文章编号:1671-4598(2024)03-0188-07 DOI:10.16526/j.cnki.11-4762/tp.2024.03.028 中图分类号:TP309.2 文献标识码:A

基于区块链技术的健康医疗数据隐私加密控制系统设计

孙 煦[1,2]
(1.北京市大兴区人民医院,北京 102600;2.武汉理工大学,武汉 430070)

摘要:针对健康医疗数据隐私加密控制系统存在的访问延时增长率高、密文大、数据安全系数低等问题,设计基于区块链技术对健康医疗数据隐私加密控制系统;采用C/S体系结构,设计4层的基于区块链技术的的加密控制系统硬件;在系统软件设计中,采用基于无证书公钥体制的内容提取签名方案,加密隐私数据;引入区块链技术,设计数据加密访问控制方法MDACSC,将后序遍历策略树匹配算法与分类分级属性算法应用到访问控制结构,完成健康医疗数据的加密访问控制;采用PoP-DPoS算法改进共识机制,优化加密控制方法;经实验测试实现了健康医疗数据隐私的加密控制,结果表明:该模型访问时延增长率较低,具有平稳、高效的访问控制性能,密文小、加密成本低,解密成本极高,并且数据安全系数达到了0.98,说明该系统总体应用效果良好。

关键词:区块链技术;无证书公钥体制;健康医疗数据;DPoS算法;隐私;加密访问控制

Design of Health and Medical Data Privacy Encryption Control System Based on Blockchain Technology

SUN Xu[1,2]
(1. Beijing Daxing District People's Hospital, Beijing 102600, China;
2. Wuhan University of Technology, Wuhan 430070, China)

Abstract: Aiming at the problems of the health and medical data privacy encryption control system, such as high access delay growth rate, large ciphertext and low data security factor, a health and medical data privacy encryption control system based on blockchain technology is designed. The client/server (C/S) architecture is adopted to design a 4-layer encryption control system hardware based on blockchain technology. In the system software design, the content extraction signature scheme based on certificateless public key system is adopted to encrypt private data. Blockchain technology is introduced to design the data encryption access control method MDACSC, which applies the post-order traversal policy tree matching algorithm and classification attribute algorithm to access the control structure, and complete the encrypted access control of health and medical data. The PoP-DPoS algorithm is used to improve the consensus mechanism and optimize the encryption control method. After experimental testing, it achieves the encryption control of health and medical data privacy, and the experimental results demonstrate that the proposed model has a lower growth rate of access delay and stable and efficient access control performance, the ciphertext size is small, and the encryption cost is low, while the decryption cost is extremely high. Furthermore, the data security coefficient reaches 0.98, indicating that the system has a good application effect.

Keywords: blockchain technology; certificateless public key infrastructure; health and medical data; DPoS algorithm; privacy; encrypted access control

0 引言

通过电子健康记录系统,能够实现化验检查结果、医疗影像、用药处方、医师诊断信息、个人身份信息等医疗健康数据[1]的数字化存储,系统中还设有各种工具及标准化模板,能够减轻医生书写病历的劳动量,使医生有更多时间集中于本职的诊疗工作。该系统在为医学研究提供参考数据、降低整体医疗服务成本以及提高医院医疗服务品质等方面有着显著的作用,已经成为医疗服务中必不可少的一部分[2]。如果可以实现可靠而高效的数据共享,能够为患者跨院转治提供很大便利,也能够为第三方机构如保险业等提供可靠而权威的客户医疗数据查询渠道,进一步促进整个保健业的发展。目前该系统仍存在很大局限性,最大的问题就是各医院系统难以达成互联互通[3]。这为患者和医院工作人员都带来了很大的不便,也带来了大量的冗余数据。只有尽快实现医疗数据共享才能解决该问题。然而,在医疗数据共享中又存在着云服务器的安全隐患问题[4-5],对于风险较大的健康医疗领域来说,容易造成极大的数据损失,基于该背景对健康医疗数据隐私加密控制模

收稿日期:2023-12-11; 修回日期:2024-01-04。
作者简介:孙 煦(1990-),女,大学本科。
引用格式:孙 煦.基于区块链技术的健康医疗数据隐私加密控制系统设计[J].计算机测量与控制,2024,32(3):188-194.

型进行研究。

对于该问题的研究，目前发达国家由于经济基础良好已经积累了很多经验，我国医疗信息标准化方面的建设现在仍处于早期阶段，但相关研究已经越来越多，并取得了一定研究成果。其中文献［6］中针对低压输电网络提出一种安全传输敏感数据加密控制技术，主要应用同态加密发送感知请求，通过对同态加密密匙池实施预设处理形成随机密钥，并通过索引值理论实现同态密文的生成，实施敏感数据加密控制，同时构建了加密认证协议。实验结果表明，该方法能够保障用户隐私数据安全性。文献［7］中针对通信网络设计了一种基于区块链的节点位置隐私加密控制模型，实验结果表明，该模型能够加强网络体系在隐私文本加密处理方面的能力。文献［8］研究了一种使用区块链保护车联网数据隐私的方法，该方法利用区块链实现数据的存储、访问和用户撤销中的信任问题，基于无证书密码体系实现区块链交易的签名和认证，首先数据隐私保护。文献［9］在分布式数据安全存储模型中采用 IPFS 存储技术及改进数据加密技术，并且结合了分散式密文策略属性基加密数据，避免数据泄露，保护数据隐私。以上方法在健康医疗数据隐私加密控的应用中存在访问时延增长率较高，控制效果不够平稳的问题，因此针对健康医疗数据设计一种新的基于区块链技术的隐私加密控制模型。

1　健康医疗数据隐私加密控制系统硬件设计

1.1　数据隐私加密控制系统整体架构设计

传统的健康医疗数据隐私加密控制系统由于未去中心化，导致系统安全性不佳，因此，本文以区块链技术为基础，采用 C/S 体系结构，设计一种新的健康医疗数据隐私加密控制系统。该系统整体架构如图 1 所示。

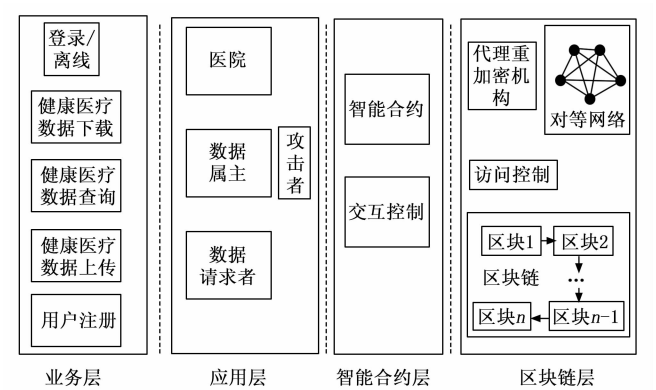

图 1　健康医疗数据隐私加密控制系统架构

根据图 1 所示的健康医疗数据隐私加密控制系统架构可知，该系统包含四层，分别为业务层、应用层、智能合约层和区块链层。针对这四层进行系统硬件设计，具体设计如下。

1.2　系统硬件设计

1.2.1　业务层

该层包含用户和管理者的登录/离线、数据下载、查询和上传。该层作用是为用户和管理者提供访问和管理系统的接口。在硬件实现方面，业务层通常需要使用计算设备（如个人电脑、智能手机等）以及采用 Cisco ISR 4000 路由器和 Cisco Catalyst 交换机网络连接设备。

1.2.2　应用层

该层包含医院、数据属主、数据请求者、攻击者，其作用是作为系统的参与方，参与数据的交互和应用。医院是医疗数据系统的核心参与方，它负责收集、存储和处理医疗数据[10-11]。在应用层中，医院需要使用特定的应用程序或接口来与系统进行交互，例如通过登录、查询、上传和下载数据等操作。医院通常需要使用专业的医疗信息系统（HIS）或电子病历系统（EMR）等应用程序来与系统进行交互。数据属主是医疗数据的所有者，他们负责授权数据请求者访问自己的数据。在应用层中，数据属主需要通过身份验证和授权机制来控制对数据的访问。通常，数据属主可以通过控制对特定数据集的访问权限来限制数据请求者的访问。数据请求者是需要访问和使用医疗数据的人员或组织，例如研究人员、数据分析师或政府部门等。在应用层中，数据请求者需要通过身份验证和授权机制来获得访问权限，并使用特定的应用程序或接口来查询和下载数据。攻击者是试图非法获取或篡改医疗数据的人员或组织。在应用层中，需要采取安全措施来防止攻击者的入侵和数据泄露。例如，采用防火墙、入侵检测系统（IDS）、加密等技术来保护数据的机密性和完整性。此外，应用层还需要支持各种不同的数据类型和格式，例如文本、图像、音频和视频等。同时，应用层还需要支持不同的数据查询和检索方式，例如基于关键词的搜索、基于结构的查询等。总之，应用层是医疗数据系统中最为关键的一层，它需要支持不同的参与者进行数据的交互和应用，并确保数据的安全性和隐私性。该层通过 Dell PowerEdge R740 服务器通过系统服务。

1.2.3　智能合约层

部署在以太坊（Ethereum）平台的智能合约。智能合约层作为应用层和区块链层之间的桥梁，将应用层的计算结果锚定到区块链层。在编写智能合约的过程中，系统定义了若干的结构体（如 File、Record、User 等），实现以自定义的数据形式存储电子数据的关键信息，并且实现交互控制功能。在该层采用 Intel Core i7-4720HQ 的 CPU。

1.2.4　区块链层

该层包含区块链、代理重加密机构、访问控制、对等网络，作为系统去中心化的核心，实现健康医疗数据隐私保护的访问控制。其提供安全的分布式数据存储和访问控制，采用 EMC Unity 650F 存储区块链数据，并且采用 IBM Power System S922 区块链服务器实现服务功能。

2　健康医疗数据隐私加密控制系统软件设计

2.1　健康医疗数据隐私加密

在完成基于区块链技术的的加密控制系统硬件设计后，

设计健康医疗数据隐私加密控制系统软件。首先，设计一种基于无证书公钥体制的内容提取签名方案，设计数据隐私加密[12]是为了提高数据的安全性，避免非法篡改或损坏，导致数据完整性降低，也是为引入区块链技术构建健康医疗数据隐私加密控制算法奠定基础。无证书公钥体制（CL-PKI，certificateless public key infrastructure）是一种公钥密码学体系结构，用于实现安全通信和数据保护。它是在传统的公钥基础设施（PKI，public key infrastructure）和身份基础设施（IBC，identity-based cryptography）之间的一种折衷方案。在传统的 PKI 中，用户的公钥需要通过数字证书进行认证，而数字证书需要由受信任的第三方证书颁发机构（CA，certificate authority）签发。然而，CL-PKI 采用了一种不依赖证书的方式，避免了由证书颁发机构带来的复杂性和单点故障问题。在无证书公钥体制中，用户的公钥和私钥是根据用户自己的身份信息以及系统的安全参数生成的。通过引入一个称为密钥生成中心（KGC，key generation center）的特殊实体，用户可以向其提供自己的身份信息，然后由 KGC 生成用户的公私钥对。KGC 仅负责密钥的生成，而不涉及有效性验证和签名。无证书公钥体制可以提供与传统 PKI 类似的功能，如身份验证、加密和签名，同时避免了传统 PKI 中需要信任第三方证书颁发机构的问题。它适用于一些特定的场景，如基于云计算的数据共享、物联网中的设备通信等，并且被广泛应用于隐私保护和安全通信领域。基于此，基于无证书公钥体制的内容提取签名方案，设计方案由七部分构成，分别为签名验证、签名提取、签名生成、完整密钥生成、部分密钥生成、秘密值生成、系统参数建立[13]。以上七部分的设计具体如下。

1）系统参数建立：

系统参数建立（System Parameter Establishment）是用于建立和分发系统中所需的公共参数，这些参数在整个签名方案中起到了关键的作用，如加密、哈希函数等。在系统参数建立过程中，用 q 表示大素数，设 q 使秘密值集合 S_q^* 在离散对数问题上难以处理，由密钥生成中心随机对系统主密钥 y 进行选择并秘密将其保存起来，对密匙 T_{pub} 进行计算，具体如下式所示：

$$T_{\text{pub}} = yQ \tag{1}$$

式（1）中，y 为系统主密钥；Q 为限域上椭圆曲线 $W_F(\alpha,\beta)$ 一个循环子群的一个生成元。

选择下式的哈希函数：

$$h:\{0,1\}^* \rightarrow S_q^* \tag{2}$$

式（2）中，h 指的是哈希函数[14]；S_q^* 为秘密值集合。

公开如下式的系统参数：

$$P_s = \{q, Q_F, R/Q_F, H, D, T_{\text{pub}}, h\} \tag{3}$$

式（3）中，D 指的是椭圆曲线 $W_F(\alpha,\beta)$ 上的一个点；R 是指椭圆曲线 $W_F(\alpha,\beta)$ 上的点集；Q_F 为限域；H 为循环子群。

2）秘密值生成：

秘密值生成（Secret Value Generation）是用于生成额外的秘密值，这些值通常用于增强安全性和提供其他功能，如随机性和防抵赖性等。在该部分中，签名者随机对秘密值 $y_s \in S_q^*$ 进行选择，将其作为自己的秘密值，计算此时的密匙，具体如下式：

$$Q_s = y_s Q \tag{4}$$

式（4）中，y_s 为签名者随机对秘密值。

通过秘密渠道将 Q_s 传送给密钥生成中心，将其作为部分公匙。

3）部分密钥生成：

部分密钥生成（Partial Key Generation）是用于生成辅助私钥和对应的辅助公钥。辅助密钥主要用于签名提取，并保证提取过程能够快速和高效地完成。该部分具体设计如下所示。

（1）由密钥生成中心对部分公匙实施计算，具体如下式：

$$J_s = h(ID_F, P_s, V_s, Q_s) \tag{5}$$

式（5）中，V_s 指的是用户 O_i 的部分公匙[15]；ID_F 为签名者的身份。

（2）由密钥生成中心对部分私匙实施计算，具体如下式：

$$I_s = e_s + J_s y \tag{6}$$

式（6）中，e_s 指的是用户 O_i 的部分私匙。

4）完整密钥生成：

完整密钥生成（Complete Key Generation）是用于生成完整的密钥对，包括主私钥和对应的主公钥。这些密钥用于签名生成和验证。该部分具体设计如下所示：

（1）签名者接收密钥生成中心发送来的 J_s 后，完整公匙是 $P_L = (J_s, V_s)$。

（2）签名者接收密钥生成中心发送来的 I_s 后，完整私匙为 $S_L = (I_s, e_s)$[16]。

5）签名生成：

签名生成（Signature Generation）是用于根据私钥和消息生成数字签名。此操作是通过对消息进行加密和哈希计算来完成的。在该部分中假设要签名的消息是 N，其全局签名具体如下式：

$$\chi_{\text{full}} = (C \| S \| \chi) \tag{7}$$

式（7）中，C 指的是内容提取访问结构；S 是指 C 的标记；χ 指的是子消息的签名。

6）签名提取：

签名提取（Signature Extraction）是用于从签名中提取出消息或相关信息。这使得可以解析签名中的特定数据，而无需拥有完整的消息。在该部分中验证全局签名的正确性后输出提取签名，具体如下式：

$$\chi_{\text{ext}} = (Z(N') \| S \| \chi_{ij}) \tag{8}$$

式（8）中，$Z(N')$ 指的是指定 C 构造出来的子消息集；χ_{ij} 是指 $Z(N')$ 中子消息的对应签名。

7）签名验证：

签名验证（Signature Verification）是用于验证签名的

有效性，确保签名是由私钥对应的公钥生成的，以及数据没有被篡改。在该部分中对于各子消息，计算其哈希函数，从中得到子签名 χ_{ij}，验证该子签名，成立则提取签名 χ_{ext} 为正确签名，反之 χ_{ext} 为无效签名。

通过上述的签名验证、签名提取、签名生成、完整密钥生成、部分密钥生成、秘密值生成、系统参数建立完成基于无证书公钥体制的健康医疗数据隐私保护设计，为基于区块链技术的健康医疗数据隐私加密控制模型设计奠定基础。

2.2　基于区块链技术的数据隐私保护加密控制方法

2.2.1　数据隐私保护加密控制的区块链技术原理

在健康医疗数据隐私经过上述加密后，数据存在被中心化机构操纵的可能，并且为了减少中间人和人为错误，并增加数据访问过程的安全性和效率，在加密健康医疗数据隐私的基础上，提出一种基于区块链技术的数据加密访问控制方法 MDACSC，将机密算法和区块链技术结合，实现健康医疗数据的加密访问控制。在 MDACSC 中，区块链技术被应用于数据访问控制的过程中，其需要移动终端用户、边缘服务器和身份管理中心三类角色对象的协同配合。移动终端用户在区块链体系中与 OBT 单元配合，确保数据隐私的定义和信息参量传输，保持系统连通状态以满足加密模板的一致性原则。边缘服务器下沉数据至身份管理中心，生成和存储加密模板，并等待身份管理中心的认证。身份管理中心管理并推送源码模板，保证数据与码源对应关系的稳定性，实现区块链技术的加密访问控制。区块链是一种分布式账本技术，它通过去中心化的方式记录和验证交易，并确保数据的不可篡改和安全性。区块链技术的区块本质是区块链中数据存储的结构单元，作用是存储访问等摘要信息。它可以消除传统的中心化控制，提供更强大的数据访问和管理机制。区块头和区块体两部分构成了每一个区块，其中，区块头中的信息拥有标识和定位两个功能，标识此区块自身信息和前一区块的摘要信息，定位区块在整个账本中的位置；另外，区块体中的信息拥有存储和验证两个功能，摘要信息的存储，信息的验证，可以保证隐私数据的安全。结合上述章节的哈希计算设计的区块如图 2 所示。

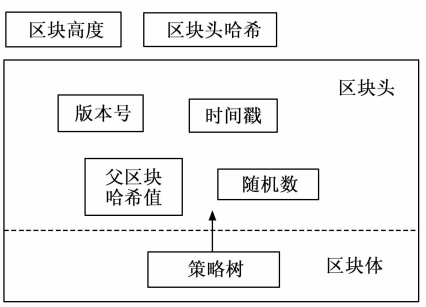

图 2　区块结构

设计区块后，设计链式存储结构，其是指将每一个区块按照生成时间的顺序依次连接起来。在整个区块链中，每一个区块的高度都不相同，从开始处算起，第一个区块的高度为 0，第二个区块的高度为 1，以此类推，后一个区块的高度都要比前一个区块高 1，并且还要将前一个区块头的父区块哈希地址写入该区块头中。区块链上各个区块之间的链接由各区块头的父区块哈希地址完成，设计的链接方式如图 3 所示。

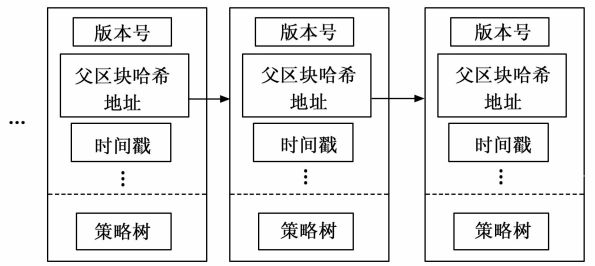

图 3　链式存储结构

因为恶意节点要想改变某区块中的健康医疗数据时，需要重新计算该区块之后的所有区块，并且计算网络中所有合法区块链并追赶上进度，从而提交该区块所在的链分叉给网络中的节点，这些计算过程完成后，才有重新上链且被认可的可能，该过程计算量庞大，因此，恶意节点访问健康医疗数据的成功率较低。

2.2.2　区块链技术的加密访问控制

基于上述通过将区块链技术应用于数据加密访问控制，MDACSC 能够增强健康医疗数据的保护和隐私，并确保数据的完整性和可追溯性。MDACSC 将后序遍历策略树匹配算法与分类分级属性算法应用到了访问控制结构中，能够实现访问控制效率的提升。MDACSC 的工作流程可以分为五个阶段，首先，初始化系统，生成系统参数，包括系统公钥、系统主密钥、系统公共参数，并将其上传至区块链中实施存储与共享，并且生成数据访问者私钥 b_k 或数据属主私钥 b_l。然后，存储数据，加密原始密文，具体如下式所示：

$$SymEncry(m,K)\rightarrow L_T \tag{9}$$

式（9）中，K 指的是加密秘钥；L_T 是指生成密文[17]；m 为健康医疗数据的明文。

在加密原始密文后，向 IPFS 发送加密文件 L_T 并实施分布式存储，获得父区块密文哈希地址后与时间戳信息、加密秘钥 K 构成关键信息集合，具体如下式：

$$I_K=(K,L_T,L_P,H_A) \tag{10}$$

式（10）中，L_P 为时间戳信息；I_K 为关键信息集合；H_A 为父区块密文哈希地址。

加密上述获取的关键信息集合，进一步提高健康医疗数据隐私的安全性。输入系统参数、数据私匙、访问结构 (κ',λ') 与关键信息集合 I_K，生成代理重加密中的第一次密文 L_F，将其上传至区块链实施存储。

在初步加密和存储数据隐私后，设计访问控制方法，

通过控制访问的安全性，提高健康医疗数据隐私加密控制系统的安全性。依据资源隐私等级为属性分配合约 AAC 设置对应属性粒度的加密访问控制策略，以策略事务的形式将其存储至区块链上[17]。返回区块链上实体属性信息与访问控制策略，将二者分别返回至策略信息点 PIP 与策略管理点 PAP 中。通过医疗数据访问实体面向策略执行点 PEP 实施访问请求的发送，由 PEP 向上下文处理器发送请求，由处理器对请求进行解析，将其转换为 XACML 格式并向 PDP 发送。PDP 解析 XACM 访问请求，向上一步骤中的处理器发送属性查询。由处理器向 PIP 实施属性信息查询信息的发送。由 PIP 检索、整理相关属性信息，向 PDP 发送。由 PDP 解析访问请求属性信息，通过优先级判决合约 PDC 比较访问资源等级与访问者，通过处理器转化判决结果，向 PEP 发送，由 PEP 完成访问控制工作[18]。在设计访问控制方法后，生成属性重加密密钥，实施属性代理重加密。在数据隐私全部加密后，需要设计数据获取方法，该方法首先实施重加密密文解密，然后，获取对称加密数据的对应 IPFS 地址，寻址后下载，最后，输入对称加密数据、对称秘钥，获取 EMR 明文，完成数据隐私获取。至此完成区块链技术的加密访问控制设计。

2.2.3 加密控制优化

为解决健康医疗数据隐私加密控制系统的加密访问控制中应用区块链技术时发生记账权竞争问题，设计一种基于 PoP-DPoS 算法的改进共识机制，确定记账权归属，通过该方法优化系统的加密控制方法。基于 PoP-DPoS 算法的改进共识机制是以 PoP 算法为基础改进后得到的。

PoP 算法在确定真目标哈希值时容易引发不必要的分叉问题，同时为避免全部医院参与竞争记账权时对于小型医院造成负担，应用 DPoS 算法对 PoP 算法进行改进，设计一种 PoP-DPoS 改进共识机制[19]。在该改进共识机制发生事务时，整个网络作出发布指令，如下式：

$$\mu = \vartheta_H + n\xi_H \tag{11}$$

式（11）中，ϑ_H 指的是真目标哈希值；n 是指伪目标哈希值的数量；ξ_H 指的是伪目标哈希值。

在发布指令后，各 PoP 节点应用自己的哈希排序算法对挖矿顺序进行确定，并且创建 PoP 节点的区块头，结合穷举 Nonce 值实施挖矿。当计算得到一个合格的哈希时，则对 Nonce 值实施处理，公式为：

$$Nonce' = \lg Nonce \tag{12}$$

式（12）中，$Nonce$ 为合穷举 Nonce 值。

比较 $Nonce'$ 与 DPoS 超级节点所给出的期望值，当二者不相同，则该 PoP 节点进入等待时间，等待时间为：

$$\begin{cases} t = 1\ \text{min} & \upsilon < 10 \\ t \leqslant 10\ \text{min} & \upsilon \geqslant 10 \end{cases} \tag{13}$$

式（13）中，t 指的是等待时间；υ 是指 PoP 节点的数量[20]。

在等待过程中，其他 PoP 节点需要继续挖掘。在计算出下一个适合的哈希值前，当前的超级节点能够多指定一个期望值，不断重复后直到第 10 次指定的期望值个数为 10 个时，二者，相同。当期望值与取模结果一致时，则向其他超级节点提交实施进一步的验证。当半数以上的超级节点通过验证，认定区块生成成功。成功验证区块后，下一个区块交由下一个超级节点实施初步验证[21]。当全部超级节点都通过区块验证后，如网络中加入新增的 DPoS 节点则实施 DPoS 节点的重新构造；否则在 DPoS 节点池内顺序选择一个节点，并利用其替换一个超级节点。至此完成基于区块链技术的健康医疗数据隐私加密控制软件设计，实现数据加密。

3 实验及分析

3.1 实验环境与实验过程

对于设计的基于区块链技术的健康医疗数据隐私加密控制模型，在其性能测试中，利用该模型对某地区的多家医院实施医院数据隐私加密访问控制。

配置以下实验环境：

1）Python 版本：3.8.0；

2）Ganache：2.5.3.8；

3）Solidity：version 0.8.2；

4）机带 RAM：32GB；

5）CPU：Intel Core i7-4720HQ；

6）操作系统：Windows10。

首先对实验地区医院的健康医疗数据应用设计的基于无证书公钥体制的内容提取签名方案，实现实验健康医疗数据的隐私保护。

接着应用基于区块链技术的数据加密访问控制方法 MDACSC，实现健康医疗数据的加密访问控制。在 MDACSC 的应用中，在联盟链内部选择多个权威节点作为数据加密访问控制中的记账节点，确保医疗联盟链能够正常运转。最后应用设计的基于 PoP-DPoS 算法的改进共识机制来确定记账节点的记账权归属。

3.2 健康医疗数据隐私加密控制模型参数设置

基于区块链技术的健康医疗数据隐私加密控制模型中涉及多个数学参数，而加密控制模型的参数取值过大或者过小等均有可能影响模型的性能，并且在一定程度上影响实验结果的准确性，因此，为了确保模型的性能和实验结果的准确性，需要设置基于区块链技术的健康医疗数据隐私加密控制模型参数的数值，数值设置如表 1 所示。

表 1 健康医疗数据隐私加密控制模型参数

序号	参数	数值
001	大素数	524 287
002	真目标哈希值	200
003	伪目标哈希值	100
004	等待时间	⩽10
005	PoP 节点的数量	40

根据上述表 1 总的数值设置健康医疗数据隐私加密控

制模型参数，完成实验的准备工作。

3.3　测试项目与测试结果分析

对本文设计的基于区块链技术的健康医疗数据隐私加密控制模型多方面的性能进行测试，在测试中将安全传输敏感数据加密控制技术与基于区块链的节点位置隐私加密控制模型作为对比方法，共同进行测试，并分别用方法 1、方法 2 来表示，并且设计的健康医疗数据隐私加密控制模型称为设计模型。

在健康医疗数据隐私加密控制过程中，首先测试其访问控制性能，共设置两个实验条件：

1）生成 4 000 条健康医疗数据属性访问请求，分别将其应用于有 1 000 条、2 000 条、3 000 条、4 000 条加密访问控制策略的对应策略集中，实施时延增长率测试。

2）选取 1 000 条访问控制策略，生成 50 条、100 条、200 条、500 条健康医疗数据属性访问请求，实施访问时间测试。

第一个实验条件下的测试结果如图 4 所示。

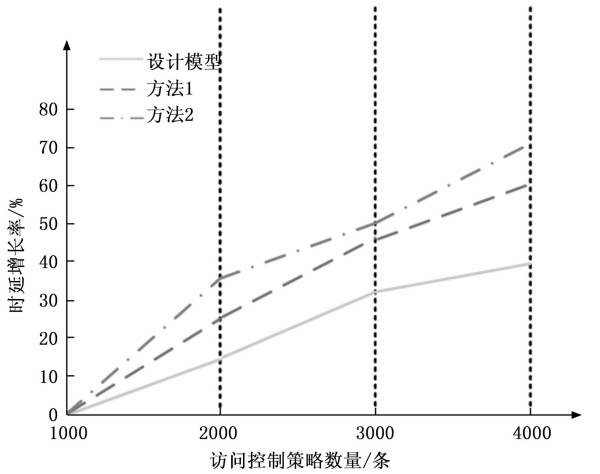

图 4　第一个实验条件下的测试结果

根据图 4 可知，随着健康医疗数据加密访问控制策略数量的增长，设计模型的访问时延增长率一直低于两种对比方法，并且差值较大。在 4 000 条加密访问控制策略的对应策略集时，设计模型的访问时延增长率仅为 37.2%，而方法 1 的访问时延增长率达到了 60.1%，方法 2 的访问时延增长率最高，该数值达到了 71.3%，3 种方法的访问时延增长率数值对比可知，设计方法的访问时延增长率降低了 20.0%以上。该实验结果说明 3 种方法相比之下，设计模型具有更为平稳、高效的访问控制性能。

在完成第一个实验条件下的测试后，进行第二个实验条件下的测试，在该部分也使用设计模型、方法 1 和方法 2 进行对比分析，测试结果如图 5 所示。

在第二个实验条件下，相比两种对比的实验方法，设计模型的访问时间明显更低，该控制模型在 50 条健康医疗数据属性访问请求时，访问时间最低，该值仅为 4.8 s，而

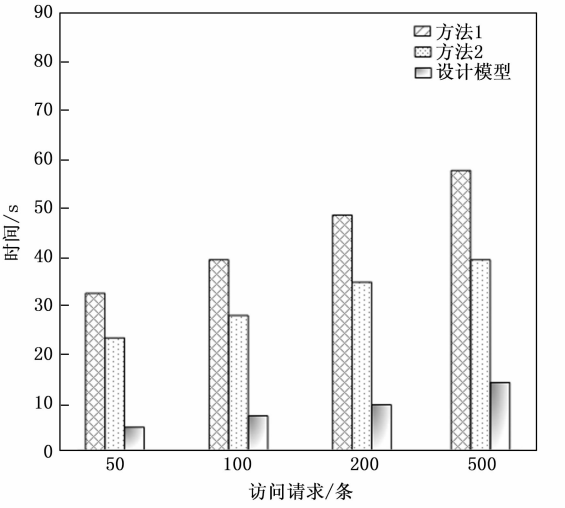

图 5　第二个实验条件下的测试结果

对应的方法 1 和方法 2 的访问时间却在 23.0 s 以上，此时对比方法的访问时间也是最低的，3 种加密控制方法的访问时间随着访问请求条数的增加而增加，在 500 条的健康医疗数据属性访问请求时，本文设计模型的访问时间仅为 16.1 s，而此时的方法 1 和方法 2 的访问时间达到了 40.0 s 以上。由此可知，设计模型的访问时间最短，有效降低了访问时间，在该方面具备了较好的性能。

以上实验结果表明，设计模型在缩短访问时延取得了明显效果，同时增强了访问控制的稳定性。

接着从多方面着手测试设计模型与两种对比方法的数据隐私保护功能与加密功能，具体来说，测试隐私保护策略与加密访问控制策略的密文大小、加密成本以及解密成本，测试结果如表 2 所示。

表 2　数据隐私保护功能与加密功能测试结果

项目		设计模型	方法 1	方法 2
隐私保护策略	密文大小	$(11+2)\lvert Y\rvert$	$(18+2)\lvert Y\rvert$	$(20+3)\lvert Y\rvert$
	加密成本	$(2\lvert\theta\rvert+1)\rho$	$(3\lvert\theta\rvert+2)\rho$	$(4\lvert\theta\rvert+3)\rho$
	解密成本	$(12\lvert\theta\rvert+2)\rho$	$(8\lvert\theta\rvert+1)\rho$	$(6\lvert\theta\rvert+1)\rho$
加密访问控制策略	密文大小	$(22+2)\lvert Y\rvert$	$(35+3)\lvert Y\rvert$	$(40+3)\lvert Y\rvert$
	加密成本	$(3\lvert\theta\rvert+1)\rho$	$(5\lvert\theta\rvert+2)\rho$	$(7\lvert\theta\rvert+3)\rho$
	解密成本	$(30\lvert\theta\rvert+5)\rho$	$(15\lvert\theta\rvert+3)\rho$	$(20\lvert\theta\rvert+3)\rho$

表 2 中 $\lvert Y\rvert$ 指的是每个循环群的元素长度；$\lvert\theta\rvert$ 是指最小授权集合的大小；ρ 表示实施一次双线性映射的时间。测试结果表明，相比两种对比方法，设计模型的密文更小，加密成本更低，而解密成本则远高出两种对比方法，说明无论是在隐私保护策略中，还是在加密访问控制策略中，设计模型的加密效果都更好。

为了进一步验证设计的一基于区块链技术的健康医疗数据隐私加密控制模型的性能，分析应用 3 种方法后的数据安全性，以数据安全系数为评估指标，该指标越高，则说明加密效果越好，安全性能越高，该值的取值在［0，1］

之间，最高值为 1。实验结果如表 3 所示。

表 3 不同方法的数据安全系数

数据量/M	数据安全系数		
	设计模型	方法 1	方法 2
200	0.98	0.94	0.93
400	0.98	0.93	0.92
600	0.99	0.93	0.91
800	0.99	0.94	0.92
1 000	0.99	0.94	0.93
1 200	0.99	0.92	0.95

根据表 3 中的不同方法的数据安全系实验结果数据可知，3 种方法的数据安全系数均较高，安全系数数值在 0.90 以上，具备一定的加密安全防护效果。但是详细分析可知，本文设计模型的数据安全系数高于对比方法的方法 1 和方法 2 的数据安全系数，设计模型的数据安全系数达到了 0.98 以上，最高为 0.99，而方法 1 和方法 2 的数据安全系数的最高值仅为 0.94 和 0.95，相比可知，本文设计模型的数据安全系数提高了 0.04 以上。由此可知，本文设计的基于区块链技术的健康医疗数据隐私加密控制模型具备更优的性能，其有效提高了健康医疗数据隐私保护加密的安全性。

4 结束语

随着信息技术的不断发展，各行业都向着数字化趋势发展，医疗行业也不例外，可以说医疗行业的数字化发展已经是一种必然的趋势。在这种发展趋势下，数字医疗这一概念获得了各界的认可，并取得了丰富的发展成果。其中获得最普遍应用的就是电子健康记录系统。为使该系统尽快实现安全地医疗数据共享，设计一种基于区块链技术的健康医疗数据隐私加密控制系统，实现了良好的加密与加密访问控制效果，对于数字医疗的发展有一定意义。设计系统的数据隐私加密的运算量降低较小，后续研究工作将针对软件方法的运算量进行深入研究，以期进一步简化算法，降低运算量，提高系统的效率。

参考文献：

[1] WANG Z, MYLES P, TUCKER A. Generating and evaluating cross : ectional synthetic electronic healthcare data: Preserving data utility and patient privacy [J]. Computational Intelligence, 2021, 37 (2): 819 - 851.

[2] 毕浩然，曾 智，姚育楠. 区块链＋医疗个人健康数据存储——基于 medicalchain 平台的分析 [J]. 中国卫生事业管理，2021，38 (5)：328 - 330.

[3] 陈 怡. 健康医疗数据共享与个人信息保护研究 [J]. 情报杂志，2023，42 (5)：192 - 199.

[4] KIRAN G M, NALINI N. Ontology-based data access control model supported with grid computing for improving security in healthcare data [J]. Transactions on Emerging Telecommunications Technologies, 2022, 33 (11): 4589.1 - 4589.19.

[5] ZHANG G, YANG Z, LIU W. Blockchain-based privacy preserving e-health system for healthcare data in cloud [J]. Computer Networks, 2022, 203 (11): 108586.1 - 108586.9.

[6] 李 远. 低压输电网络安全传输敏感数据加密控制技术 [J]. 信息技术，2023，47 (1)：191 - 196.

[7] 马亚蕾，张 怡. 基于区块链的通信网络节点位置隐私加密控制模型设计 [J]. 计算机测量与控制，2023，31 (4)：246 - 251.

[8] 杨颜博，张嘉伟，马建峰. 一种使用区块链保护车联网数据隐私的方法 [J]. 西安电子科技大学学报，2021，48 (3)：21 - 30.

[9] 赵 钦，蔡杰杰，蔡耀君，等. 基于分布式区块链的数据安全保障技术研究 [J]. 电子设计工程，2022，30 (23)：33 - 36，41.

[10] YAN S, HE L, SEO J, et al. Concurrent Healthcare Data Processing and Storage Framework Using Deep-Learning in Distributed Cloud Computing Environment [J]. IEEE transactions on industrial informatics, 2021 (4): 17.

[11] LIU M, LI S, YUAN H, et al. Handling missing values in healthcare data: a systematic review of deep learning-based imputation techniques [J]. Artificial Intelligence in Medicine, 2023, 142 (8): 1. 1 - 1. 13.

[12] LAKSHMI, THENMOZHI C, RAYAPPAN K. Neural-assisted image-dependent encryption scheme for medical image cloud storage [J]. Neural Computing & Applications, 2021, 33 (12): 1 - 14.

[13] 赵丙镇，陈智雨，闫龙川，等. 基于区块链架构的电力业务交易数据隐私保护 [J]. 电力系统自动化，2021，45 (17)：20 - 26.

[14] 李雅兰，王 倩，袁 可，等. 雾辅助的隐私保护分层多维数据聚合研究 [J]. 小型微型计算机系统，2022，43 (7)：1499 - 1504.

[15] 牛淑芬，戈 鹏，宋 蜜，等. 移动社交网络中基于属性加密的隐私保护方案 [J]. 电子与信息学报，2023，45 (3)：847 - 855.

[16] 田 静，杜云明，李 帅，等. Paillier 加密的隐私保护群智感知任务发布算法 [J]. 计算机科学与探索，2022，16 (6)：1327 - 1333.

[17] 殷新春，王梦宇，宁建廷. 轻量级可搜索医疗数据共享方案 [J]. 通信学报，2022，43 (5)：110 - 122.

[18] 刘海辉，陈建伟，黄 川. 物联网中无可信权威中心的隐私保护数据聚合方案 [J]. 福建师范大学学报：自然科学版，2022，38 (3)：35 - 45.

[19] 张泽辉，富 瑶，高铁杠. 支持数据隐私保护的联邦深度神经网络模型研究 [J]. 自动化学报，2022，48 (5)：1273 - 1284.

[20] 张应辉，陈博文，曹 进，等. 具有隐私保护的细粒度智能家居远程数据安全更新方案 [J]. 电子与信息学报，2023，45 (3)：810 - 818.

[21] 张嘉伟，马建峰，马 卓，等. 云计算中基于时间和隐私保护的可撤销可追踪的数据共享方案 [J]. 通信学报，2021，42 (10)：81 - 94.