计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(5):97−104 [doi: 10.15888/j.cnki.csa.009087]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于跨链的医疗数据安全共享方案①

何全文[1], 林庆新[2], 林　晖[1], 汪晓丁[1], 范新民[3]

[1](福建师范大学 计算机与网络空间安全学院, 福州 350117)
[2](福州大学至诚学院, 福州 350002)
[3](福建师范大学 网络与数据中心, 福州 350117)
通信作者: 林庆新, E-mail: lqx@fdzcxy.edu.cn

摘　要: 医疗机构之间的医疗数据共享对于实现跨医院诊断并促进医学研究发展有着举足轻重的作用. 为了解决医疗机构之间医疗数据共享困难的问题, 我们提出了一种基于跨链的医疗数据安全共享方案. 采用中继链、跨链网关和数据链结合的跨链架构, 结合 AES 和 CP-ABE 加密算法进行细粒度的医疗数据访问控制. 同时利用可搜索加密技术实现医疗数据的安全搜索. 为缓解区块链的计算存储开销, 将 IPFS 和区块链相结合, 链下存储密文, 链上存储密文地址和密钥. 通过安全性分析和实验证明, 该方案在医疗数据安全共享方面具有可行性.

关键词: 区块链; 跨链; 属性基加密; 可搜索加密; 访问控制

引用格式: 何全文,林庆新,林晖,汪晓丁,范新民.基于跨链的医疗数据安全共享方案.计算机系统应用,2023,32(5):97–104. http://www.c-s-a.org.cn/1003-3254/9087.html

Cross-chain-based Medical Data Security Sharing Scheme

HE Quan-Wen[1], LIN Qing-Xin[2], LIN Hui[1], WANG Xiao-Ding[1], FAN Xin-Min[3]

[1](College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China)
[2](Fuzhou University Zhicheng College, Fuzhou 350002, China)
[3](Network and Data Center, Fujian Normal University, Fuzhou 350117, China)

Abstract: The sharing of medical data among medical institutions plays an important role in realizing cross-hospital diagnosis and promoting the development of medical research. In order to solve difficult medical data sharing among medical institutions, this study proposes a cross-chain-based medical data security sharing scheme. The scheme adopts a cross-chain architecture combining relay chains, cross-chain gateways, and data chains and conducts fine-grained medical data access control based on AES and CP-ABE encryption algorithms. Moreover, searchable encryption is used to realize the safe search of medical data. In order to alleviate the computational storage overhead of blockchain, IPFS and the blockchain are combined for off-chain storage of ciphertext and on-chain storage of ciphertext addresses and keys. The security analysis and experiment prove that the scheme is feasible in medical data security sharing.

Key words: blockchain; cross-chain; attribute-based encryption (ABE); searchable encryption; access control

1　引言

随着物联网技术、人工智能和区块链等技术的不断发展, 智慧医疗也在逐步发展. 可穿戴设备、智能传感器等产生大量的医疗数据. 为方便数据共享, 越来越多的医疗机构开始将医疗数据存储到云服务器中. 但是医疗数据涉及了大量的患者隐私信息, 一旦云服务器被攻击或者在共享过程中被未经授权的用户获取, 可能造成医疗数据被篡改或者患者隐私信息遭到泄露. 因此保证存储在云服务器中的医疗数据不被未经授权的用户获取是非常重要的[1–3].

① 收稿时间: 2022-09-29; 修改时间: 2022-11-04, 2022-12-10; 采用时间: 2022-12-23; csa 在线出版时间: 2023-03-24
CNKI 网络首发时间: 2023-03-27

Goyal 等[4] 为了解决电子病历共享过程中隐私泄露问题, 提出了一种基于密文策略属性加密算法的细粒度访问控制方案, 并将加密后的电子病历存储在云服务器上, 通过云服务器实现医疗机构之间的电子病历共享. 基于密文策略的属性加密方案不仅实现了细粒度的数据访问控制也可以对电子病历进行了加密. Yang 等[5] 将区块链和属性加密相结合, 实现了医疗数据的安全共享. 首先, 对医疗数据进行加密, 并将密文存储到云服务器中. 而后将加密数据的存储地址和医疗相关信息上传到区块链中, 这样不仅可以确保数据高效率的存储, 而且缓解了区块链的存储开销. 其次, 为了解决医疗数据隐私和签名者身份泄露问题, 同时也要保证医疗数据源真实可信的问题, 该方案将基于属性的加密 (attribute-based encryption, ABE) 和基于属性的签名 (attribute-base signature, ABS) 相结合. Wu 等[6] 为了解决电子病历安全共享问题, 提出了一种基于联盟区块链和代理重加密的电子病历共享方案. 此方案中的电子设备连接到区块链网络, 通过自动执行区块链链代码确保数据访问的安全性; 基于属性的访问控制方法保证了对数据的细粒度访问; 代理重加密技术可以保证相对敏感数据的安全共享和传输.

Sun 等[7] 利用区块链和智能合约技术, 提出了一种分布式电子病历搜索方案. 首先基于属性的加密方法加密数据, 而后将其存储到星际文件系统 (interplanetary file system, IPFS) 中. 然后, 将电子病历的加密关键字索引信息存储到区块链上, 通过部署在区块链上的智能合约实现关键字搜索. 应作斌等[8] 将变色龙哈希和零知识证明结合解决区块链上恶意用户追踪溯源问题. 然后提出基于多个解密机构的属性基加密方案, 解决了密钥管理中的单点故障问题. Lee 等[9] 引入区块链和智能合约技术, 建立一个医疗区块链. 实现患者共享病历时对其隐私进行保护. Lai 等[10] 为了解决医疗数据安全共享问题, 将可追踪环签名和区块链相结合. 首先提出一种分布式密钥生成的无证书可追踪环签名算法, 以保证数据完整性和隐私保护. 其次, 智能合约结合访问控制和自控制对象 (self controlled objects, SCO) 可以实现解密外包和数据共享. 此外, 该方案利用 IPFS 存储海量的医疗隐私数据, 并对哈希索引进行加密存储, 提高了数据共享的效率. 最后, 结合区块链选择代理节点, 并使用共识机制将 SCO 包上传到区块链节点进行数据共享. Jiang 等[11] 将 Tangle 集成到物联网区块链中, 并在数据管理背景下构建了跨链交互式分散模型[12], 解决了数据存储和物联网区块链的隐私问题.

从上述方案讨论可以看出, 目前在医疗数据领域, 利用区块链来进行医疗数据的访问控制, 解决医疗数据的隐私泄露问题. 但随着医疗数据的不断增加, 应用的不断增多, 区块链的存储瓶颈成为发展瓶颈, 同时也出现了医疗机构之间数据共享不畅, 出现数据孤岛问题[13]. 同时数据隐私也是数据共享面临的关键问题. 针对医疗数据孤岛问题和医疗数据共享过程中的数据隐私问题. 本文主要研究工作如下.

1) 提出一种基于跨链的医疗数据安全共享方案, 解决医疗数据共享过程中加密数据的搜索和细粒度访问控制.

2) 访问策略隐藏, 未经授权的数据用户不能从访问策略中获得任何属性信息. 同时, 将访问控制和关键字搜索, 数据加密相结合, 只有两者都匹配, 用户才能解密数据.

3) 利用 IPFS 存储医疗数据密文, 区块链只存储密文在 IPFS 中的存储地址和密钥的密文. 这不仅缓解了区块链的存储压力, 也实现了细粒度的数据访问控制.

2 预备知识

2.1 属性基加密

属性基加密 (ABE)[14] 的思想来源于模糊身份基加密 (fuzzy identity-based encryption, FIBE), 属性基加密的思想是让密文和密钥与属性集合和访问结构产生关联, 当且仅当属性集合满足访问结构的时候, 方能解密成功.

2.2 可搜索加密

当数据存储在一个不可信的服务器时, 为了让服务器不能够了解到数据内容, 需要对数据加密后再存储. 为了实现在加密后的数据上进行关键词检索, 提出了可搜索加密 (searchable encryption, SE) 的思想[15]. SE 分为对称可搜索加密 (symmetric searchable encryption, SSE) 和非对称可搜索加密 (asymmetric searchable encryption, ASE). 两者的区别在于 SSE 使用对称加密算法, 加密和解密的密钥一样; ASE 使用非对称加密算法.

2.3 双线性映射

G和G_T是两个阶为素数p的乘法循环群, $g \in G$. 定义一个满足双线性、可计算性和退化性[16] 的双线性映射$e: G \times G \to G_T$.

(1) 双线性: 对于$\forall x, y \in G$, $\exists \alpha, \beta \in Z_p$, 使得等式

$e(x^{\alpha},y^{\beta})=e(x,y)^{\alpha\beta}$成立.

(2) 可计算性: 对于$\forall x,y\in G$, 存在一个有效的算法计算$e(x,y)$.

(3) 非退化性: $\exists g\in G$, 使得$e(g,g)\neq 1$.

2.4 困难性假设

Decisional bilinear Diffie-Hellman (DBDH) 困难问题假设[17], $g\in G$. 随机选取$a,b,c,z\in Z_p$, 挑战者给予敌手两个元组$(g,g^a,g^b,g^c,e(g,g)^{abc})$和$(g,g^a,g^b,g^c,e(g,g)^z)$, 敌手对$e(g,g)^{abc}$和$e(g,g)^z$进行判定是否相等, 如果相等, 敌手输出 1; 否则, 输出 0. 如果没有一个多项式时间算法以不可忽略的优势解决 DBDH 困难问题假设, 则 DBDH 假设成立.

Decisional Diffie-Hellman (DDH) 困难问题假设[18], $g\in G$, 随机选取$a,b,c,z\in Z_p$, 挑战者给予敌手两个元组(g^a,g^b,g^c)和(g^a,g^b,g^{ab}). 如果没有一个多项式时间算法以不可忽略的优势ε区分g^{ab}和g^c, 则 DDH 假设成立.

2.5 符号描述

本文涉及的符号描述如表 1 所示.

表 1 符号描述

符号	说明
κ	安全参数
Z_p	有限域
G, G_T	阶为素数p的乘法循环群
H	哈希函数
PP	系统公共参数
AA	属性授权中心
APK	属性授权中心公钥
ASK	属性授权中心私钥
ζ	用户属性集
SK_u	用户私钥
u	IPFS中存储地址
M	医疗数据明文
σ	对称加密密钥
C_M	医疗数据密文

3 本文方案

3.1 系统模型

如图 1 所示, 本文提出的系统模型由 6 个实体组成: 属性授权中心、患者、数据使用者、IPFS 和区块链.

1) 属性授权中心 (attribute authorities, *AA*). 属性授权中心负责管理用户属性并生成用户属性密钥.

2) 患者 (data owner, DO). 医疗数据所有者, 使用对称加密算法对医疗数据进行加密并将其存储到 IPFS 中. 同时为对称加密密钥和搜索关键字设置访问控制策略, 并将其上传到区块链.

3) 数据使用者 (data user, DU). 主要是医护人员或研究员, 用户生成关键字搜索陷门, 区块链节点进行搜索匹配, 当关键字匹配, 且数据使用者的属性满足患者所设置的访问控制策略时, 数据使用者便可以获得用于解密医疗数据密文的密钥, 从而对医疗数据密文进行解密.

4) IPFS. 存储医疗数据所有者将加密后的数据. 在降低区块链存储开销的同时, 实现密文数据的分布式存储.

5) 数据主链. 存储医疗数据的关键字密文和 IPFS 中的地址以及对称加密密钥的密文. 保证医疗数据的不可篡改.

6) 中继链. 主要用于数据主链的跨链管理, 以及跨链信息验证与存储.

7) 跨链网关. 是中继链和数据主链的中转站, 负责监听数据主链的跨链请求消息, 用于转发跨链请求.

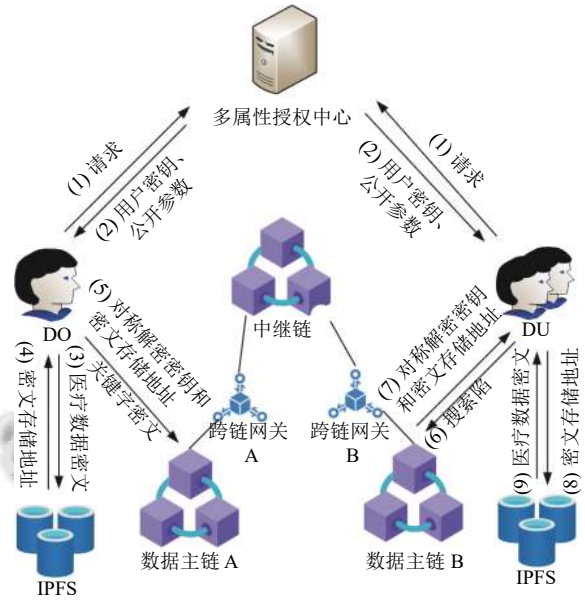

图 1 系统模型

3.2 属性基可搜索加密医疗数据共享方案定义

1) 系统初始化阶段

输入一个安全参数κ, 生成系统公共参数PP. 获得属性授权中心公钥APK和私钥ASK.

2) 密钥生成阶段.

输入公共参数PP、属性授权中心AA私钥ASK和用户属性集ζ, 输出用户私钥SK_u.

3) 数据加密阶段

使用对称加密算法加密原始的医疗数据, 将密文

上传到 IPFS 中存储, IPFS 返回其存储地址u, 而后使用 CP-ABE 加密对称加密密钥. 同时, 对关键字kw进行加密. 最后, 将数据密文的摘要, IPFS 存储地址u、对称加密密钥加密结果以及关键字密文存储到区块链上.

4) 数据搜索阶段

输入公共参数PP, 用户密钥SK_u, 关键字w获得陷门T_w. 将其上传到区块链节点, 如果用户上传的关键字匹配成功, 则返回加密医疗数据的密钥密文CT和医疗数据在 IPFS 中的存储地址μ.

5) 数据使用者解密阶段

首先, 数据使用者从区块链获得密钥密文CT, 如果数据使用者的属性满足数据用户设定的访问控制策略, 数据使用者便可以解密密文获得医疗数据密文的解密密钥σ. 最后, 数据使用者 DU 根据下载链接u下载密文C_M, 获得C_M后, 使用解密出的密钥σ解密密文C_M, 得到医疗数据明文M.

3.3 跨链交互

当数据主链 A 的用户想要获得数据主链 B 上的患者的数据时, 数据主链 A 的用户可以通过该跨链架构查询获取数据. 跨链查询流程如图 2 所示.

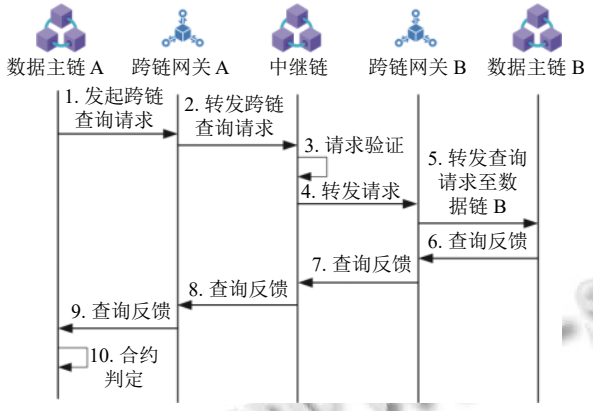

图 2 跨链查询流程图

首先, 数据主链 A 发起跨链查询请求. 跨链网关 A 监听到跨链请求事件. 跨链网关 A 将跨链请求转发到中继链. 中继链收到跨链请求后, 首先对请求进行验证, 验证通过后, 将请求信息存储到中继链节点上并转发给跨链网关 B, 网关 B 将收到的请求转给数据主链 B, 数据主链根据请求, 调用相应的智能合约. 因为查询反馈也是跨链的, 所以数据主链 B 将查询到的数据返回给数据主链 A 的过程, 与数据主链 A 发送跨链查询给数据主链 B 的过程一致. 既跨链网关 B 转发数据给中继链, 中继链转发给跨链网关 A, 跨链网关 A 将数据转给数据主链 A.

3.4 安全模型

本文方案安全模型通过敌手 Att 和挑战者 C 之间的挑战游戏进行刻画, 具体过程如下.

游戏 1. 关键字不可区分性.

1) 初始化阶段. 首先挑战者 C 运行初始化算法, 获得公共参数PP并生成属性授权中心的密钥, 并将其发送给敌手 Att.

2) 密钥询问阶段. 敌手 Att 向挑战者 C 进行属性私钥询问, 但所询问的属性不能满足要挑战的访问结构(M^*,ρ^*). 挑战者 C 生成属性私钥, 并将生成的属性私钥返回给敌手 Att.

3) 挑战阶段. 敌手 Att 向挑战者 C 发送两个等长关键字w_0和w_1. 挑战者 C 随机选择$b\in\{0,1\}$, 在访问结构(M^*,ρ^*)下, 对消息w_b进行加密, 加密完成后将密文发送给敌手 Att.

4) 猜测阶段. 敌手 Att 输出猜测$b'\in\{0,1\}$, 当$b'=b$时, 敌手 Att 赢得挑战游戏.

定义 1. 如果存在敌手 Att 能够在多项式时间内以优势$Adv_{Att}=\left|\Pr[b=b']-\frac{1}{2}\right|$赢得上述挑战游戏, 则我们的方案是安全的.

游戏 2. 陷门不可区分性.

1) 初始化阶段. 首先挑战者 C 运行初始化算法, 获得公共参数PP并生成属性授权中心的密钥, 并将其发送给敌手 Att.

2) 密钥询问阶段. 敌手Att向挑战者C进行私钥SK_u询问. 挑战者C生成私钥SK_u, 并发送给敌手Att. 陷门询问阶段. 敌手Att对关键字w进行询问, C生成搜索陷门T_w, 并将其发送给Att.

3) 挑战阶段. 敌手Att向挑战者C发送两个等长关键字w_0和w_1. 挑战者C随机选择$b\in\{0,1\}$, 生成加密关键字T_{w_b}并发送给Att.

4) 猜测阶段. 敌手Att输出猜测$b'\in\{0,1\}$, 当$b'=b$时, 敌手Att赢得挑战游戏.

定义 2. 如果存在敌手Att能够在多项式时间内以优势$Adv_{Att}=\left|\Pr[b=b']-\frac{1}{2}\right|$赢得上述挑战游戏, 则我们的方案是安全的.

3.5 属性基可搜索加密医疗数据共享方案构造

(1) 系统初始化阶段

输入安全参数κ. 选择阶为素数p的乘法循环群G和

G_T, 其中g为G的生成元. 定义双线性映射$e: G\times G\to G_T$. 选择哈希函数$H_1:\{0,1\}^*\to\mathbb{Z}_p$, $H_2:\{0,1\}^*\to G$. 生成系统公共参数$PP=\{e,p,g,H_1,H_2G,G_T\}$. 属性授权中心随机选择$\alpha,\beta,\mu\in\mathbb{Z}_p$, 计算属性授权中心公钥$APK=\{e(g,g)^{\alpha}, g^{\beta},g^{\mu}\}$和密钥$ASK=\{\alpha,\beta,\mu\}$.

(2) 密钥生成阶段

属性授权中心 AA 根据用户属性集ζ为用户计算属性私钥.

1) 随机选取$t\in\mathbb{Z}_p$, 计算$SK_{u1}=g^{\alpha+\mu t}$.

2) 对$\forall att\in\zeta$ (att 表示用户属性), 随机选取$r\in\mathbb{Z}_p$, 计算$SK_{ua}=g^{\mu r}$, $SK_{ua}^{'}=g^{t}H_2(att)^{-r}$.

最后, 输出用户密钥$SK_u=\{SK_{u1}=g^{\alpha+\mu t},\forall att\in\zeta: SK_{ua}=g^{\mu r},SK_{ua}^{'}=g^{t}H_2(att)^{-r}\}$, 并通过安全信道发送给用户.

(3) 数据加密阶段

1) 医疗数据第 1 次加密与存储. 患者首先使用 AES 对称加密算法, 通过 AES 加密算法的密钥σ对原始医疗数据M进行加密, 得到数据的密文.

$$C_M=Enc_{AES}(\sigma,M)$$

为了降低区块链的存储开销, 将密文C_M存储到 IPFS 中, 随后 IPFS 返回一个密文下载链接μ.

2) 数据第 2 次加密与存储. 用户设置访问控制策略(X,ρ), X是一个$l\times n$的矩阵, ρ是一个映射函数, 将X中的每一行 x 映射到用户属性. X_i表示X的第i行. 随机选择$s\in\mathbb{Z}_p$, 随机选取$\chi_1,\chi_2,\cdots,\chi_n\in\mathbb{Z}_p$, 设置向量$\overrightarrow{v}=(s,\chi_1,\chi_2,\cdots,\chi_n)$, 计算$\lambda_i=X_i\overrightarrow{v}$, 对密钥$\sigma$进行加密, 获得密文$C_0=\sigma\cdot e(g,g)^{\alpha s},C=g^{s},C_{1,i}=g^{\mu\lambda_i},C_{2,i}=H_1(\rho(i))^{\lambda_i},\forall i\in\zeta$.

(3) 关键字加密阶段

数据拥有者 DO 对关键字kw加密, $C_w=(H_1(kw)\cdot H_2(\rho(i)))^{\lambda_i}$, $C_w^{'}=e(g^{\mu s},g^{\beta})$.

数据拥有者将密文的存储地址μ, 密文摘要, 对称密钥σ的密文$CT=\{C_0,C,C_{1,i},C_{2,i}C_w,C_w^{'}\}$上传到区块链中.

(4) 数据搜索阶段

数据使用者 DU 先进行陷门生成, 输入关键字w, 对于$\forall att\in\zeta$, 数据使用者 DU 随机选择$\vartheta_i\in\mathbb{Z}_p$, 计算$T_1=(H_1(w),H_2(att))^{\vartheta_i}$, $T_2=g^{\mu\vartheta_i}$. 所以, 陷门$T_w=\{T_1,T_2\}$.

数据搜索, 用户提交搜索陷门T_w, 如果用户属性满足数据拥有者设定的访问控制策略(X,ρ), 存在一个常数集$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$, 其中$I=\{i:\rho(i)\in\zeta\}$, 使得$\sum_{i\in I}\omega_i\lambda_i=s$. 计算:

$$\theta=\frac{\prod_{i\in I}e(g^{\beta}\cdot T_1,C_{1,i})^{\omega_i}}{\prod_{i\in I}e(T_2,C_w)^{\omega_i}}=\frac{\prod_{i\in I}e(g^{\beta}\cdot(H_1(w)\cdot H_2(att))^{\vartheta_i},g^{\mu\lambda_i})^{\omega_i}}{\prod_{i\in I}e(g^{\mu\vartheta_i},(H_1(kw)\cdot H_2(\rho(i)))^{\lambda_i})^{\omega_i}}=\prod_{i\in I}e(g^{\beta},g^{\mu\lambda_i\omega_i})=e(g^{\beta},g^{\mu s})$$

验证θ是否等于$C_w^{'}=e(g^{\mu s},g^{\beta})$, 如果相等, 则搜索成功, 区块链节点将密文和数据存储地址发送给用户. 如果不相等, 则表示搜索失败. 终止算法运行.

(5) 数据使用者解密阶段

如果用户属性满足访问控制策略, 则计算$D=e(C_{1,i},SK_{ua}^{'})\cdot e(C_{2,i},SK_{ua})=e(g,g)^{t\mu s}$, 用户再根据自己的私钥计算出对称密钥:

$$\sigma'=\frac{C_0\cdot D}{e(C,SK_{u1})}=\frac{\sigma\cdot e(g,g)^{\alpha s}e(g,g)^{t\mu s}}{e(g^{s},g^{\alpha}g^{\mu t})}=\sigma$$

数据使用者根据 IPFS 下载链接u下载密文, 根据对称密钥σ对密文进行解密, 得到明文信息$M=Dec_{AES}(\sigma,C_M)$.

4 安全性分析

4.1 关键字安全

定理 1. 如果在多项式时间内, 敌手Att可以以不可忽略的优势ε赢得挑战游戏, 则挑战者C能够以$\frac{\varepsilon}{2}$的优势解决 DBDH 困难问题.

通过刻画敌手Att和挑战者C之间的挑战游戏证明方案的安全性.

1) 初始化阶段. 首先挑战者C运行初始化算法, 获得公共参数$PP=\{e,p,g,H_1,H_2G,G_T\}$. 随机选取$\alpha,\beta,\mu\in\mathbb{Z}_p$, 生成属性授权中心的主密钥, 并将$APK=\{e(g,g)^{\alpha},g^{\beta},g^{\mu}\}$返回给敌手$Att$.

2) 密钥询问阶段. 敌手Att向挑战者C进行私钥询问, 挑战者C运行密钥生成算法生成SK, 然后将SK返回给Att. 但所询问的属性不能满足要挑战的访问结构(M^*,ρ^*).

3) 挑战阶段. 敌手Att向挑战者C发送两个长度相等的关键字w_0和w_1. 挑战者C随机选择$b\in\{0,1\}$, 在访问结构(M^*,ρ^*)下, 对消息w_b进行加密, 获得密文CT. 随机选择$s,\chi_1,\chi_2,\cdots,\chi_n\in\mathbb{Z}_p$, 设置向量$\overrightarrow{v}=(s,\chi_1,\chi_2,\cdots,\chi_n)$,

计算$\lambda_i = M_i\vec{v}$, $C_0 = \sigma \cdot e(g,g)^{\alpha s}$, $C = g^s$, $C_{1,i} = g^{\mu\lambda_i}$, $C_{2,i} = H_1(\rho(i))^{\lambda_i}, \forall i \in \zeta$. $C_w = (H_1(kw) \cdot H_2(\rho(i)))^{\lambda_i}$, $C'_w = e(g^{\mu s}, g^{\beta})$. 然后将密文$CT = \{C_0, C, C_{1,i}, C_{2,i} C_w, C'_w\}$发送给敌手$Att$.

4) 猜测阶段. 敌手Att输出猜测$b' \in \{0,1\}$, 如果$b' = b$, 挑战者C输出 1, 敌手Att破解 DBDH 困难问题的优势为$Adv_{Att} = \left|\Pr[b = b'] - \frac{1}{2}\right| \leqslant \varepsilon$, 否则, 输出 0.

因此, 如果敌手Att以不可忽略的优势赢得挑战游戏, 那么挑战者C就能解决 DBDH 困难问题.

4.2 陷门安全

定理 2. 如果在多项式时间内, 敌手Att以不可忽略的优势赢得挑战游戏, 则挑战者C能构建一个算法去解决 DDH 困难问题.

通过刻画敌手Att和挑战者C之间的挑战游戏证明方案的安全性.

1) 初始化阶段. 首先挑战者C运行初始化算法, 获得公共参数$PP = \{e, p, g, H_1, H_2 G, G_T\}$. 随机选取$\alpha, \beta, \mu \in \mathbb{Z}_p$, 生成属性授权中心的主密钥, 并将$APK = \{e(g,g)^{\alpha}, g^{\beta}, g^{\mu}\}$发送给敌手$Att$.

2) 密钥询问阶段. 敌手Att向挑战者C进行私钥询问, 计算私钥$SK_u = \{SK_{u1} = g^{\alpha+\mu t}, \forall att \in \zeta : SK_{ua} = g^{\mu r}, SK'_{ua} = g^t H_2(att)^{-r}\}$,

然后将私钥SK_u发送给敌手Att. 陷门询问, 计算陷门, 输入关键字w, 对于$\forall att \in \zeta$, 随机选择$\vartheta_i \in \mathbb{Z}_p$, 计算$T_1 = (H_1(w), H_2(att))^{\vartheta_i}$, $T_2 = g^{\mu\vartheta_i}$. 所以, 陷门为$T_w = \{T_1, T_2\}$.

3) 挑战阶段. 敌手Att向挑战者C发送两个等长关键字w_0和w_1. 挑战者C随机选择$b \in \{0,1\}$, 计算关键字w_b陷门, 获得陷门T_w. 并返回给Att.

4) 猜测阶段. 敌手Att输出猜测$b' \in \{0,1\}$, 如果$b' = b$, 挑战者 C 输出 1, 敌手Att破解 DDH 困难问题的优势为$Adv_{Att} = \left|\Pr[b = b'] - \frac{1}{2}\right| \leqslant \varepsilon$, 否则, 输出 0.

因此, 如果敌手Att以不可忽略的优势赢得挑战游戏, 那么挑战者C就能解决 DDH 困难问题.

5 性能分析和仿真实验分析

5.1 功能性分析

如表 2 所示, 本文方案与文献 [19–22] 在访问控制策略、可搜索、策略隐藏和区块链技术方面的功能对比, 可以看出, 本文方案在功能上有一定的优势.

5.2 仿真实验分析

本节仿真实验是基于 Ubuntu 20.04 系统, i5-7500 3.40 GHz, 8 GB 运行内存, 构建 Hyperledger Fabric v1.4.2 联盟链.

表 2 功能对比

方案	访问控制策略	可搜索	策略隐藏	区块链技术
文献[19]	访问树	×	×	√
文献[20]	访问树	√	×	√
文献[21]	访问树	×	×	×
文献[22]	LSSS	√	×	×
本文方案	LSSS	√	√	√

5.2.1 区块链网络性能

测试区块链查询数据与写入数据的性能. 不同并发量下区块链的读写性能如图 3 所示, 实验结果表明, 随着并发量的增加, 区块链的读写时延也在逐渐地增加, 在并发量为 300 TPS 时, 查询平均时延为 2 134.41 ms, 写入的平均时延为 4 239.72 ms.

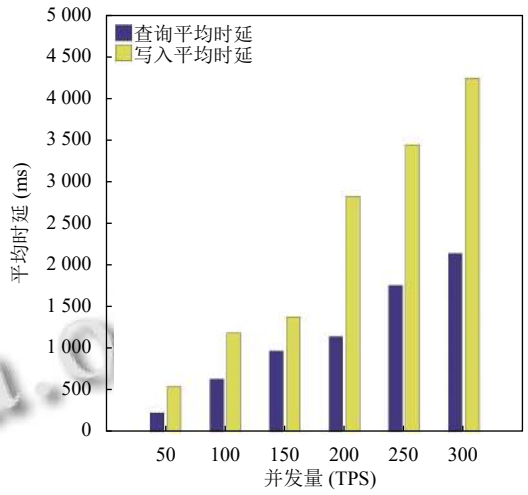

图 3 区块链读写时延

5.2.2 数值实验分析

本节实验是在虚拟机上运行 Linux 系统, 利用 JPBC 库, 采用 Java 语言进行编程.

图 4 是用户密钥生成时间与用户属性个数之间的关系, 将本文方案与文献 [19,23] 方案进行对比, 由图 4 可知, 用户的属性数量影响着用户密钥生成时间耗费. 随着用户属性数量的增加, 用户密钥生成时间也在增加.

图 5 是本文方案的加解密时间与属性个数的关系. 加密时间由 AES 算法加密数据的时间和 CP-ABE 算

法加密 AES 密钥的时间组成. 解密时间由 CP-ABE 算法解密 AES 密钥的时间和 AES 算法解密数据的时间组成. 从图 5 可知, 用户加解密所消耗的时间与用户的属性数量呈线性关系. 数据解密时间的整体消耗要低于加密时间消耗.

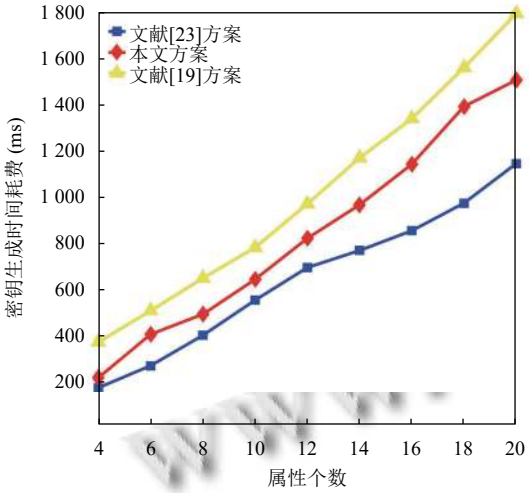

图 4 密钥生成时间消耗

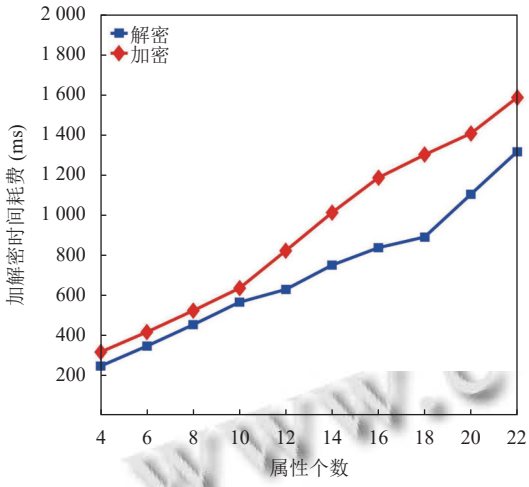

图 5 加解密时间消耗

6 结束语

为了解决医疗机构之间医疗数据共享困难的问题, 本文提出基于跨链的医疗数据安全共享方案. 为了保护的患者隐私信息, 使用 CP-ABE 算法进行细粒度的访问控制. 此外, 利用可搜索加密技术使数据用户可以快速查找到数据同时, 不泄露任何搜索信息. 同时使用 IPFS 存储医疗数据密文, 将存储地址和密钥存储到区块链中, 以缓解区块链存储压力. 实验结果表明了本文方案在医疗数据传输和共享方面是可行的.

参考文献

1 Saini A, Zhu QY, Singh N, *et al*. A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet of Things Journal, 2021, 8(7): 5914–5925. [doi: 10.1109/JIOT.2020.3032997]

2 Shen BQ, Guo JZ, Yang YL. MedChain: Efficient healthcare data sharing via blockchain. Applied Sciences, 2019, 9(6): 1207. [doi: 10.3390/app9061207]

3 Sun J, Yao XM, Wang SP, *et al*. Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE Access, 2020, 8: 59389–59401. [doi: 10.1109/ACCESS.2020.2982964]

4 Goyal V, Pandey O, Sahai A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria: ACM, 2006. 89–98.

5 Yang XD, Li T, Pei XZ, *et al*. Medical data sharing scheme based on attribute cryptosystem and blockchain technology. IEEE Access, 2020, 8: 45468–45476. [doi: 10.1109/ACCESS.2020.2976894]

6 Wu S, Du J. Electronic medical record security sharing model based on blockchain. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. Kuala Lumpur: ACM, 2019. 13–17.

7 Sun J, Ren LL, Wang SP, *et al*. A blockchain-based framework for electronic medical records sharing with fine-grained access control. PLoS One, 2020, 15(10): e0239946. [doi: 10.1371/journal.pone.0239946]

8 应作斌, 斯元平, 马建峰, 等. 基于区块链的分布式 EHR 细粒度可追溯方案. 通信学报, 2021, 42(5): 205–215.

9 Lee JS, Chew CJ, Liu JY, *et al*. Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. Journal of Information Security and Applications, 2022, 65: 103117. [doi: 10.1016/j.jisa.2022.103117]

10 Lai CZ, Ma Z, Guo R, *et al*. Secure medical data sharing scheme based on traceable ring signature and blockchain. Peer-to-Peer Networking and Applications, 2022, 15(3): 1562–1576. [doi: 10.1007/s12083-022-01303-w]

11 Jiang YM, Wang CX, Huang Y, *et al*. A cross-chain solution to integration of IoT tangle for data access management. Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and

Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax: IEEE, 2018. 1035–1041.

12 Jin H, Dai XH, Xiao J. Towards a novel architecture for enabling interoperability amongst multiple blockchains. Proceedings of the 38th IEEE International Conference on Distributed Computing Systems (ICDCS). Vienna: IEEE, 2018. 1203–1211.

13 Lin SF, Kong YH, Nie ST, *et al*. Research on cross-chain technology of blockchain. Proceedings of the 6th International Conference on Smart Grid and Electrical Automation (ICSGEA). Kunming: IEEE. 2021. 405–408.

14 Yan XX, Ni H, Liu Y, *et al*. Privacy-preserving multi-authority attribute-based encryption with dynamic policy updating in PHR. Computer Science and Information Systems, 2019, 16(3): 831–847. [doi: 10.2298/CSIS180830029Y]

15 Song DX, Wagner D, Perrig A. Practical techniques for searches on encrypted data. Proceedings of the 2000 IEEE Symposium on Security and Privacy. Berkeley: IEEE, 2000. 44–55.

16 李双, 徐茂智. 基于属性的可搜索加密方案. 计算机学报, 2014, 37(5): 1017–1024.

17 葛纪红, 沈韬. 基于区块链的能源数据访问控制方法. 计算机应用, 2021, 41(9): 2615–2622. [doi: 10.11772/j.issn.1001-9081.2020111844]

18 周艺华, 扈新宇, 李美奇, 等. 云环境下基于属性策略隐藏的可搜索加密方案. 网络与信息安全学报, 2022, 8(2): 112–121. [doi: 10.11959/j.issn.2096-109x.2022019]

19 阳真, 黄松, 郑长友. 基于区块链与改进 CP-ABE 的众测知识产权保护技术研究. 计算机科学, 2022, 49(5): 325–332. [doi: 10.11896/jsjkx.210900075]

20 牛淑芬, 谢亚亚, 杨平平, 等. 区块链上基于云辅助的属性基可搜索加密方案. 计算机研究与发展, 2021, 58(4): 811–821. [doi: 10.7544/issn1000-1239.2021.20200041]

21 Miao YB, Ma JF, Liu XM, *et al*. Attribute-based keyword search over hierarchical data in cloud computing. IEEE Transactions on Services Computing, 2020, 13(6): 985–998.

22 Zheng QJ, Xu SH, Ateniese G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data. Proceedings of the 2014 IEEE Conference on Computer Communications. Toronto: IEEE, 2014. 522–530.

23 Lewko A, Waters B. Decentralizing attribute-based encryption. Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn: Springer, 2011. 568–588.

(校对责编: 孙君艳)