拟机 Intel(R) Xeon(R) 金牌 6136 CPU，3 GHz 1 块，内存 8 G，硬盘 20 G。软件环境如下：操作系统均为 ubuntu 18.04，Hyperledger Fabric 版本 V1.4.0。

2.2　性能评估

基于计算开销测试来评估系统性能。需注意，测试时忽略了一次性计算开销阶段的测试，例如系统构建和注册阶段。表 1 为系统测试情况说明，共包含 15 种计算指标。

表 1　系统测试情况说明

实验	说明
1	RSA 算法加密数据
2	RSA 算法解密数据
3	SHA384 算法计算消息摘要
4	AES 算法加密数据
5	AES 算法解密数据
6	用户数据签名
7	构造 P_{DE} 对象并将其上载
8	查询 P_{DE} 数据
9	生成转换密钥和数据共享密钥
10	应用代理重加密算法转换数据共享密钥
11	构造 D_{UE} 对象并将其上载
12	查询 D_{UE} 数据
13	将加密数据文件上传到云存储服务器
14	从云存储服务器下载加密数据文件
15	验证数字签名

从上表可以看出，加解密及数字签名计算消耗随着未加密医疗数据文件的大小而增加(实验 1—5)。这些计算消耗主要都是由用户的个人数据客户端应用程序计算和完成的，因此不会影响区块链系统或半可信云服务器的性能。测试结果还表明，区块链网络的计算开销与医疗数据文件的大小没有明显的关系(实验 6—15)。区块链网络的效率对整个系统的性能至关重要。

测试时，分别使用不同大小的未加密医疗数据文件(文件 1、2 和 3 分别为 64、256 kB 和 1 MB)对每个操作进行 1 000 次，最终试验结果的计算开销平均值统计如表 2 所示。

(下转第 45 页)