

基于区块链的医疗信息属性加密访问控制方案

郑丽娟^{1,2}, 刘佳琪¹, 陶亚男¹, 章睿², 张宇¹, 吴朋钢¹, 尤军考³

¹ 石家庄铁道大学信息科学与技术学院 石家庄 中国 050043

² 中国科学院信息工程研究所, 信息安全国家重点实验室 北京 中国 100093

³ 中国移动通信集团河北有限公司政企客户部 石家庄 中国 050021

摘要 医疗信息的访问互通有助于医生掌握转诊患者的病情, 及时准确地为患者提供医疗服务。然而医疗数据涉及到患者的隐私, 存在数据泄露的风险, 一旦泄露不仅会损害医疗机构的声誉, 还会影响患者的个人生活, 并且医疗信息大多由医疗机构管理, 患者对自己医疗数据的使用情况并不知情。访问控制是医疗信息共享中重要的安全机制, 其中, 基于属性的加密机制可以实现细粒度的访问控制, 但是仍存在属性授权集中、解密开销大和追溯难的问题。区块链技术在实现分布式医疗机构节点间信任建立和数据共享方面有很多优势。因此, 针对上述问题, 本文从医疗数据共享场景下患者敏感信息保护的需求出发, 结合区块链技术对医疗信息的访问控制机制进行研究, 提出了一个基于区块链的医疗信息属性加密访问控制方案, 建立了多授权机构的访问控制模型, 避免了单一授权带来的信任问题; 设计了代理解密算法, 降低了终端的解密开销, 提高了解密效率; 支持访问者的属性撤销, 实现了患者对医疗数据的灵活控制; 同时, 利用区块链自身优势实现了对属性授权机构的追溯问责。安全性分析与性能分析表明, 所提方案在随机预言机模型下是静态安全的, 且具有更低的计算开销和存储开销。

关键词 区块链; 医疗信息; CP-ABE; 访问控制

中图分类号 TP309.2 DOI号 10.19363/J.cnki.cn10-1380/tn.2023.01.07

Medical Information Attribute Encryption Access Control Scheme Based on Blockchain

ZHENG Lijuan^{1,2}, LIU Jiaqi¹, TAO Yanan¹, ZHANG Rui², ZHANG Yu¹, WU Penggang¹, YOU Junkao³

¹ School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang 050043, China

² State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

³ Department of Enterprise Customer, China Mobile Communications Corporation Hebei Co., Ltd, Shijiazhuang 050021, China

Abstract The access and intercommunication of medical information helps doctors to grasp the patient's condition when the patient goes to the different hospitals, and provides convenience for medical services. However, the medical data involves patients' privacy, and there is a risk of data leakage. Once the medical data is leaked, it will not only damage the reputation of medical institutions, but also affect the personal life of patients. Moreover, most medical information is managed by medical institutions, and patients are not aware of the use of their own medical data. The access control is an important security mechanism in the medical data sharing scenario. Among them, the attribute-based encryption mechanism can realize fine-grained access control, but it has the problems of centralized attribute authorization, large decryption overhead, and difficulty in traceability. The blockchain technology has many advantages in establishing trust and sharing data among nodes in distributed medical institutions. Therefore, in order to solve these problems, in this paper, based on the demand of patient sensitive information protection in the medical data sharing scenario, the access control mechanism of medical information is studied with blockchain technology, and a medical information attribute encryption access control scheme based on blockchain is proposed. The access control model of multiple authorization agencies is established to avoid the trust problem caused by single authorization, and a proxy decryption algorithm is designed to reduce the terminal decryption cost and the decryption efficiency is improved. The scheme supports the revocation of visitors' attributes and realizes the flexible control of medical data by data owners. At the same time, it uses the advantages of blockchain itself to achieve traceability accountability of attribute authorization institutions. The security and performance analysis shows that the proposed scheme is statically secure under the random oracle model, and has better system performance and computing efficiency.

Key words blockchain; medical information; CP-ABE; access control

通讯作者: 郑丽娟, 博士, 副教授, Email: zhengljuan@stdu.edu.cn。

本课题得到信息安全国家重点实验室开放课题(No. 2021-MS-09); 石家庄铁道大学研究生创新资助项目(No. YC2021074)资助。

收稿日期: 2021-09-28; 修改日期: 2022-01-19; 定稿日期: 2022-11-04

1 引言

随着信息时代的发展,数据已经成为当代社会的重要生产要素之一,通过数据挖掘和提取将会获得大量的有价值的信息资源。尤其是医疗数据信息,医疗机构中保存了患者的身份信息、联系方式、健康数据、诊疗情况、电子保单等敏感信息,这些信息涉及患者个人隐私,需要得到妥善的管理。一旦被恶意利用将会损害患者和医疗机构的利益。此外,医疗机构间存在信息孤岛问题,在患者跨医疗机构就诊时,医生不能全面掌握患者病情。并且医疗信息大多由医疗机构管理,面对众多具有不同需求的访问者,患者无法掌握其医疗数据的使用情况,数据的非法访问时有发生。

访问控制是医疗信息共享中重要的安全机制,不仅可以保障医疗信息免受未经授权的非法用户访问,还可以通过对医疗信息设置访问权限,使医疗信息仅能被拥有对应权限的合法用户访问^[1]。传统的访问控制^[2-3]主要是基于用户身份鉴别来实现的,多用于静态分配权限,数据访问控制粒度粗,灵活性、安全性较差。针对此问题,2005 年, Sahai 和 Wate^[4]提出一种模糊身份加密方案(Fuzzy Identity-based Encryption, FIBE),该方案对用户的身份信息进行了模糊化处理,使用属性因素作为用户的身份标识,提出了属性加密思想,把安全控制细化到数据库的行级或列级,实现了数据的细粒度访问控制。该方案保护了访问者的真实身份信息不被泄露,实现了一对多的数据共享,能够根据访问策略的变化调整数据访问的粒度,具有更好的灵活性。

根据解密策略嵌入在用户的密钥中还是嵌入在密文中,可以分为:基于密钥策略的属性加密机制^[5](key policy attribute-based encryption, KP-ABE)和基于密文策略的属性加密机制^[6](ciphertext policy attribute-based encryption, CP-ABE)。在 CP-ABE 中,数据拥有者可以根据数据共享和访问的实际应用需求,对数据的访问权限进行设置,实现对数据的控制。将其应用于医疗领域,可以解决在患者不知情的情况下发生的医疗数据滥用问题。

Akinyele 等人^[7]提出了一个基于属性加密的个人健康数据信息访问控制方案,用于实现移动设备上的电子医疗记录的隐私保护,使数据拥有者能够细粒度的控制数据的访问和共享。Zhou 等人^[8]提出了一个基于 CP-ABE 的远程医疗诊断方案,患者使用身份属性进行匿名问诊,患者也可以设置医生对自己诊疗记录的访问权限,实现医疗数据隐私的保

护。Zhu 等人^[9]提出了一个基于 CP-ABE 的无线医疗传感网数据共享方案,针对数据请求者含有的不同的属性特征,数据拥有者为其分配相应的访问权限,制定相应的数据访问策略;使用属性时间戳实现数据请求者的属性撤销。Frederic 等人^[10]提出了一个基于 CP-ABE 的密文大小和计算成本恒定的数据访问控制方案,通过用户身份凭据进行判定,当用户身份凭据与加密健康信息携带的凭据相符时,用户才可以解密和访问患者的健康数据。

上述采用属性加密的访问控制方案存在的问题:所有属性的分发和密钥的生成都由唯一的授权机构完成。这样一方面可能会导致系统效率低下,另一方面,对授权机构的可信度要求性较高,一旦该中心不再可信,整个系统的安全性就会丧失。

为解决单一授权的问题,Chase 等人^[11]提出了采用多授权中心管理的访问控制方案,但该方案中引进了中央授权机构,并没有完全实现无中心化。Liu 等人^[12]构建了一个多授权的 CP-ABE 方案,引入多个中央授权机构和多个属性授权机构,由不同的属性授权机构管理不同的属性域,属性授权机构之间彼此独立,并在标准模型下证明了方案的安全性。文献[13-14]通过采用密钥分发和零秘密共享等方法逐渐避免了对中央授权机构的依赖。文献[15]提出了一个适用于移动医疗的多授权的访问控制方案,具有多个独立工作的属性授权机构,并且能够动态增加新的属性授权机构,而不需要重构系统。文献[16]提出了一个具有隐私感知的多授权的 CP-ABE 方案,将用户属性信息隐藏在密文中,用户从多个属性授权机构获得解密密钥,只有满足密文策略的用户才能解密密文,能够对泄露解密密钥的用户进行追踪。Qian 等人^[17]提出了一种个人健康记录隐私保护方案,采用多授权的属性基加密机制对健康数据进行细粒度的访问控制,并且能够实现用户属性撤销和策略更新。许盛伟等人^[18]采用多个属性授权机构共同管理私钥分发,有效防止了用户私钥的泄露,然而文献[17]和文献[18]均基于树形结构制定数据访问策略,访问效率较低。文献[19-22]基于云环境实现多授权数据访问控制,当监管不力或遭遇特定攻击时,数据容易被篡改、泄露或丢失。

此外,上述这些多属性授权方案,虽然可以解决单一授权机构存在的信任问题,但通常其每个属性授权机构之间管理的属性不交叉,对于单个属性在解密授权时并没有完全实现多机构授权,例如属性 $attr_i$ 由且仅由属性授权机构 AA_i 负责管理,属性 $attr_j$ 由且仅由属性授权机构 AA_j 负责管理,如果属性

授权机构 AA_i 出现故障或者遭到腐化, 那么属性 $attr_i$ 将得不到验证, 在解密时同样会产生单点故障问题。并且操作记录难以做到公开透明, 无法对属性授权过程进行追溯问责。

2008 年, 文献[23]提出一种去中心化的新型技术—区块链技术, 顾名思义就是将一个个数据区块以链的方式连接起来, 其去中心化、不可篡改、可追溯、多方共同维护的特点, 突破了传统建立在可信第三方下的信任机制, 使得直接在两个陌生实体间建立信任成为可能, 为数据的安全共享和访问提供了一种新的解决思路。其中, 根据区块链控制权限的开放程度以及应用范围可以将其分为公有链、私有链和联盟链。公有链是对所有人开放的, 任何人都可以作为节点参与到系统中来, 并且可以得到完整的区块链数据信息; 私有链是一种不对外开放的, 只有被许可的节点才能够参与到系统中来, 只适用于特定的机构内部; 联盟链则介于公有链和私有链之间, 既不是完全公开也不是完全私有, 是由多方组织结构共同达成联盟的一种模式, 这些组织机构之间不必彼此信任, 通过准入机制使只有具有合法的证书的节点才能够在区块链系统中进行数据访问或发起交易。因此, 相对于公有链和私有链, 联盟链更适用于行业应用, 主要用于建立多个组织机构间的信任体系。

Hyperledger Fabric^[24]是目前联盟链中常用的一种解决方案, 融合了成员管理服务机制, 由多个组织机构共同参与和管理, 支持拜占庭共识协议^[25]和基于 Kafka 的崩溃容错共识协议^[26], 可以实现快速有效的交易共识, 同时支持多种常规编程语言编写智能合约, 在实际部署和应用时能够更加灵活。

研究者将区块链技术与访问控制结合起来, 实现了数据的分布式存储, 保证了数据不被恶意篡改。Witchey N^[27]提出了一种用于医疗保健交易验证的系统和方法, 把通过验证的设备确认为有效的交易添加在患者医疗保健区块链中。Ariel 等人^[28]提出了一个 MedRec 框架, 将智能合约与访问控制相结合进行自动化的权限管理, 实现了跨医疗机构的数据去中心化整合。Omar 等人^[29]提出了一个以患者为中心的医疗数据管理系统, 利用区块链实现医疗数据的安全存储和共享, 同时使用加密功能来保护患者数据。Zhang 等人^[30]提出了一种基于区块链的体系结构 FHIRChain, 采用 HL7 标准封装需要共享的临床数据, 结合区块链实现医疗数据的共享和访问。Jiang 等人^[31]提出了一个基于区块链的医疗保健信息交换平台 BlocHIE, 使用两个松散耦合的区块链来处理不

同种类的医疗数据。Uchi 等人^[32]提出了一种基于区块链的访问控制生态系统, 赋予了数据所有者自主管理个人数据集的权利。

但是, 上述方案仍然没有解决单一授权问题, 也没有实现细粒度的访问控制。

综上所述, 针对医疗机构间信息共享难, 患者对医疗数据使用情况不知情, 单一授权、用户计算开销大、操作记录难追溯等问题, 本文提出一种基于区块链的医疗信息属性加密访问控制方案, 将属性加密和区块链技术结合起来实现患者医疗数据的高效和安全的访问控制。

本文主要的研究工作如下:

(1) 基于区块链平台, 建立多授权机构, 解决了单一授权问题; 将访问控制权限和响应规则编写成智能合约, 自动完成主体间的通信过程。

(2) 利用区块链透明性、不可篡改性和可追溯性等优势实现了对属性授权机构的追溯问责。

(3) 建立新的访问控制模型: 从属性和时间两个维度控制访问者的访问权限, 实现了患者对医疗信息细粒度的访问控制; 支持直接撤销访问者的属性, 实现了患者对医疗数据的灵活控制; 改进了解密密钥的生成方法, 降低了终端的解密开销, 提高了解密效率。

(4) 对本方案进行了安全性证明, 建立了敌手游戏模型, 证明了该方案在随机预言机模型下是静态安全的。最后通过性能分析与仿真实验分析, 验证了本方案在满足安全性的同时具有较低的计算开销和存储开销。

2 基于区块链的医疗信息属性加密访问控制方案

2.1 系统模型

本模型主要包含六个部分: 医疗数据拥有者、患者、属性授权机构、区块链、分布式文件存储系统 (Interplanetary File System, IPFS) 和访问者, 使用区块链的智能合约技术实现主体间的相互通信。方案的系统模型如图 1 所示:

医疗数据拥有者: 即数据的持有者, 这里指各医疗机构。主要负责审核访问策略并加密上传数据。

患者: 医疗数据的主体, 主要负责制定访问策略并交由各医疗机构的监管部门审查确认, 验证访问者拥有的属性令牌是否符合制定的访问策略。

属性授权机构: 多个属性授权机构共同管理所有属性, 验证访问者属性信息并颁发属性令牌, 生成访问者代理解密密钥和访问者私钥。

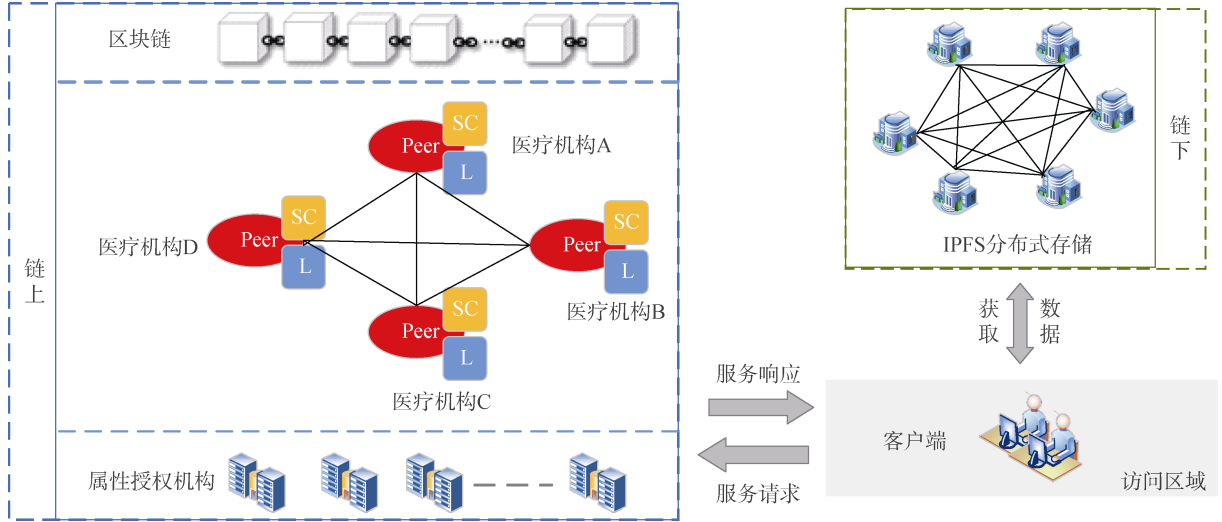


图 1 基于区块链的数据访问控制方案模型

Figure 1 The model of data access control scheme based on blockchain

区块链: 本方案选取联盟链, 联盟成员主要是各医疗机构。主要负责安全地存储加密的 IPFS 路径, 维护代理密钥列表, 管理每个访问者对应的属性代理密钥。访问过程中产生的所有操作记录均存储在区块链中, 透明公开, 可用于追溯和问责。

IPFS 分布式存储网络: 主要负责存储经过加密的患者医疗信息。

访问者: 系统的合法用户, 拥有自己的身份属性集合。访问者发起数据访问请求并在规定的时间内进行访问。

2.2 具体方案

本方案中涉及的医疗信息是患者在某医疗机构就诊期间, 由该医疗机构内的医生创建的患者病历记录。为确保共享医疗信息的真实有效, 只有病历的创建者可以“写”病历, 且一旦数据写入, 就不能被删除或修改。方案的整体流程包括初始化阶段、数据加密阶段、密钥生成阶段、数据访问阶段和访问者撤销阶段。方案的具体流程如图 2 所示。

阶段 1 初始化阶段

(1) 系统初始化 $\text{GlobalSetup}(\lambda) \rightarrow \{\text{GP}\}$

选择参数 λ , 确定一个与之对应的非退化性的双线性对 $e: G \times G \rightarrow G_F$ 。双线性对 e 中的两个乘法循环群 G 和 G_F 的阶均为素数 p , 双线性群 G 的随机生成元为 g 。

定义一个映射函数 $F: \mathcal{U} \rightarrow \mathcal{U}_{aid}$, 其中 \mathcal{U} 代表方案的属性域, \mathcal{U}_{aid} 代表身份标识为 aid 的属性授权机构所管理的属性集合。选择三个安全的哈希函数 $H_1: \{0, 1\}^* \rightarrow G$, $H_2: G_F \rightarrow Z_p^*$ 和 $H_3: \mathcal{U} \rightarrow G$, 一个对称密码算法 $\text{SE}=(\text{SE.Enc}(\cdot), \text{SE.Dec}(\cdot))$, 其中 $\text{SE.Enc}(\cdot)$ 是加密算

法, $\text{SE.Dec}(\cdot)$ 是解密算法。最后, 输出全局公共参数 $\text{GP}=\{p, G, g, e, H_1, H_2, H_3, \mathcal{U}, \mathcal{U}_{aid}, F, \text{SE}\}$ 。

(2) 属性授权机构初始化 $\text{AuthoritySetup}(\text{GP}, aid) \rightarrow \{\text{PK}_{aid}, \text{SK}_{aid}\}$

每个属性授权机构各自执行初始化操作。每个属性授权机构管理一类或几类属性, 不同的属性授权机构管理的属性有交叉部分。例如对于同一类属性, 访问者有奇数个属性授权机构可供选择, 如果其中某个属性授权机构发生故障, 访问者可选择其它管理该类属性的授权机构进行属性验证, 这些属性授权机构之间彼此独立工作, 这样可以避免解密过程中访问者进行属性验证时发生单点失效问题。该算法输入为: 全局公共参数 GP 和属性授权机构的身份标识 aid 。每个属性授权机构在 z_p^* 中随机选取两个元素 A_{aid} 和 B_{aid} , 计算其对应的公钥 $\text{PK}_{aid}=\{e(g, g)^{A_{aid}}, g^{A_{aid}}, g^{B_{aid}}\}$ 和私钥 $\text{SK}_{aid}=\{A_{aid}, B_{aid}\}$ 。

阶段 2 数据加密上链阶段

(3) 制定数据访问策略

由患者对可读的医疗共享信息设置访问策略, 患者制定的访问策略经由医疗机构监管部门审查确认之后, 数据拥有者对共享的医疗信息进行加密处理。

本方案基于线性秘密共享矩阵访问结构, 患者的每一条医疗数据对应一条访问控制策略, 拥有不同属性的访问者对数据的访问权限不同, 能够访问到的数据信息也不同。这里将访问策略用二元组 (W, ρ) 表示: W 是一个具有 l 行 n 列的矩阵, ρ 是一个实现 W 到属性 $\rho(x)$ 映射的函数。函数 $\delta(\cdot)=F(\rho(\cdot))$ 将矩阵的行映射到一个属性授权机构。

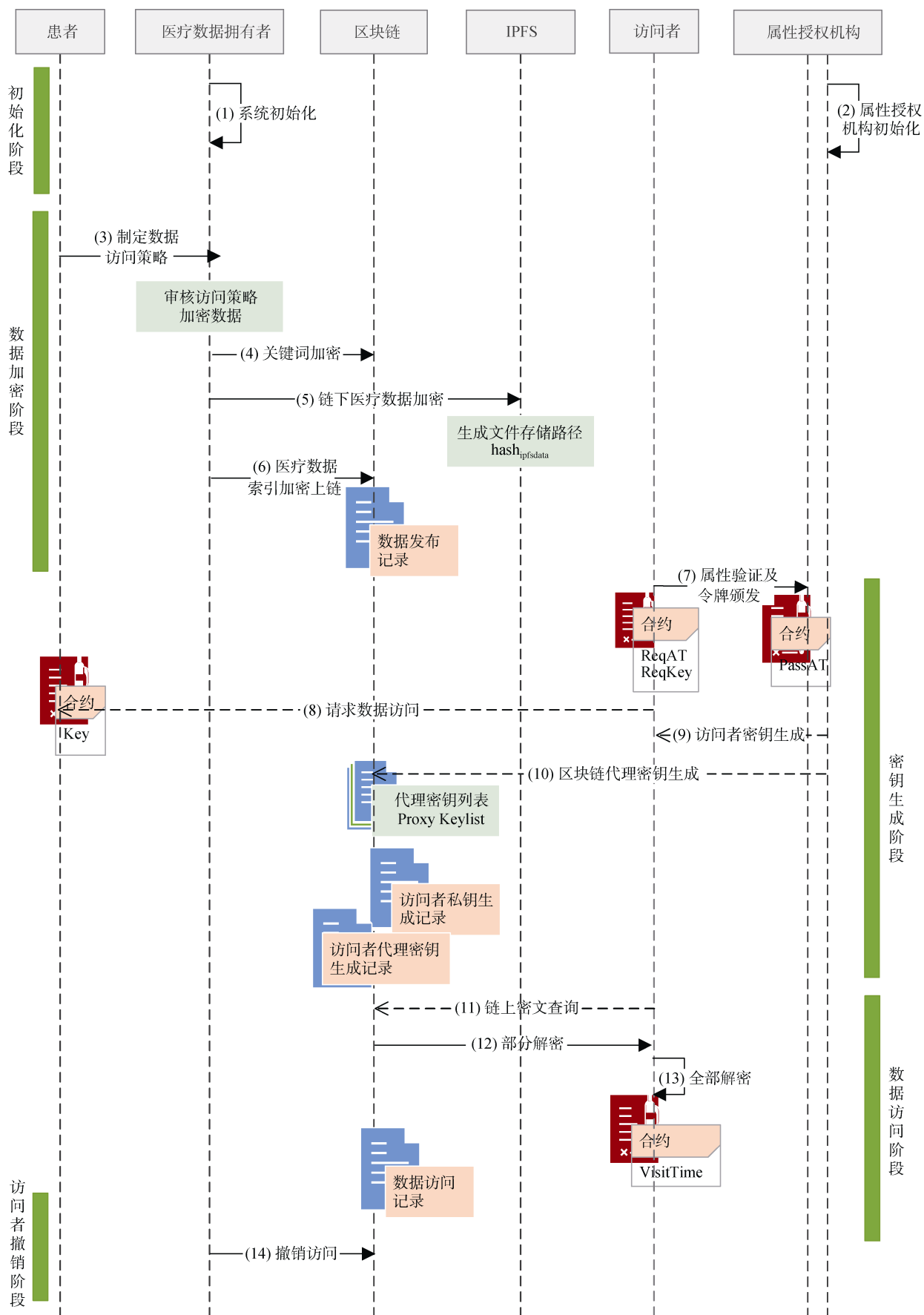


图 2 基于区块链的数据访问控制方案流程

Figure 2 The process of data access control scheme based on blockchain

(4) 关键词加密 $\text{KeywordEncrypt}(\text{PK}_{\text{kw}}, \text{KeyWord}) \rightarrow \text{C}_{\text{kw}}$

在加密数据之前, 数据拥有者随机选择元素 $\theta \in Z_p^*$, 计算私钥 $\text{SK}_{\text{kw}} = \{\theta\}$ 和公钥 $\text{PK}_{\text{kw}} = \{g^\theta\}$, 提取数据的关键词 $\text{KeyWord} = \{0, 1\}^*$, 使用公钥 PK_{kw} 对关键词 KeyWord 加密得到关键词密文 C_{kw} 。

(5) 链下医疗数据加密 $\text{SE.Enc}(\text{M}, \text{key}_{\text{se}}) \rightarrow \text{M}_{\text{se}}$

数据拥有者根据选用的 $\text{SE} = (\text{SE.Enc}(\cdot), \text{SE.Dec}(\cdot))$ 生成一个对称密钥 key_{se} , 然后使用 key_{se} 对数据 M 进行加密, 得到数据密文 M_{se} 。将 M_{se} 存储在 IPFS 网络中, 得到消息检索路径 $\text{hash}_{\text{ipfsdata}}$, 即该条数据 M 的链下存储地址。

(6) 医疗数据索引加密上链 $\text{MEncrypt}(\text{GP}, \text{PK}_{\text{aid}}, \text{key}_{\text{se}}, \text{hash}_{\text{ipfsdata}}, (W, \rho)) \rightarrow \text{CT}$

数据拥有者在对称密钥 key_{se} 和链下存储路径 $\text{hash}_{\text{ipfsdata}}$ 中附上患者为该条数据制定的访问策略。该算法输入为: 全局公共参数 GP 、属性授权机构的公钥 PK_{aid} 、对称密钥 key_{se} 、链下存储地址 $\text{hash}_{\text{ipfsdata}}$ 和访问策略 (W, ρ) 。

首先, 随机选择 $s, y_2, \dots, y_n, z_2, \dots, z_n \in Z_p^*$, 并令向量 $\mathbf{v} = (s, y_2, \dots, y_n)^T$, $\mathbf{w} = (0, z_2, \dots, z_n)^T$ 。然后, 对于所有的 $x \in [l]$, 计算 $\lambda_x = (W\mathbf{v})_x$, $w_x = (W\mathbf{w})_x$, 随机选取 Q_x , R_x , $r_x \in Z_p^*$, 计算 $C_0 = \text{key} * e(g, g)^s$, $C_{1,x} = g^{Q_x} * g^{r_x * A_{\delta(x)}}$, $C_{2,x} = g^{-r_x}$, $C_{3,x} = g^{r_x * B_{\delta(x)}} * g^{R_x}$ 和 $C_{4,x} = H_3(\rho(x))^{r_x}$, $C_{5,x} = \lambda_x - Q_x$, $C_{6,x} = w_x - R_x$ 。计算生成密文 $\text{CT} = ((W, \rho), C_0, \{C_{1,x}, C_{2,x}, C_{3,x}, C_{4,x}, C_{5,x}, C_{6,x}\}_{x \in [l]}, \text{hash}_{\text{ipfsdata}})$, 上传至区块链。同时形成一条区块链交易记录, 该记录主要包括数据 ID、非对称公钥、时间戳、数字签名、关键字密文和加密信息。

阶段 3 密钥生成阶段

(7) 属性验证及令牌颁发

当访问者想要访问共享的医疗信息时, 首先调用合约 ReqAT 中的 $\text{CheckforAT}()$ 函数, 请求属性授权机构对自身的属性进行验证。属性授权机构接收到来自访问者的属性验证请求后, 触发合约 PassAT 中的 $\text{CheckUserAT}()$ 函数, 对访问者的属性进行验证。若经过验证表明访问者的属性是合法有效的, 该属性授权机构调用合约 PassAT 的 $\text{SendUserToken}()$ 函数, 给访问者分配对应的属性令牌。颁发的属性令牌包含该属性授权机构 aid 、访问者身份标识 uid 、时间戳、属性验证信息和失效时间等控制信息。

(8) 请求数据访问

当访问者自身属性全部验证完毕后, 访问者执

行合约 Reqkey , 调用 $\text{CheckforToken}()$ 函数, 向患者请求访问私钥; 患者触发合约 Key 的 $\text{CheckUserToken}()$ 函数, 对访问者的属性集合进行检查, 判断访问者的属性集合 S_{uid} 与访问策略 (W, ρ) 是否匹配, 若匹配, 患者调用合约 Key 的 $\text{SendUserKey}()$ 函数, 访问者获得访问私钥。

(9) 访问者密钥生成 $\text{VisitorKeyGen}(\text{GP}, \text{uid}, S_{\text{uid}}, \text{aid}) \rightarrow \{\text{PK}_{\text{uid}, \text{aid}}, \text{SK}_{\text{uid}, \text{aid}}\}$

各属性授权机构执行访问者公私钥生成算法, 对于所有的属性 $u \in S_{\text{uid}}$, 如果属性 u 被属性授权机构 aid 管理 ($F(u) = \text{aid}$), 则记作 $S_{\text{uid}, \text{aid}}$ 。该算法输入为: 全局公共参数 GP 、访问者身份标识 uid 和 $S_{\text{uid}, \text{aid}}$ 。

属性授权机构 aid 在 Z_p^* 中随机选取元素 $x_{\text{uid}, \text{aid}}$, 计算

公钥 $\text{PK}_{\text{uid}, \text{aid}} = (g^{x_{\text{uid}, \text{aid}}}, H_1(\text{uid})^{x_{\text{uid}, \text{aid}}})$ 以及私钥 $\text{SK}_{\text{uid}, \text{aid}} = 1/x_{\text{uid}, \text{aid}}$, 产生一条访问者私钥生成记录, 该记录

主要包括属性授权机构 aid 、访问者身份标识 uid 、私钥组件编号 id 和私钥生成时间。其中, 为保护访问者属性不被泄露, 使用私钥组件编号 id 对应访问者的某条属性, 用于表示某时刻该属性授权机构为某访问者生成了某部分访问者私钥, 用于后期的追溯问责。

(10) 区块链代理密钥生成 $\text{BCProxyKeyGen}(\text{GP}, \text{uid}, S_{\text{uid}, \text{aid}}, \text{SK}_{\text{aid}}, \text{PK}_{\text{uid}, \text{aid}}) \rightarrow \text{DPxK}_{\text{uid}, \text{aid}}$

各属性授权机构执行区块链代理密钥生成算法, 该算法输入为: 全局公共参数 GP 、访问者身份标识 uid 、访问者的属性集 $S_{\text{uid}, \text{aid}}$ 、相关属性授权机构的私钥 SK_{aid} 及其生成的访问者公钥 $\text{PK}_{\text{uid}, \text{aid}}$ 。对于所有的属性 $u \in S_{\text{uid}, \text{aid}}$, 如果属性 u 被属性授权机构 aid 管理 ($F(u) = \text{aid}$), 则属性授权机构 aid 为访问者 uid 生成相应的代理密钥, 属性授权机构选择随机元素 $f_u \in Z_p^*$, 计算 $\text{DPxK}_{\text{uid}, \text{aid}} = g^{A_{\text{aid}} * x_{\text{uid}, \text{aid}}} * H_1$

$(\text{uid})^{B_{\text{aid}} * x_{\text{uid}, \text{aid}}} * H_3(u)^{f_u}$ 和 $\text{DPxK}'_{\text{uid}, \text{aid}} = g^{f_u}$, 输出该访问者对应的各属性授权机构的代理密钥 $\text{DPxK}_{\text{uid}, \text{aid}}$, 产生一条访问者代理密钥生成记录, 主要包括属性授权机构 aid 、访问者身份标识 uid 、代理密钥组件编号 id 和代理密钥生成时间, 用于表示某时刻该属性授权机构为某访问者生成了某部分区块链代理密钥。区块链缓存节点存储该访问者的区块链代理密钥 $\text{BCPxK}_{\text{uid}} = (\text{DPxK}_{\text{uid}, \text{aid}}, \text{DPxK}'_{\text{uid}, \text{aid}})_{u \in S}$, 并形成一条 $(\text{uid}, \text{BCPxK}_{\text{uid}})$ 的二元组记录, 添加到代理密钥列表 Proxy Keylist 中。

阶段 4 数据访问阶段

(11) 链上密文查询

访问者执行算法 $\text{Trapdoor}(\text{SK}_{\text{kw}}, \text{KeyWord}) \rightarrow \text{T}_{\text{kw}}$,

得到关键词陷门 T_{kw} , 生成查询交易单发送至共识节点, 区块链上共识节点收到查询交易单后, 提取出陷门并执行匹配算法 $\text{Test}(\text{PK}_{kw}, C_{kw}, T_{kw}) \rightarrow j$, 得到结果 j , 若 $j=1$, 则查询成功, 若 $j=0$, 则查询失败。

(12) 部分解密 $\text{PxDecrypt}(\text{GP}, \text{CT}, S_{uid}, \text{BCPxK}_{uid}) \rightarrow \text{CT}'$

当查询到待访问数据且访问者的属性集 S_{uid} 符合患者制定的访问策略 (W, ρ) 时, 令 $I = \{x: \rho(x) \in S_{uid}\} \subseteq \{1, 2, \dots, l\}$, 计算 $c_x \{c_x \in z_p^*\}$ 。区块链缓存节点根据访问者的解密请求, 执行代理解密算法, 输入全局公共参数 GP 、链上密文 CT 、该访问者的代理密钥 BCPxK_{uid} , 计算: $c_{1,uid} = \prod_{x \in I} e(c_{1,x} * g^{C_{5,x}}, g)^{C_x}$ 和 $C_{2,uid} = \prod_{x \in I} (e(\text{BCPxK}_{\rho(x),uid}, C_{2,x})e(H_1(uid)^{x_{uid}}, C_{3,x}g^{C_{6,x}})e(\text{BCPxK}'_{\rho(x),uid}, C_{4,x}))^{C_x} \circ$ 最后将部分解密的密文 $\text{CT}' = (C_0, C_{1,uid}, C_{2,uid}, \text{hash}_{\text{ipfsdata}})$, 发送给相应的访问者 uid 。

(13) 全部解密 $\text{Udecrypt}(\text{CT}', \text{SK}_{uid}) \rightarrow \text{M}$

区块链缓存节点代理解密后, 由访问者自行解密剩余密文获得明文。访问者获得 CT' 后, 使用个人私钥 SK_{uid} 计算 $C_{1,uid} (C_{2,uid})^{1/x_{uid}} = e(g, g)^s$ 。之后计算对称密钥 $\text{key}_{se} = C_0 / e(g, g)^s = \text{key}_{se} * e(g, g)^s / e(g, g)^s$, 其中 $v * (1, 0, \dots, 0) = s$ 和 $w * (1, 0, \dots, 0) = 0$ 。最后, 访问者依据存储路径 $\text{hash}_{\text{ipfsdata}}$ 检索到数据文件, 解密 M_{se} 恢复出明文消息 $\text{M} = \text{SE.Dec}(\text{M}_{se}, \text{key})$ 。在解密过程中同时产生一条数据访问记录, 以用于后期的追溯问责。

阶段5 访问者撤销阶段

访问者解密成功, 开始进行医疗信息访问时, 触发合约 VisitTime , 调用 $\text{CountT}()$ 函数对访问时间进行倒计时。当访问者的访问时间结束, 或者访问者的属性令牌到期时, 将执行访问者撤销指令。

(14) 撤销访问 $\text{Revoke}(uid, \text{Proxy Keylist}) \rightarrow \text{Proxy Keylist} \setminus \{uid, \text{BCPxK}_{uid}\}$

当需要撤销访问时, 数据拥有者只需要给区块链缓存节点发布一条包含访问者身份标识 uid 的撤销命令, 区块链缓存节点更新代理密钥列表 Proxy Keylist , 输出更新后的密钥列表 $\text{Proxy Keylist} \setminus \{uid, \text{BCPxK}_{uid}\}$, 该访问者的原代理密钥失效。

以上为本方案的访问控制整体流程。本方案提出的访问控制模型是基于区块链平台的, 访问过程中发生的数据发布、属性授权、密钥生成以及数据访问等操作记录均存储在区块链中, 并且每条记录与各主体的身份标识 ID 相互绑定, 操作记录公开透明。

对于数据拥有者, 在完成整个数据发布的过程中生成的数据发布记录会被保存在区块链上; 对于访问者, 当进行数据访问操作时, 产生的数据访问

记录会被保存在区块链上; 对于属性授权机构, 访问授权过程中的操作, 也会形成操作记录被上传至区块链保存, 并且每条操作记录都与相应的属性授权机构的身份标识相互绑定。因此, 当需要进行审计或问责时, 区块链不可篡改、可追溯的特性保证了数据访问过程有迹可循。

2.3 实例分析

以医疗行业中各医疗机构之间的数据交互作为实例进行分析。各医疗机构位于不同的地理位置, 相互之间存在协作关系, 各医疗机构之间需要进行频繁的数据共享和信息访问。然而每个医疗机构存储的医疗数据包含患者的敏感信息, 无法做到完全开放, 因此各医疗机构需要根据实际情况与患者的安全需求制定访问策略。基于上述场景本模型的应用具体如下:

首先系统进行初始化, 实施身份认证获得唯一的身份标识符。例如患者 Alice 身份标识为 $\text{identity}_{\text{Alice}}$, 访问者 Bob 身份标识为 $\text{identity}_{\text{Bob}}$, 假设有 10 个属性授权机构, 分别记为 $\text{AA}_{i(1 \leq i \leq 10)}$, 每个属性授权机构管理 2 类属性, 一个属性授权机构每次只能为同一用户验证一类属性, 若其中某一属性授权机构出现故障或安全问题, 访问者可选择其他管理同类属性的属性授权机构进行验证, 避免验证过程中发生单点失效的情况。

在医疗行业中, 每个医疗机构对实体的描述都基本相似, 因此在本系统中, 各医疗机构共同协商对实体属性的描述标准, 使用 $\{\langle \text{identity}_{uid}, \text{data}_i \rangle, \langle \text{attribute set} \rangle, \langle \text{visit time} \rangle\}$ 对访问策略进行描述, 其中 identity_{uid} 表示数据拥有者身份, data_i 表示数据片段, attribute set 表示访问该数据片段所需要的属性集合, visit time 表示访问执行时间, 患者可从访问者身份属性以及访问时间两个维度控制其医疗共享数据的访问。

首先患者 Alice 制定一条健康体检记录的访问策略 $\text{EMR}_{15}(\langle \text{identity}_{\text{Alice}}, \text{seq}_{15} \rangle, \langle \text{archiater}, \text{PhD student}, \text{cardiologist} \rangle, \langle t_{\text{start}}, t_{\text{end}} \rangle)$, 接下来, Alice 将该策略发送给相应医疗机构 A 的监管部门进行审核, 监管部门审核通过后, 提取出该健康体检记录的关键词 $\text{Keyword}_{\text{Alice}} = \{\text{identity}_{\text{Alice}}, \text{medical examination report}, 20210910\}$, 使用 PK_{kw} 加密该健康体检记录的关键词, 获得关键词密文 $C_{kw-A} = E_{\text{PK}_{kw}}(\text{Keyword}_{\text{Alice}})$; 然后使用对称密钥 $\text{key}_{\text{Alice-15}}$ 加密 Alice 的健康体检记录 $\text{M}_{A-\text{mer-2021091015}} = E_{\text{key}_{\text{Alice-15}}}(\text{medical examination report})$, 保存至 IPFS 分布式存储网络中, 并获得 IPFS 存储路径哈希值

$\text{hash}_{\text{ipfsdata}} = \text{"E0789A1498A220A D828E54A5491BF 8D6"}.$ 接下来使用基于密文策略的属性加密算法加密链下存储路径 $\text{hash}_{\text{ipfsdata}}$ 和对称密钥 $\text{key}_{\text{Alice-15}}$ 获得链上密钥密文 $\text{CT}_{\text{A-mer-2021091015}}$, 同时形成一条区块链交易记录 $\{\text{ID}_{\text{data}}, \text{PK}_{\text{kw}}, 20210911, \text{identity}_{\text{Alice}}, \text{C}_{\text{kw-A}}, \text{CT}_{\text{A-mer-2021091015}}\}.$

假设 $\text{Bob} = [\text{archiater}, \text{PhD student}, \text{cardiologist}, \text{male}]$ 想访问医疗机构 A 中患者 Alice 的健康体检记录, Bob 在客户端选择相应的属性授权机构验证自己的属性: 例如 Bob 可从属性授权机构 AA_1 验证职称属性 $= [\text{住院医师}, \text{主治医师}, \text{副主任医师}, \text{主任医师}, \dots]$, 从 AA_2 验证学位属性 $= [\text{博士研究生}, \text{硕士研究生}, \text{学士}, \dots]$, 从 AA_3 验证科室属性 $= [\text{心内科}, \text{呼吸内科}, \text{神经内科}, \dots]$, 从 AA_4 验证性别属性 $= [\text{男性}, \text{女性}].$ Bob 的 4 个属性验证完毕后, 分别获得 4 个属性令牌 $= [\text{access_token}, \text{token_type}, \text{expires_in}, \text{scope}, \text{others}],$ 患者检验其职称、学位、职位和性别属性是否符合访问策略, 如果符合, 负责验证 Bob 属性的授权机构生成相应的私钥构件 $\text{SK}_{\text{Bob}, \text{AA}_i (1 \leq i \leq 4)}$ 和代理解密密钥构件 $\text{DPxK}_{\text{Bob}, \text{AA}_i (1 \leq i \leq 4)},$ 最终组合成 Bob 的私钥 SK_{Bob} 及其区块链上代理密钥 $\text{BCPxK}_{\text{Bob}},$ 分别交由 Bob 和区块链上缓存节点保存, 并在链上产生一条 $(\text{Bob}, \text{BCPxK}_{\text{Bob}})$ 的二元组记录。

Bob 使用 SK_{kw} 生成陷门 $\text{T}_{\text{kw}} = \{\text{SK}_{\text{kw}}, \text{identity}_{\text{Alice}}, \text{medical examination report}, 20210910\},$ 链上节点进行查找, 匹配后给 Bob 返回经部分解密的密钥密文 $\text{CT}'_{\text{A-mer-2021091015}},$ 接着 Bob 使用私钥继续解密得到对称密钥及数据密文路径, 最终获得 Alice 的健康体检记录。

当 Bob 的属性令牌到期失效、Bob 的数据访问时间超出规定的访问时间限制, 或者由于其他特殊原因需要将 Bob 的访问进行撤销时, 负责发布该条健康体检记录的医疗机构 A 将会向区块链缓存节点发送撤销命令。区块链缓存节点收到撤销命令之后, 更新代理密钥列表, 添加一条带有标签的列表记录 $(\text{Bob}, \text{BCPxK}_{\text{Bob}}, \text{tag}=1),$ 标签 $\text{tag}=1$ 说明该用户已被撤销, 其代理密钥失效。区块链缓存节点无法根据已失效的代理密钥 $\text{BCPxK}_{\text{Bob}}$ 对链上密钥密文进行预解密, Bob 不能继续解密获得明文, Bob 的允许访问时间归零, 无法进行后续的数据访问。

综上所述, 本文提出的基于区块链的医疗信息属性加密访问控制方案能够适应医疗领域内各机构间数据共享和访问的应用场景, 能够保证患者隐私数据的安全可控。

3 安全性证明

3.1 构建安全模型

敌手必须在进入挑战之前完成所有的询问。同时, 敌手可以多次向访问者询问其私钥。如果敌手能够向区块链缓存节点询问代理密钥, 那么敌手也能够获得访问者对应的部分解密密文。同时, 敌手能够为腐化的属性授权机构生成公钥。在游戏中, 假设一个属性授权机构仅可以管理一类属性。

系统初始化: 挑战者根据安全需求输入参数 $\lambda,$ 调用算法 $\text{GlobalSetup}(\lambda) \rightarrow \{\text{GP}\},$ 将输出的全局公共参数 GP 返回给敌手, 完成系统初始化。

询问: 已知属性域 U 和属性授权机构的全局唯一身份标识 $\text{aid},$ 符号 C_{aid} 表示腐化的属性授权机构, $\text{C}_{\text{aid}} \subseteq U_{\text{aid}},$ 符号 N_{aid} 表示未被腐化的属性授权机构, $\text{N}_{\text{aid}} \subseteq U_{\text{aid}}.$ 敌手开始向挑战者发出询问:

(1) 敌手向挑战者询问未被腐化的属性授权机构 N_{aid} 的公钥 $\text{PK}_{\text{aid}}.$

(2) 敌手向挑战者询问部分合法访问者的私钥 $\text{SK}_{\text{uid}}.$

(3) 敌手向挑战者询问区块链代理密钥 $\text{BCPxK}_{\text{uid}}:$ 输入部分访问者的全局身份标识 uid 和访问者的属性集合 $\text{S}_{\text{uid}} (\text{S}_{\text{uid}} \subseteq U \text{ 且 } \text{S}_{\text{uid}} \not\subseteq \text{C}_{\text{aid}}).$ 这里输入的访问者不仅仅是指在上一次询问中被提及的访问者, 也指在这一次询问中, 被问及区块链上代理密钥的其他访问者。挑战者调用算法 $\text{BCProxyKeyGen}(\text{GP}, \text{uid}, \text{S}_{\text{uid}}, \text{aid}, \text{SK}_{\text{aid}}, \text{PK}_{\text{uid}}, \text{aid}) \rightarrow \text{DPxK}_{\text{uid}, \text{aid}},$ 将输出的区块链代理密钥 $\text{BCPxK}_{\text{uid}}$ 返回给敌手。

挑战: 敌手把两个长度相等的明文 M_1 和 M_2 以及访问策略 (W, ρ) 提交给挑战者, 挑战者随机选取 $b \in \{0, 1\},$ 调用加密算法 $\text{Encrypt}(\text{GP}, \text{PK}_{\text{aid}}, \text{M}, (W, \rho)) \rightarrow \text{CT},$ 将输出的挑战密文 CT 返回给敌手。其中, 曾被询问私钥的访问者的属性集合 $\text{S}_{\text{C}_{\text{aid}}} \cup \text{S}_{\text{uid}}$ 不能再次与访问策略 (W, ρ) 匹配。

猜测: 敌手对挑战者在挑战阶段随机选取的 b 值进行猜测, 若敌手猜测值 b' 与挑战者选取值 b 相同, 即 $b=b',$ 则敌手猜测成功, 取得游戏胜利。

在游戏中, 敌手获得胜利的优势定义为 $|\text{Pr}[b=b'] - \frac{1}{2}|.$

定义 1 给定一个多项式时间, 如果敌手无法在多项式时间内以不可忽略的优势取得该游戏的胜利, 那么该方案在随机预言机模型^[33] (Random Oracle Model, ROM) 下是静态安全的。

3.2 静态性安全证明

为了证明方案的安全性, 将其安全性规约到求解离散对数的数学困难问题上, 如果敌手求解该数学困难问题的优势在一个多项式时间内是可以被忽略掉的, 则方案的安全性得证。

定义 2 q-DBPBDHE2 假设问题。

根据安全参数, 选择两个阶都为素数 p 的乘法循环群 G 和 G_F , 两个群满足映射关系 $e: G \times G \rightarrow G_F$ 。随机选取 $a, s, b_1, \dots, b_q \in \mathbb{Z}_p^*$, $R \in G_F$, 已知向量 $D: (p, g, G, e, g^s, \{g^{a^i}\}_{i \in [2q], i \neq q+1}, \{g^{b_j a^i}\}_{(i,j) \in [2q, q], i \neq q+1}, \{g^{s/b_i}\}_{i \in [q]}, \{g^{s b_j a^i / b_j}\}_{(i,j,j') \in [q+1, q, q], j \neq j'})$ 。假设存在算法 A

用来区分 $e(g, g)^{a^{q+1}s}$ 和 $R (R \in G_F)$, 当 $|\Pr[A(D, e(g, g)^{a^{q+1}s})=0] - \Pr[A(D, R)=0]| \geq \varepsilon$, 则称算法 A 解决 q-DBPBDHE2 问题的优势是 ε 。

若在概率多项式时间内, 敌手不能以一个不可忽略的优势 ε 区分 $e(g, g)^{a^{q+1}s}$ 和 $R (R \in G_F)$, 那么 q-DBPBDHE2 的假设成立。

定理 1 如果上述 q-DBPBDHE2 的假设问题成立, 则所提方案在随机预言模型下是静态安全的。

引理 1 如果上述 q-DBPBDHE2 的假设问题成立, 则文献[34]所提的 RW 方案在随机预言模型下是静态安全的。

引理 2 如果文献[34]所提的 RW 方案在随机预言机模型下是静态安全的, 那么本文提出的方案在随机预言模型下也是静态安全的。

若引理 1、2 可被证明成立, 定理 1 自然得证。而引理 1 在文献[34]中已被证明成立, 则下面将对引理 2 进行论证。

证明: 假设存在这样一个多项式时间, 敌手能够在这段时间内以不可忽略的优势成功攻破本文方案, 那么一定存在一个模拟者, 这个模拟者也能以相同的优势攻破 RW 方案, 并借助敌手和 RW 方案中的挑战者攻破本方案。根据构建的安全模型, 安全游戏的详细过程为:

系统初始化: 模拟者利用挑战者给出的 RW 方案的公共参数 $GP=(G, p, g, H_1, H_3, U, U_\theta, T)$, 调用本方案的 $GlobalSetup(\lambda) \rightarrow \{GP\}$ 算法, 将更新后的全局公共参数 GP 返回给敌手。

询问: 已知 U 表示属性域, aid 表示属性授权机构的全局唯一身份标识, C_{aid} 表示腐化的属性授权机构 ($C_{aid} \subseteq U_{aid}$), N_{aid} 表示未被腐化的属性授权机构

($N_{aid} \subseteq U_{aid}$)。其中 $C_{aid} \cup N_{aid} = U_{aid}$, $C_{aid} \cap N_{aid} = \emptyset$ 。敌手向模拟者发出询问:

(1) 敌手向模拟者询问未被腐化的属性授权机构 N_{aid} 的公钥 PK_{aid} 。模拟者将此询问传递给挑战者, 挑战者调用 RW 方案的 $AuthoritySetup(GP, \theta) \rightarrow \{PK_\theta, SK_\theta\}$ 算法, 计算出公钥 $PK_\theta = \{e(g, g)^{\alpha_\theta}, g^{y_\theta}\}$ 并返回给模拟者。接下来模拟者调用本方案的 $AuthoritySetup(GP, aid) \rightarrow \{PK_{aid}, SK_{aid}\}$ 算法输出 $PK_{aid} = \{e(g, g)^{A_{aid}}, g^{A_{aid}}, g^{B_{aid}}\}$, 最后将更新后的公钥 PK_{aid} 返回给敌手。

(2) 敌手向模拟者询问部分合法访问者的私钥 SK_{uid} 。模拟者调用算法 $VisitorKeyGen(GP, uid, S_{uid}, aid) \rightarrow \{PK_{uid, aid}, SK_{uid, aid}\}$, 计算私钥 $SK_{uid, aid} = 1/x_{uid, aid}$, 将整合输出的私钥 SK_{uid} 返回给敌手。

(3) 敌手向模拟者询问区块链代理密钥 $BCPxK_{uid}$ 。模拟者将敌手的询问发送给挑战者, 挑战者调用 RW 方案中的算法, 得到输出结果。敌手输入访问者的全局身份标识 uid 及其属性集合 S_{uid} , 由于敌手可以控制受腐化的属性授权机构所管理的属性, 因此输入的访问者属性集合不能是被腐化的属性授权机构所管理的属性, 即 $S_{uid} \subseteq U$ 且 $S_{uid} \not\subseteq U_{C_{aid}}$ 。接下来模拟者调用算法 $BCProxyKeyGen(GP, uid, S_{uid}, aid, SK_{aid}, PK_{uid, aid}) \rightarrow DPxK_{uid, aid}$, 将输出的区块链代理密钥 $BCPxK_{uid}$ 返回给敌手。另外, 这里输入的访问者不仅仅是指在上一次询问中被提及的访问者, 也指在这一次询问中, 被问及区块链上代理密钥的其他访问者, 因此, 在本次询问中, 模拟者需要根据以下两种情况分别计算对应的区块链代理密钥:

a) 如果在第三次询问中被要求输入全局身份标识的访问者也在第二次询问中被询问私钥, 模拟者在整数群 \mathbb{Z}_p^* 中随机选取元素 $f_k (k \in S_{uid})$, 计算 $DPxK_{uid, aid} = (g^{A_{aid}} H_1(uid)^{B_{aid}} H_3(k)^{f_k})^{x_{uid, aid}} = g^{A_{aid} * x_{uid, aid}} * H_1(uid)^{B_{aid} * x_{uid, aid}} * H_3(k)^{f_k * x_{uid, aid}}$ 和 $DPxK'_{uid, aid} = (H_3(k)^{f_k})^{x_{uid, aid}} = H_3(k)^{f_k * x_{uid, aid}}$, 得到访问者区块链上代理密钥 $BCPxK_{uid} = (DPxK_{uid, aid}, DPxK'_{uid, aid})_{k \in S}$ 。

b) 如果在第三次询问中被要求输入全局身份标识的访问者不是曾被询问过的访问者时, 模拟者分别在循环群 G 和整数群 \mathbb{Z}_p^* 中随机选取元素 g_k 和 $f_k (k \in S_{uid})$, 计算 $DPxK_{uid, aid} = g_k H_3(k)^{f_k} g_k$ 和 $DPxK'_{uid, aid} = H_3(k)^{f_k}$ 。由于循环群 G 中有 $g^{A_{aid}} * H_1(uid)^{B_{aid}}$, 因

此一定存在随机元素 $x_{uid, aid} \in Z_p^*$, 满足 $g_k = (g^{A_{aid}} * H_1(uid)^{B_{aid}})^{x_{uid, aid}} = g^{A_{aid} * x_{uid, aid}} * H_1(uid)^{B_{aid} * x_{uid, aid}}$, 进而可得对应区块链上代理密钥, 计算 $DPxK_{uid, aid} = g_k H_3(k)^{f_k} g_k = g^{A_{aid} * x_{uid, aid}} * H_1(uid)^{B_{aid} * x_{uid, aid}} * H_3(k)^{f_k}$, $DPxK'_{uid, aid} = H_3(k)^{f_k}$ 。然后将 $BCPxK_{uid} = (DPxK_{uid, aid}, DPxK'_{uid, aid})_{k \in S}$ 返回给敌手。

挑战: 敌手把两个长度相等的明文 M_1 和 M_2 以及访问策略 (W, ρ) 提交给模拟者, 模拟者随机选取 $b \in \{0, 1\}$, 调用加密算法 $Encrypt(GP, PK_{aid}, M, (W, \rho)) \rightarrow CT$, 将输出的挑战密文 CT 返回给敌手。其中, 在第二次的询问中曾被询问私钥的访问者的属性集合 $S_{C_{aid}} \cup S_{uid}$ 不能再次与访问策略 (W, ρ) 匹配。

猜测: 模拟者根据敌手给出的不同的 b' 值 ($b' \in \{0, 1\}$), 输出不同的猜测值 b' 。

在整个游戏过程中, 模拟者充当了本方案的挑战者, 挑战者返回的区块链代理密钥对应于在 RW 方案中调用 $UserKeyGen$ 算法输出的用户私钥。模拟者根据 b' 值确定本方案在执行加密算法时用到的对称密钥, 可以对应为在 RW 方案中调用 $Encrypt$ 算法时需要输入的消息 M 。因为文献[34]所提的 RW 方案在随机预言机模型下是静态安全的, 所以本文提出的方案在随机预言机模型下也具有静态安全性。至此, 可得引理 2 成立, 定理 1 得证。

综上所述, 本方案能够抵抗多个合法用户的联

合攻击, 在随机预言机模型下是静态安全的。

4 性能分析

4.1 功能分析

本方案与文献[20]、文献[21]、文献[35]和文献[36]中方案的功能对比在功能上的对比如表 1 所示。

与本方案一样, 文献[20]、文献[21]、文献[35]和文献[36]都支持多个属性授权机构, 并且能够实现细粒度的数据访问控制。文献[20]、文献[35]和文献[36]不是在素数阶群下构建的, 并且不支持大属性域, 在这些方案中属性空间的大小受到制约, 影响了系统的可扩展性和实际应用效果。文献[21]虽然是在素数阶群下构造的且支持大属性域, 但却不支持代理解密, 这样会给用户带来相对较多的计算压力。文献[20]、文献[21]和文献[36]不支持追踪溯源, 当出现问题时不能明确责任方。文献[35]虽然能够进行追踪溯源, 但该方案是在合数阶群下构造的, 效率较低, 并且该方案不具备属性撤销的能力, 存在一定的安全隐患。另外, 与本方案相比, 文献[20]、文献[21]、文献[35]和文献[36]在实现多授权的同时引进了中央机构, 没有实现完全的去中心化, 仍然存在信任问题。

4.2 安全性分析

本方案与文献[20]、文献[21]、文献[35]和文献[36]中方案的安全性比较如表 2 所示。

表 1 功能对比分析

Table 1 Comparative analysis of functions

方案	素数阶群	多机构	中央机构	大属性域	属性撤销	代理解密	可追溯
文献[20]	否	是	是	否	是	是	否
文献[21]	是	是	是	是	是	否	否
文献[35]	否	是	是	否	否	否	是
文献[36]	否	是	是	否	是	是	否
本方案	是	是	否	是	是	是	是

表 2 安全性对比分析

Table 2 Security comparative analysis

方案	匿名性	前向安全性	抗用户合谋攻击	抗平台合谋攻击	不可抵赖性
文献[20]	是	是	是	否	否
文献[21]	是	是	是	否	否
文献[35]	是	否	是	否	是
文献[36]	是	是	是	否	否
本方案	是	是	是	是	是

如表 2 所示, 文献[20]、文献[21]、文献[35]和文献[36]的方案中均使用用户属性代替用户身份, 具有一定的匿名性, 可以抵抗用户的合谋攻击, 但这些方案都没考虑平台的合谋攻击。本方案采用区块链平台, 在多个节点间都保存了相同的数据副本, 并且按照共识机制保证节点间数据的一致性, 使得攻击者无法直接篡改所有的账本, 必须控制平台中超过半数的节点才可能实现链上记录的非法篡改, 因此能够抵抗平台的合谋攻击。同时, 文献[35]无法实现访问者属性撤销, 已经失去访问资格的访问者能够使用其此前的属性私钥解密后续数据, 不具有良好的前向安全性。文献[20]、文献[21]和文献[36]不具备不可抵赖性, 不能确保每一次交易在事后都能够被证实, 不便于日后的审计问责, 在应用中会存在一定的安全问题。本方案在访问过程中产生的所有交易记录都会被存储在区块链中, 每条记录都与各主体的身份标识 ID 相互绑定, 因此各主体无法对自己已经产生的操作进行抵赖。

4.3 计算开销

方案中的各个符号及其含义如表 3 所示。

表 3 符号及其含义

Table 3 Symbols and meanings

符号	含义
$ U $	属性域
$ F_{all} $	属性授权机构的数量
$ S_{uid} $	访问者属性数量
l	访问策略属性数量
$ F_{encry} $	参与加密的属性授权机构数量
$ l $	参与解密的属性数量
P	双线性对运算
E	指数运算

本方案与文献[20]、文献[21]、文献[35]和文献[36]方案中的计算开销对比如表 4 所示。

由于系统中属性授权机构的数量 $|F_{all}| < |U|$, 因此在初始化阶段, 本方案的计算开销小于文献[20]、文献[35]和文献[36]。在密钥生成阶段, 本方案的计算开销与文献[20]、文献[35]中的方案的计算开销相同, 比文献[36]中方案多两次指数运算, 当参与运算的属性授权机构较少时, 与文献[21]中方案的计算开销相差不大。

在加密与解密阶段, 文献[21]和文献[35]中的方案没有实现代理解密, 计算开销较大, 本方案和文献[20]和[36]中方案实施了代理解密策略, 本方案中将部分解密操作交给区块链缓存节点去完成, 区块链缓存节点通过访问者代理密钥能够对密文进行预解密, 因而其产生的解密开销要小于文献[21]和文献[35]。

最后, 从总体的计算开销看, 由于本方案在数据加密和解密阶段具有的较大优势: 在对医疗数据加密时, 采用了对称密码算法, 加解密速度快, 并且在解密时, 访问者只需要对对称密钥进行解密, 具有常量的计算开销, 因此本方案的计算开销从总体上优于其他方案。

4.4 存储开销

本方案与文献[20]、文献[21]、文献[35]和文献[36]方案中访问者产生的存储开销对比如表 5 所示。其中 $|SE_{CT}|$ 表示对称加密后数据密文的长度, $|G_{length}|$ 表示循环群 G 的长度, $|G_{Flength}|$ 表示循环群 G_F 的长度, $|Z_p|$ 表示整数群 Z_p 的长度。

从表 5 可以看出, 在私钥的存储开销上, 本方案的私钥存储开销仅与整数群 Z_p 的长度有关, 恒为常量, 明显优于其他方案; 在密文的存储开销上, 本方案先采用对称加密算法加密数据, 再采用属性基加

表 4 计算开销对比分析

Table 4 Comparative analysis of computational expenses

方案	初始化	加密	密钥生成	解密	总计
文献[20]	$(U + F_{all})E+ F_{all} P$	$(3l+ F_{encry} +1)E$	$(2 F_{encry} + S_{uid} +2)E$	E	$(U + F_{all} +3 F_{encry} + S_{uid} +3l+4)E+ F_{all} P$
文献[21]	$(F_{all} +2)E+ F_{all} P$	$(3l+ F_{encry} +1)E+ F_{encry} P$	$(F_{encry} + S_{uid} +4)E$	$(l+ F_{encry} +2)E$	$(F_{all} +3 F_{encry} + S_{uid} +4l+9)E+(F_{encry} + F_{all})P$
文献[35]	$(U + F_{all} +1)E+ F_{all} P$	$(3l+2 F_{encry} +1)E$	$(2 F_{encry} + S_{uid} +2)E$	$(l +2)E+(2 l +1)P$	$(U + F_{all} +4 F_{encry} + S_{uid} + l +3l+6)E+(F_{all} +2 l +1)P$
文献[36]	$(U +2 F_{all} +2)E+ F_{all} P$	$(3l+ F_{encry} +1)E+ F_{encry} P$	$(2 F_{encry} + S_{uid})E$	E	$(U +2 F_{all} +3 F_{encry} + S_{uid} +3l+4)E+(F_{all} + F_{encry})P$
本方案	$2 F_{all} E+ F_{all} P$	$(3l+2 F_{encry} +1)E$	$(2 F_{encry} + S_{uid} +2)E$	E	$(2 F_{all} +4 F_{encry} + S_{uid} +3l+4)E+ F_{all} P$

表 5 存储开销对比分析

Table 5 Comparative analysis of storage overhead

方案	私钥	密文
文献[20]	$(S_{uid} + F_{encry} +2) G_{length} + Z_p $	$2 G_{Flength} + SE_{CT} $
文献[21]	$(2 F_{encry} +2) G_{length} $	$ F_{encry} G_{Flength} +(2l+1) G_{length} $
文献[35]	$(S_{uid} + F_{encry} +4) G_{length} +4 Z_p $	$3 G_{Flength} + SE_{CT} $
文献[36]	$(2 F_{encry} +2) G_{length} $	$ F_{encry} G_{Flength} +(2l+1) G_{length} $
本方案	$ Z_p $	$3 G_{Flength} + SE_{CT} $

密算法对对称密钥和链下地址信息进行加密, 其密文存储开销不随参与加密的属性授权机构数量和访问策略属性数量的增加而增加, 循环群 G 和 G_F 的长度不变, 因此优于文献[21]和文献[36], 与文献[35]密文存储开销相同, 与文献[20]相比, 密文存储开销略高。从总的存储开销来看, 本方案优于其他方案。

4.5 仿真实验

本文基于 charm 框架, 在虚拟机 Ubuntu 16 中进行仿真实验, 区块链采用 HyperLedger Fabric 开源框架, 计算机配置为 Intel(R) Core(TM) i5-4210 CPU, 2.90GHz 主频, 12GB 内存, 64 位操作系统。在实验仿真过程中, 假设访问者属性始终符合访问策略。令属性授权机构的数量为 20, 每个属性授权机构管理的属性数量为 10。

在计算开销方面, 首先设置自变量为访问者属性数量 $|S_{uid}|$, 固定访问策略属性数量 l 的值为 200。随着 $|S_{uid}|$ 的增加, 文献[21]、文献[35]和文献[36]中参与加密的属性授权机构数量 $|F_{encry}|$ 和参与解密的属性数量 l 也在增加, 产生了大量的双线性对运算, 并且计算开销与访问者属性数量 $|S_{uid}|$ 呈线性相关, 而文献[20]和本方案中, 主要增加了指数运算, 计算开销受影响较少。因此如图 3 所示, 随着访问者属性数量 $|S_{uid}|$ 的增加, 本方案与文献[20]的计算开销基本相同, 而文献[21]、文献[35]和文献[36]的增长幅度远大于本方案。由此在访问策略属性数量 l 不变的情况下, 本方案产生的计算开销最小。

再设置自变量为访问策略属性数量 l , 固定访问者属性数量 $|S_{uid}|$ 的值为 10。如图 4 所示, 随着访问策略属性数量 l 的增加, 各方案的计算开销呈缓慢增长趋势, 文献[21]、文献[35]和文献[36]的计算开销都大于 300ms, 文献[20]的计算开销略高于本方案的计算开销, 都在 250ms 以下。因此在访问者属性数量 $|S_{uid}|$ 不变的情况下, 本方案产生的计算开销最小。

令 $l=|S_{uid}|+100$, 如图 5 所示, 随着访问策略属性数量 l 和访问者属性数量 $|S_{uid}|$ 的增加, 文献[21]、文献[35]和文献[36]需要的双线性对运算量明显增多, 导致这三种方案的计算开销明显增大。由于本方案

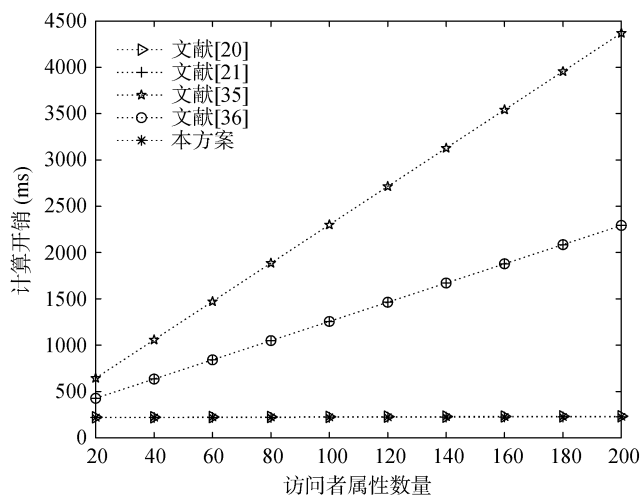


图 3 访问策略属性数量固定时计算开销对比

Figure 3 Comparison of calculation overhead for fixed strategy attributes

和文献[20]双线性对的运算量不受 l 和 $|S_{uid}|$ 变化的影响, l 和 $|S_{uid}|$ 的增加仅会导致指数运算量有所增长, 增加的计算开销较小, 因此两个方案的计算开销基本保持持平。因此从总体来看, 本方案的总计算开销优于其他方案。

在存储开销方面, 同计算开销相同, 令 $l=|S_{uid}|+100$, 经对称加密后得到的对称密文长度 $|SE_{CT}| \cdot |G_F| = 256\text{bits}$ 。文献[21]和文献[36]中存储开销与 G 和 G_F 中元素的长度 $|G_{length}|$ 和 $|G_{Flength}|$ 线性相关, 随着访问策略属性数量 l 和访问者属性数量 $|S_{uid}|$ 的增加, $|G_{length}|$ 和 $|G_{Flength}|$ 也呈线性增长趋势, 因此存储开销也是线性增长的。文献[20]和文献[35]存储开销与 G 中元素的长度 $|G_{length}|$ 线性相关, 因此存储开销的值要低于文献[21]和文献[36]。本方案的存储开销与访问策略属性数量 l 和访问者属性数量 $|S_{uid}|$ 的变化无关, 因此仿真实验中总存储开销恒为常量。图 6 所示为上述方案总存储开销的对比, 可以看出本方案的总存储开销优于其他方案。

5 结论

医疗机构间的信息共享有利于医疗领域的协同

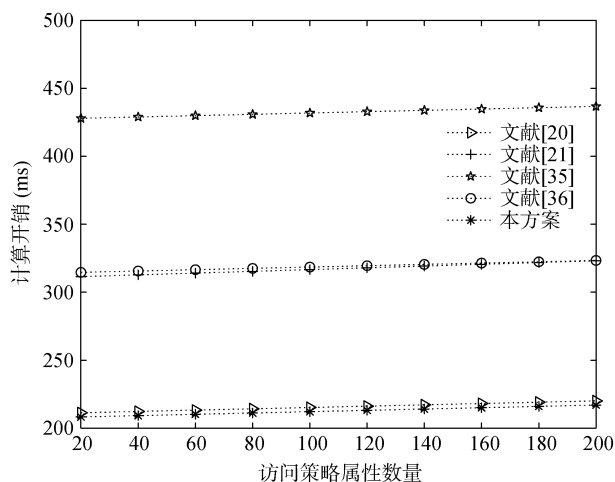


图4 访问者属性数量固定时计算开销对比

Figure 4 Comparison of calculation overhead for fixed user attributes

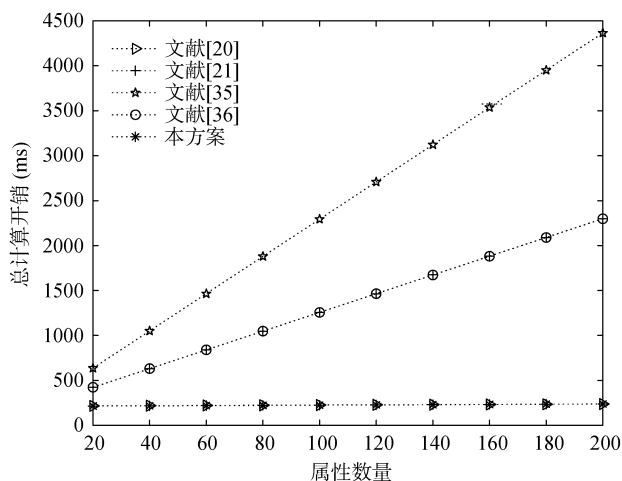


图5 各方案的总计算开销对比

Figure 5 Comparison of the total computational overhead of each scheme

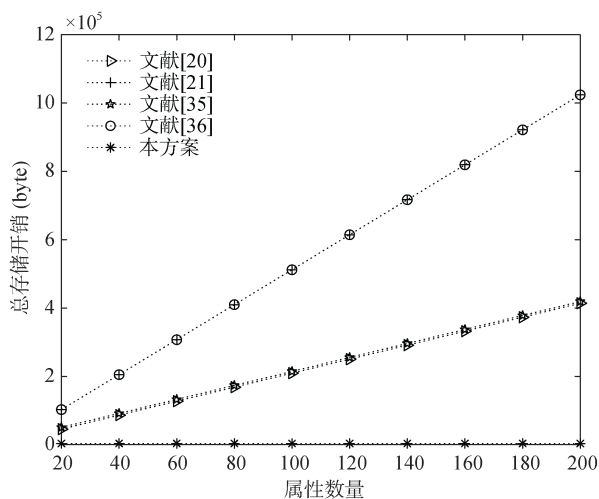


图6 各方案总存储开销对比

Figure 6 Comparison of total storage overhead of each scheme

发展, 为患者的诊治提供更加方便快捷的途径。但随着科技的发展, 在信息共享过程中存在信息泄露、未经授权访问等安全风险, 由于医疗信息本身的隐私性和敏感性, 信息一旦泄露很有可能会对患者以及相关人士带来一定的损失和伤害, 因此对患者医疗信息数据共享过程中的安全访问提出了较高的要求。本文将区块链技术与基于密文策略属性加密机制相结合, 提出一种基于区块链的医疗信息属性加密访问控制方案, 通过安全性证明、性能分析和实验对比, 结果表明本方案能够实现多个属性授权机构的访问控制以及对属性授权机构的追溯问责, 有效避免了单点故障问题; 降低了计算开销; 实现了患者对医疗信息细粒度、动态的访问控制, 能够更好的适用于医疗信息的安全共享。

参考文献

- [1] Wang X L, Jiang X Z, Li Y. Model for Data Access Control and Sharing Based on Blockchain[J]. *Journal of Software*, 2019, 30(6): 1661-1669.
(王秀利, 江晓舟, 李洋. 应用区块链的数据访问控制与共享模型[J]. *软件学报*, 2019, 30(6): 1661-1669.)
- [2] Shuwei Fan. Research on data access control method and application based on blockchain[J]. *Digital world*, 2019, (7):2-3.
- [3] Frank M, Buhman J M, Basin D. Role Mining with Probabilistic Models[J]. *ACM Transactions on Information and System Security*, 2013, 15(4): 15.
- [4] Sahai A, Waters B. Fuzzy Identity-Based Encryption[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 457-473.
- [5] Goyal V, Pandey O, Sahai A, et al. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data[C]. *The 13th ACM conference on Computer and communications security*, 2006: 89-98.
- [6] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]. *2007 IEEE Symposium on Security and Privacy*, 2007: 321-334.
- [7] Akinyele J A, Pagano M W, Green M D, et al. Securing Electronic Medical Records Using Attribute-Based Encryption on Mobile Devices[C]. *The 1st ACM workshop on Security and privacy in smartphones and mobile devices*, 2011: 75-86.
- [8] Yuping Zhou, Junjie Chen, and Xiaofang Zhou. Telemedicine scheme for wireless body area networks with privacy protection based on CP-ABE[J]. *Journal of Jilin Normal University (Natural Science Edition)*, 2018, 39(4):106-114.
- [9] Zhu S W, Zhong B C, Ding J R, et al. Research on Access Control Mechanism Based on Attribute Encryption in Wireless Medical Sensor Networks[J]. *Microcontrollers & Embedded Systems*, 2019, 19(2): 23-26.
(朱淑文, 钟伯成, 丁佳蓉, 等. 医疗传感网中基于属性加密的访问控制研究[J]. *单片机与嵌入式系统应用*, 2019, 19(2):

- 23-26.)
- [10] Nzanywayingoma F, Huang Q M, Communication N A B T, et al. Improving energy efficiency in M2M healthcare systems using CP-ABE schemes[C]. *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Automatic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops*, 2016: 1243-1248.
 - [11] Chase M. Multi-Authority Attribute Based Encryption[M]. *Theory of Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 515-534.
 - [12] Liu Z, Cao Z F, Huang Q, et al. Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption without Random Oracles[M]. *Computer Security - ESORICS 2011*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 278-297.
 - [13] Chase M, Chow S S M. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption[C]. *The 16th ACM conference on Computer and communications security*, 2009: 121-130.
 - [14] Lin H, Cao Z F, Liang X H, et al. Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority[J]. *Information Sciences*, 2010, 180(13): 2618-2632.
 - [15] Li Q, Zhu H B, Xiong J B, et al. Fine-Grained Multi-Authority Access Control in IoT-Enabled mHealth[J]. *Annals of Telecommunications*, 2019, 74(7): 389-400.
 - [16] Li J, Chen X F, Chow S S M, et al. Multi-Authority Fine-Grained Access Control with Accountability and Its Application in Cloud[J]. *Journal of Network and Computer Applications*, 2018, 112: 89-96.
 - [17] Qian H L, Li J G, Zhang Y C, et al. Privacy-Preserving Personal Health Record Using Multi-Authority Attribute-Based Encryption with Revocation[J]. *International Journal of Information Security*, 2015, 14(6): 487-497.
 - [18] Xu S W, Guo C R, Yuan F, et al. Encryption Scheme of Policy Hidden File Hierarchy Attribute Based on Access Tree[J]. *Computer Applications and Software*, 2021, 38(2): 323-327, 333.
(许盛伟, 郭春锐, 袁峰, 等. 基于访问树的策略隐藏文件层次属性加密方案[J]. *计算机应用与软件*, 2021, 38(2): 323-327, 333.)
 - [19] Sun J Z. *Research on searchable encryption schemes using CP-ABE in A cloud medical environment*[D]. Haikou: Hainan University, 2018.
(孙敬张. 云医疗环境下基于属性基的可搜索加密方案研究[D]. 海口: 海南大学, 2018.)
 - [20] Li Q, Ma J F, Li R, et al. Secure, Efficient and Revocable Multi-Authority Access Control System in Cloud Storage[J]. *Computers & Security*, 2016, 59: 45-59.
 - [21] Wu G Q. Multi-Authority CP-ABE with Policy Update in Cloud Storage[J]. *Journal of Computer Research and Development*, 2016, 53(10): 2393-2399.
(吴光强. 适合云存储的访问策略可更新多中心 CP-ABE 方案[J]. *计算机研究与发展*, 2016, 53(10): 2393-2399.)
 - [22] Cao H J. *Research on medical data security access and sharing mechanism in cloud storage*[D]. Xi'an: Xidian University, 2019.
(曹慧娟. 云存储医疗数据安全访问与共享机制研究[D]. 西安: 西安电子科技大学, 2019.)
 - [23] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org, 2008.
 - [24] Androulaki E, Manevich Y, Muralidharan S, et al. Hyperledger fabric[M]. *Proceedings of the Thirteenth EuroSys Conference on EuroSys* 18.2018.
 - [25] Sukhwani H, Martínez J M, Chang X L, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)[C]. *2017 IEEE 36th Symposium on Reliable Distributed Systems*, 2017: 253-255.
 - [26] KREPS J, NARKHEDE N, RAO J. Kafka: a distributed messaging system for log processing[C]. *The NetDB*, 2011(11):1-7.
 - [27] Witchey N J. Healthcare Transaction Validation via Blockchain proof-Ofwork, Systems and Methods: US20190267119[P]. 2019-08-29.
 - [28] Ariel Ekblaw, Asaph Azaria, John D. Halamka, et al. A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data[J]. *White Paper*, 2016:1-13.
 - [29] Al Omar A, Rahman M S, Basu A, et al. MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data[M]. *Security, Privacy, and Anonymity in Computation, Communication, and Storage*. Cham: Springer International Publishing, 2017: 534-543.
 - [30] Zhang P, White J, Schmidt D C, et al. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data[J]. *Computational and Structural Biotechnology Journal*, 2018, 16: 267-278.
 - [31] Jiang S, Cao J N, Wu H Q, et al. BlocHIE: A BLOCKchain-based platform for healthcare information exchange[C]. *2018 IEEE International Conference on Smart Computing*, 2018: 49-56.
 - [32] Ugobame Uchibeke U, Schneider K A, Hosseinzadeh Kassani S, et al. Blockchain access control ecosystem for big data security[C]. *2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, 2019: 1373-1378.
 - [33] Bellare M, Rogaway P. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols[C]. *The 1st ACM conference on Computer and communications security*, 1993: 62-73.
 - [34] Rouselakis Y, Waters B. Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption[M]. *Financial Cryptography and Data Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 315-332.
 - [35] Li Q, Zhu H B, Xiong J B, et al. Multi-Authority Attribute-Based Access Control System in m Health with Traceability[J]. *Journal on Communications*, 2018, 39(6): 1-10.
(李琦, 朱洪波, 熊金波, 等. mHealth 中可追踪多授权机构基于属性的访问控制方案[J]. *通信学报*, 2018, 39(6): 1-10.)
 - [36] Wu Z J, Zhang Y, Xu E Z. Multi-Authority Revocable Access Control Method Based on CP-ABE in NDN[J]. *Future Internet*, 2020, 12(1): 15.



郑丽娟 于 2014 年在北京交通大学信息安全专业获得博士学位。现为石家庄铁道大学信息科学与技术学院副教授。研究领域为隐私保护、区块链、访问控制。Email: zhengljjuan@stdu.edu.cn



张宇 于 2019 年在石家庄铁道大学网络工程专业获得工学学士学位。现在石家庄铁道大学计算机技术专业攻读硕士学位。研究领域为信息安全、区块链。Email: zhangsir077@outlook.com



吴朋钢 于 2018 年在石家庄铁道大学网络工程专业获得工学学士学位。现在石家庄铁道大学网络空间安全专业攻读硕士学位。研究领域为网络安全理论与技术。Email: wuppgg@foxmail.com



刘佳琪 于 2019 年在石家庄铁道大学教育技术学专业获得工学学士学位。现在石家庄铁道大学计算机科学与技术专业攻读硕士学位。研究领域为属性加密、数据访问控制、区块链。Email: liuxxhh2022@163.com



尤军考 于 2006 年在西南交通大学计算机应用专业获得硕士学位, 现任中国移动通信集团河北有限公司通信工程师, 研究领域: 互联网技术、信息安全。Email: youjunkao@he.chinamobile.com



陶亚男 现在石家庄铁道大学计算机科学与技术专业攻读学士学位。研究领域为计算机应用技术、实时计算机应用。Email: taoyanan@student.stdu.edu.cn



章睿 于 2011 年在北京交通大学信息安全专业获得博士学位。现为中国科学院信息工程研究所、信息安全国家重点实验室副研究员。研究领域为数据安全与隐私保护、区块链。Email: zhangrui@iie.ac.cn