基于区块链的去中心化多授权机构访问控制方法

刘　炜[1,2,3,4]，李淑培[2,3,5]，田　钊[1,2]，佘　维[1,2,3]

(1. 郑州大学 网络空间安全学院　河南 郑州 450002；
2. 郑州市区块链与数据智能重点实验室　河南 郑州 450002；
3. 郑州大学 互联网医疗与健康服务河南省协同创新中心　河南 郑州 450052；
4. 河南省网络密码技术重点实验室　河南 郑州 450001；
5. 郑州大学 计算机与人工智能学院　河南 郑州 450001)

摘要：传统的基于单一授权机构的访问控制方案存在单点故障、效率低下等问题，为此提出一种基于区块链的去中心化多授权机构访问控制方法。首先，采用基于联盟链的多授权机构取代传统访问控制方法中的中心化实体，提供可靠、细粒度的访问控制；其次，智能合约允许自动化访问判决，为了解决多授权机构带来的访问效率问题，提出一种基于智能合约的数据映射算法，利用数据关键信息构建映射表实现数据快速访问；最后，实验表明，所提出的方案能够有效降低用户访问时延，实现数据访问过程中的安全共享。

关键词：访问控制；区块链；智能合约；属性加密；数据共享

中图分类号：TP311.13　　**文献标志码**：A　　**文章编号**：1671-6841(2025)05-0046-08

DOI：10.13705/j.issn.1671-6841.2024032

Blockchain-based Decentralized Multi-authority Access Control Method

LIU Wei[1,2,3,4], LI Shupei[2,3,5], TIAN Zhao[1,2], SHE Wei[1,2,3]

(1. *School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou* 450002, *China*;
2. *Zhengzhou Key Laboratory of Blockchain and Data Intelligence, Zhengzhou* 450002, *China*;
3. *Collaborative Innovation Center of Internet Medical and Health Services, Zhengzhou University, Zhengzhou* 450052, *China*;
4. *Henan Key Laboratory of Network Cryptography Technology, Zhengzhou* 450001, *China*;
5. *School of Computer and Artificial Intelligence, Zhengzhou University, Zhengzhou* 450001, *China*)

Abstract: The traditional access control scheme based on single authorization authority. To solve its single point of failure and inefficiency, a decentralized multi-authorization authority access control method was proposed based on blockchain. Firstly, The approach used the consortium blockchain based multi-authorization authorities to replace the centralized entity in traditional access control methods, which could provide reliable and fine-grained access control. Secondly, smart contract allowed automatic policy judgments, and to solve the access efficiency problem caused by multiple authorized institutions, a data mapping algorithm based on smart contract was proposed to achieve fast access, which constructed a mapping table of key data information. Finally, experiments showed that the proposed scheme could effectively reduce user access delay and realize secure sharing during data access.

Key words: access control; blockchain; smart contract; attribute-based encryption; data sharing

收稿日期：2024-02-25
基金项目：河南省高等学校重点科研项目(24A520045)
第一作者：刘炜(1981—)，男，副教授，主要从事区块链、信息安全，智慧医疗研究，E-mail：wliu@zzu.edu.cn。
通信作者：田钊(1985—)，男，副教授，主要从事区块链、信息安全、智能交通研究，E-mail：tianzhao@zzu.edu.cn。

0　引言

随着科技的不断发展,实现数据共享和促进数据互操作性变得至关重要,这有助于更精准地访问数据并提高数据的潜在利用价值[1]。然而敏感数据的集中存储和滥用给数据的有效共享带来了重大的安全风险[2-3],包括潜在的数据泄露和未经授权的访问。访问控制是提高数据安全性的一种重要方法。Gupta 等[4]提出的模型定义了相关不可信方之间的访问策略和通信协议。董江涛等[5]提出的雾计算中基于无配对密文策略属性加密(ciphertext policy attribute-based eneryption,CP-ABE)可验证的访问控制方案保证了数据机密性和细粒度访问控制。Zheng 等[6]设计了基于类型的代理重加密进行细粒度共享。陈英杰等[7]提出基于 RBAC 的访问控制增强模型,确保合法用户的访问授权。Zhang 等[8]和 Jiang 等[9]实现了密文策略的 ABE 方案,通过加密算法秘密传输数据信息。以上研究解决了云存储环境中的数据存储和共享问题,然而需要通过中心组织机构授权来完成权限审查和数据校验。

传统访问控制存在访问流程不透明、难以溯源等问题[10]。区块链去中心化的环境为访问控制机制的实施提供了可信透明的保障,为数据共享和安全访问提供了全新模式[11-12]。巩坪等[13]提出基于区块链表示资源访问策略的方法,并将权限交换过程展现在区块链上。牛淑芬等[14]提出了包含联盟链、私有链和云服务器等的访问控制模型。以上方案在访问策略实施和授权判决过程中为去中心化的执行环境提供了透明的数据使用情况,但是在分布式环境下仍无法实现高效访问。为提高访问控制策略评估的可审计性和效率,Liu 等[15]提出一种基于 ABAC 的智能合约访问控制方法。Wang 等[16]提出了基于区块链构建私有数据的共享方案,并使用智能合约制定细粒度的访问策略,同时设计链下智能合约来辅助处理用户隐私数据。以上研究虽然解决了数据共享过程中涉及交互机构和用户范围广泛而导致的难以审计的问题,但在访问属性隐私和策略表达粒度层面有待加强。

目前,基于区块链的数据访问控制方法研究在数据安全可控方面取得了一定进展,但访问授权过程仍集中在中央权威机构,数据授权容易受到外部入侵和内部扰动。为了解决上述挑战,本文提出了一种基于区块链的去中心化多授权机构访问控制方法,结合智能合约实现访问控制和数据可控共享,同时保护数据隐私。去中心化的属性授权机构共同验证用户属性和管理密钥,并颁发密钥构件以保证密钥安全性,同时引入基于智能合约的数据映射表和时间限制策略,实现高效的访问请求和去中心化的授权。

1　相关技术

区块链技术是一种分布式的同步共享账本技术,具有去中心化、可追溯、持久性的特征,可提供灵活可编程的环境开发出去中心化的应用程序(DApp),允许点对点传输,具有防篡改特性,通过加密安全的链上交易完成事务和状态的转变,可以为访问控制过程提供去中心化的执行环境,实现可信访问。

传统访问授权方案中单一属性授权机构造成权威集中,策略判决仅存在于少数机构间。本文方法采用联盟链架构,由多个监管组织共同管理,只有经过授权的实体能够访问特定信息。利用区块链的不可篡改和分布式特性,将联盟链网络中的节点机构取代传统 CP-ABE 方案中的属性授权机构,该方案构建一个保证用户数据隐私以及各方数据安全交换的模型,并结合联盟链、属性加密以及智能合约自动执行实现安全可靠的访问控制过程,用户私钥由分布式的节点协作生成,避免传统 CP-ABE 方案中权威集中的情况,实现细粒度访问控制和数据隐私保护。同时为避免数据的关键信息泄露,具有限时访问控制,有效识别重复数据,并拒绝相应存储请求,且由联盟链中各节点共同维护映射表,以提高访问速度。

2　系统方法

在传统 CP-ABE 模型基础上,提出了基于区块链的去中心化多授权机构访问控制(blockchain-based decentralized multi-authority access control, BC-DMAC)方法,利用智能合约为访问控制过程提供高效可信的自动化执行环境。

2.1　访问控制模型

模型的主要组成实体包括联盟链 CB、星际文件传输系统 IPFS、授权机构、数据拥有者 DO、数据访问者 DU。授权机构又分为监管机构 RA 和属性授权机构 AA,属性授权机构 AA 主要基于联盟链,由监管部门组成。模型中涉及的符号和意义见表 1。

本文采用区块链中的联盟链模式进行构造,其

表1 符号及其含义

Table 1 Symbols and meaning

符号	含义	符号	含义
CB	联盟链	$hash_{ipfs}$	对称密文存储地址
IPFS	星际文件系统	key	对称密钥
RA	监管机构	M_{se}	对称密文
DO	数据拥有者	GPK_{uid}	用户全局公钥
DU	数据访问者	GSK_{uid}	用户全局私钥
AA_k	属性授权机构	$atrr_k$	属性授权机构属性公钥
m	明文数据	$SK_{uid,k}$	用户私钥构件
uid	用户身份标识	$\{SK_{uid,k}\}$	用户私钥

具有部分去中心化的特点,由联盟链CB作为系统方案的底层平台,由多个组织或部门的监管机构RA负责共同管理,建立机构间的信任,同时保留公有链的特性。普通节点负责存储和打包上传相关访问控制信息,用户相关的访问操作通过授权节点触发智能合约完成数据访问,区块链网络通过链上交易和事务提供可审计的分布式账本。

数据拥有者DO和数据访问者DU是隐私数据共享过程中最关键的实体,要求用户必须具有全局唯一的标识符 uid。同时由权威监管部门担任监管机构RA,对数据进行管理。相较于其他属性基方案,本文基于联盟链构建分布式多授权机构,不同的授权机构交叉管理同一个属性,同时一个属性由多个授权机构共同管理,避免单个AA失效的时候无法验证其属性域。属性授权机构主要由需要负责审核和控制数据共享的各个机构内的监管部门担任。包含一个RA和多个AA。RA机构在联盟链中地位可信,并接受链上链下的监控,在链上记录认证信息。所有AA授权机构都可以验证用户的 uid。

基于区块链的访问控制模型描述见图1。

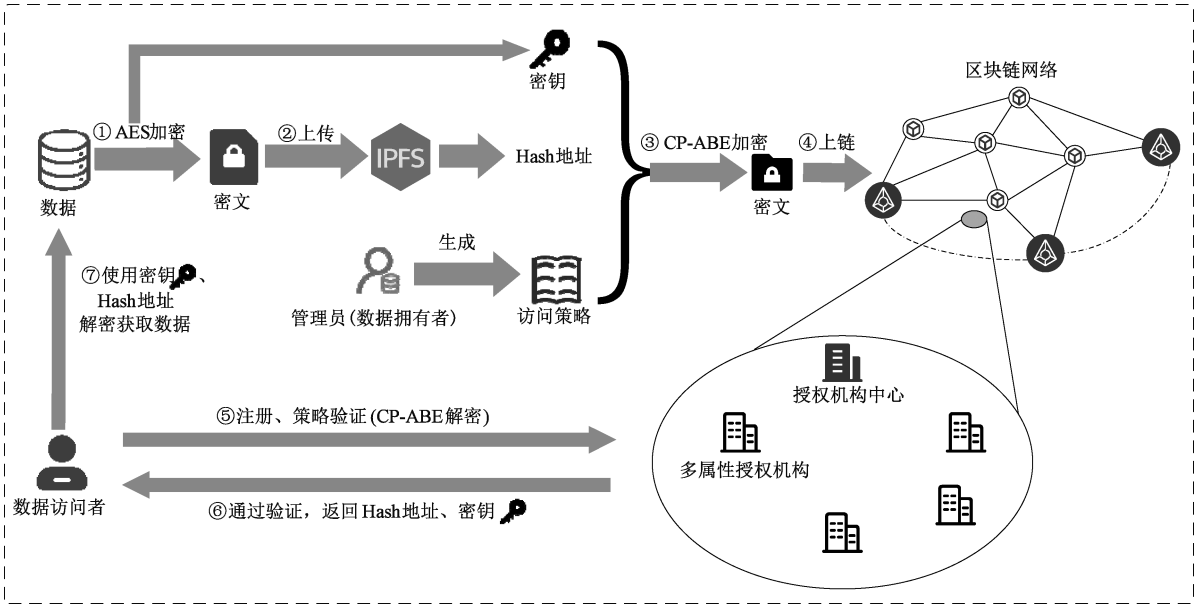

图1 基于区块链的访问控制模型

Figure 1 Blockchain-based access control model

2.2 基于智能合约的数据映射算法

针对数据共享模型中单点故障、效率低下的问题,本文构造了去中心化的多授权机构访问控制方法,并提出了基于智能合约的数据哈希检索算法。针对访问控制过程中不可靠的单点授权造成的隐私威胁,BC-DMAC将区块链网络替代传统的中心服务器。

2.2.1 *授权机构初始化* 由区块链节点共同选出可靠的监管机构RA节点,区块链内各个节点互相承认链上操作和记录,其中RA节点不包含任何属性,也不负责验证用户属性,只负责全局钥对的构成。

参数设置算法由RA执行,并生成相应的双线性对 $e:G_0\cdot G_0\rightarrow G_1$,群 G_0,G_1 的阶均为素数 p。首先对数据进行哈希散列,为了在请求数据时快速检索和查找,产生一个哈希散列表DHT(data Hash table),使用SHA-1(secure Hash algorithm 1)选择一个哈希函数 $H_0:\{0,1\}^*\rightarrow G$,便于验证数据完整性的同时在DET中快速检索数据。

为了减少CP-ABE对数据直接加密产生的大量计算,同时缩短存储的加密密文,本文使用AES(advanced encryption standard)对称加密,遵循混合加密的思想保护数据隐私,初始化选择 $AES()$ 对称算法,其中包括对称加密 $AES.Enc()$ 和解密 $AES.Dec()$。RA执行RASetup(),系统安全参数 q 作为

输入,生成一对签名钥对(sk_{RA}, vk_{RA}),随机选择参数 $a \in Z_p$,输出系统公共参数为 $GPP(g, g^a, G_0, G_1, H_0, AES())$,其中 g 是 G_0 的生成元。

RA 将属性随机分给 AA,每个属性由 K 个属性授权机构共同管理,同时每个 AA 获得不同的属性集进行独立管理。算法 AASetup 选择三个随机数 $\alpha_k, \beta_k, \gamma_k \in Z_r$ 作为 AA_k 的密钥,$ASK_k = (\alpha_k, \beta_k, \gamma_k)$,对于 AA 管理的每个属性 $atrr_k$,生成属性公私钥对。同时,AA 生成公钥 APK_k。RA 汇集 AA_k 的所有属性公钥 $\{atrr_k\}$ 和公钥 APK_k,将集合 $\{APK\}$ 和 $\{APK_{attr}\}$ 上传至区块链。

2.2.2 *多授权机构密钥颁发*　每个用户向 RA 注册,其动作触发注册合约,RA 运行注册合约 RegisterSC,以系统参数和用户信息为输入,为每个用户分配一个全局用户标识符 uid,随机选择 $u_{uid}, z_{uid} \in Z_p$,生成用户 uid 的全局公钥 $GPK_{uid} = g^{uid}$ 和全局私钥 $GSK_{uid} = z_{uid}$。RA 为用户 uid 颁发认证证书 $Cert(uid)$,包含 RA 对用户 uid 的签名信息 $Sign_{RA}$,并将用户公钥、私钥和认证证书发送给用户 uid。

每个 AA 应该审核用户身份,根据验证密钥 vk_{RA} 识别用户是否合法,如果用户身份合法,则 AA_k 基于管理的属性域以及与用户匹配的属性集合执行 SKeyGen 算法,输出 AA 颁发给用户的私钥 $SK_{uid,k}$,具体流程如算法 1 所示。

算法 1　密钥颁发

输入:系统参数 GPP,用户注册信息 $UsrInfo$,属性授权机构 AA 的标识 AA_k。

输出:用户 uid,用户全局公钥 GPK_{uid},用户全局私钥 GSK_{uid},认证证书 $Cert(uid)$,属性私钥集合 $\{SK_{uid,k}\}$。

1) if($UsrInfo$ = = null)
2) return Error("args error")
3) end if
4) $uid \leftarrow setuid(UsrInfo)$
5) $u_{uid}, z_{uid} \in Z_p$ //选择随机数
6) $(GPK_{uid}, GSK_{uid}) \leftarrow$ KeyGen(u_{uid}, z_{uid}) //生成用户的公私钥对
7) for $k=0 \rightarrow K-1$ in AA do//遍历属性授权机构 AA
8)　for $i=0 \rightarrow m-1$ in O_{AA} do//遍历 AA 支配的属性 O_{AA}
9) while($attr_i$ in O_{AA}) //判断 AA 支配的属性是否匹配
10) i++
11) if $i \geqslant 1$
12) $uid \leftarrow SK_{uid,k}$
13) end if
14) $\{SK_{uid,k}\} \leftarrow SK_{uid,k}$
15)　end while
16)　end for
17) end for

2.2.3 *数据上传*　由数据拥有者 DO 制定访问结构。在将数据外包传到云环境之前,DO 通过利用 SHA-1 对数据 m 进行哈希运算获得哈希摘要值 $hash$,DO 向 RA 申请数据加密权限,DO 通过运行加密算法对数据加密。算法接受系统公共参数 GPP,在加密中附上对称密钥 key 和制定的访问结构 (M, ρ)。为了方便后续快速查找数据映射表(data mapping table,DET),在加密数据前,对数据 m 提取 x 个关键字 w,按照数据关键词随机哈希构成 m 的关键字集 $keyWord$,随机选取 $\theta \in Z_p^*$,计算私钥 $SK_{kw} = \theta$,$PK_{kw} = g^{\theta}$,使用 PK_{kw} 将关键字集合 $keyWord$ 加密成 C_{kw}。

根据数据 m 的逻辑粒度、数据类型等将数据划分成 $m = \{m_1, m_2, \cdots, m_n\}$,使用 AES 对称加密密钥 $(key_1, key_2, \cdots, key_n)$ 加密对应的块,key_i 加密相应的 m_i,将 AES 加密获得的密文 M_{se} 上传至星际文件系统(inferplanetary file system,IPFS),IPFS 返回 $hash_{IPFS}$。

DO 制定详细的访问结构,将访问结构嵌入加密密文 CT。密码学的基础计算量和密码库中的随机数为 g, e, k, i,算法随机选择 $r_1, r_2, \cdots, r_n \in Z_p$,计算密文,

$$CT = \{M_{se} = En_{key}(m), C = k \cdot (\prod_{k \in I_A} e(g,g)^{\alpha_k})^s,$$

$$C' = g^s, C'' = g^{s/\beta_k} \forall i \in (1,l),$$

$$C_i = g^{a\hat{\lambda}_i} \cdot ((g^{v_{\alpha it}} H(\rho(i)))^{\gamma_k})^{-r_i},$$

$$D_{1,i} = g^{\frac{r_i}{\beta_k}}, D_{2,i} = g^{-\frac{\hat{\Lambda}_k}{\beta_k} r_i}, \rho(i) \in O_k\}。$$

2.2.4 *基于哈希映射的数据检索*　为了提高数据关键信息的快速查找,以数据描述信息和数据访问部分构建数据映射表,在运行解密算法之前能方便快速查找数据,并以数据的限时时间限制其有效访问时长。

DO 基于密文 ct 上传至 IPFS 上,IPFS 返回密文存储的 $hash$ 地址 $hash_{IPFS}$ 构建链上数据映射表 DET,映射表 DET 以数据唯一标识符 $DataID$ 标注,由数据描述信息和数据访问信息两部分构成:包括数据来源 $DataSource$、数据概要 $DataSummary$、限时时间 $RestrictTime$、地址 ID、数据大小 $Size$。IPFS 存储

地址 $hash_{\text{IPFS}}$、数据哈希摘要 *hash* 及密文 *CT*。数据映射表生成过程由智能合约 UploadDataSC 完成,在智能合约中创建映射表存储数据的访问权限,映射表将数据的唯一标识符和数据的关键信息进行关联,同时形成一条区块链交易记录。使用映射表 DET 将数据的标识符和数据的属性信息的映射关系存储在智能合约中,具体流程如算法 2 所示。

算法 2 数据映射表上链

输入:数据标识符 *DataID*,数据拥有者 *ID*。

输出:bool。

1) if (*DataID* = = null ‖ *DataSource* = = null ‖ *DataSummary* = = null ‖ *ID* = = null ‖ *Size* = = null ‖ $hash_{\text{IPFS}}$ = = null ‖ *hash* = = null ‖ *CT* = = null) then

2) return Error("args error")

3) else

4) *flag* ← *dataExist*(*DataID*)

5) if *flag* = = True then

6) return Error("*DataID* 的 DET 已经存在")

7) else

8) DET ← { *DataID*, *DataSource*, *DataSummary*, ID, Size, $hash_{\text{IPFS}}$, *hash*, *CT*, *RestrictTime* }//构建一条新的 DET 记录,存储在区块链中

9) Record(DET)

10) return (ture)//数据信息的 DET 成功上传到区块链中

11) end if

12) end if

数据关键字 *keyWord* 是查找 DET 表的关键,在真正运行解密算法之前快速查找和比对,实现在数据加密状态下对数据关键字进行高效的搜索,用户生成关键字的陷门发送给服务器端,并利用数据映射表快速定位。实现解密时根据查看数据关键字查找到数据描述信息进行比对和查验,确认交易信息和访问数据是否为访问者感兴趣的数据,而无须解密整个数据集。任何人可以查询感兴趣的 DET,通过验证和查看 DET 中的数据描述信息确定获得访问的数据。

数据访问者 DU 发起访问请求,查询区块链交易记录,当 DU 需要查看数据时,需要提交自己的令牌信息。合法用户的属性集满足嵌入到密文当中的访问结构时,就能解密此内容密钥,并进一步使用密钥解密数据,包括颁发属性令牌和数据解密两个步骤。

访问者执行陷门算法提取陷门,根据关键字 *keyWord* 获得关键词陷门 T_{kw},提取出陷门后匹配和查询交易,$Query(PK_{\text{kw}}, C_{\text{kw}}, T_{\text{kw}}) \rightarrow \eta$,若 $\eta = 1$,则查询成功,$\eta = 0$,则查询失败。

待查询到访问交易的数据时,来自授权机构 $\{AA_1, AA_2, \cdots, AA_k\}$ 颁发的用户私钥构建成用户 *uid* 的集合 $\{SK_{uid,k}\}$,从而获得私钥 $k \in \boldsymbol{N}^+$ 发送至服务器请求解密密文的解密令牌。只有当用户拥有的属性集合满足密文 *CT* 中嵌入的属性访问结构设置时,返回给用户解密令牌 *TK*,用户才能正确解密密文。运行令牌生成算法 TKGen,算法接收 *CT*,GPK_{uid},$SK_{uid,k}$ 作为输入,计算解密令牌 *TK*。

将解密令牌 *TK* 颁发给用户 *uid*。用户 *uid* 收到解密 *TK* 和用户的全局私钥 $GSK_{uid} = z_{uid}$ 解密密文,之后计算出用来解密数据的对称密钥 $key = CT/TK^{z_{uid}}$。最后访问者依据存储路径 $hash_{\text{IPFS}}$ 检索到数据文件 M_{se},根据对称密钥恢复出明文消息 $m = DEC(M_{\text{se}})$。

2.2.5 *访问撤销* 如果 AA_k 中的属性 $attr'_k$ 发生撤销,同时保证属性撤销后的前向安全和后向安全,属性撤销包括被撤销属性所在的 AA 更新密钥,未吊销的用户更新其密钥。通过更新与撤销属性相关的密钥组件、密文组件,无须变化密钥、密文的其他部分,提高属性撤销的效率。

3 实验与分析

3.1 安全分析

3.1.1 *抗攻击性* 本文所提方法可以有效地保证数据的隐私性和安全性。假设多个合谋用户共同合作,由于单一用户只持有交换密钥信息,每个合法用户在区块链上都有一个唯一的钱包地址用于标识其身份,且本文基于区块链的多授权机构访问方法中,不同授权机构 AA 独立设置和管理对应属性域 O_k,保证 $\forall i, j \in N, O_i \cap O_j \neq \varnothing, \Omega = \wedge O_k$,控制单个属性授权机构,只可颁发与范畴域对应的属性密钥,因此,用户合谋时无法获得来自其他属性授权机构的属性私钥组件 $\{attr_k\}$。假设存在来自一个合谋用户的私钥集合 $\{SK_{uid,k}\}$,由于合法用户的密钥集合均与 *uid* 相关,即 $TK(GPK_{uid}, SK_{uid,k}) \neq TK(GPK_{uid}, \{SK_{uid,k}\})$。数据的存储路径与数据关键信息 *keyWord* 相关,其中 *keyWord* 存储于区块链中,其含义与数据的关键查找信息相关,由于伪随机数函数 $H(m)$ 随机生成 *keyWord*,在不知道访问密钥对应数据信息的情况下,合谋用户恶意攻击时无法区分陷门 T_p 和 T_q 的输出,因此合谋用户的组合攻击无法

解密密文。同时数据加密没有使用系统内的唯一公钥进行加密,进一步避免了中心化管理密钥带来的隐私泄露的风险。对于所有的安全参数 $\lambda \in N$,运行 $KeyGen\ (1^{\lambda}) \rightarrow (GSK, GPK)$,在任意的多项式时间内,合谋用户伪造访问密钥的可能性是可以忽略不计的。因此,本方案可以抵抗恶意用户之间的合谋攻击,对比传统 CP-ABE[8] 和 CEC-ABE 方法[9] 保证了数据的安全性。

3.1.2 隐私性　一方面,区块链网络中用户的隐秘身份标识仅通过属性标识来访问数据,很大程度保护了访问数据的请求者在验证属性时的身份特性。在访问控制记录中使用匿名身份标识,隐藏了用户的隐私信息避免直接泄露真实身份。另一方面,大多数 CP-ABE 中访问策略或制定的属性集合公开透明,间接泄露了策略和数据隐私,降低了访问安全性。在本文方法中,基于策略矩阵 $\boldsymbol{\Gamma}(M, \rho)$ 进行密钥构件分发,只有满足关联属性集合 S 的用户能在多项式时间内恢复共享密钥。且在本文中密文不能直接获取,合法注册的用户经验证后,通过查询数据映射表披露数据信息描述部分,触发智能合约的查询和获取数据操作才能下载获取密文信息,而 CEC-ABE 方法[9] 通过边缘云服务器完成密文查询和解密。因此基于区块链实现访问记录透明的同时,又很好地保护了用户隐私。

3.1.3 完整性　在存储数据和设定访问结构后,为了验证数据的完整性,本文方法是在数据获取过程中执行智能合约的完整性检查,通过属性验证的用户从区块链中下载数据哈希摘要值,验证和检查数据的完整性。即使密文是在区块链上公开透明的,也能通过哈希摘要值验证数据完整性,检查有无非法的访问和篡改。

3.1.4 可追溯性　根据用户在区块链网络中注册的属性和标识被赋予全局唯一的标识符,用户的操作都通过区块链上事务触发操作记录在链上,同时包括密钥生成和使用,在区块链上都将被记录在一个可信任且不可篡改的访问日志中。由于区块链的公开和不可更改的特性,区块链上相关区块记载的历史记录可以被监管者进行检查,对比 CP-ABE[8] 和 CEC-ABE 方法[9],这进一步增强了访问流程的透明度和可追溯性。

3.2　仿真分析

通过仿真实验对基于区块链的共享数据模型进行性能测试,验证本文方案的高效性和正确性。本节仿真分析的操作系统为 Ubuntu 16.04,CPU 为酷睿 i7 9 代,主频为 2.60 Hz,内存为 16 GB,依赖配对的 JPBC(Java pairing-based cryptography library)函数库来实现本文算法,并利用 Solidity 编写的智能合约进行模拟实验。

实验中使用 MIMIC-Ⅲ临床试验数据库中的部分医疗数据集,模拟了基于区块链的多授权机构属性加密访问控制过程。针对方案存储性能,在本文 BC-DMAC 中,每个用户的存储开销来自 RA 颁发的全局密钥和 AAs 颁发的密钥。此外,服务器仅需存储公共参数。

实验首先分析智能合约执行中 *gas* 消耗,其值反映智能合约中执行代码和存储数据消耗计算资源的大小。由于需要在区块链上执行算法相关的必要函数,*gas* 的产生主要来源于函数执行复杂度与数据初始化和修改等操作。访问执行中用户注册合约和数据上传合约涉及对数据的读取和写入操作而产生较高的 *gas* 消耗,实际交易费用分别为 0.000 299 ETH,0.000 286 ETH,但数据访问合约借助数据哈希表明显降低了访问时的 *gas* 消耗,因此实际交易费用为 0.000 012 ETH。

为测试访问效率,实验中对属性授权机构数量、属性个数分别进行设置,在实际部署中固定涉及的属性授权机构数目为 10,测试属性数量对效率的影响。取多次测评结果并求平均值。系统初始化时间的比较如图 2 所示,系统初始化时间随属性授权机构管理的属性个数增加而增加,系统初始化时间不仅依赖于公共参数和主密钥的大小,还和属性数量相关,考虑到多个属性授权机构分别管理部分属性,本文方案与传统 CP-ABE 方案[8] 相比具有明显优势。

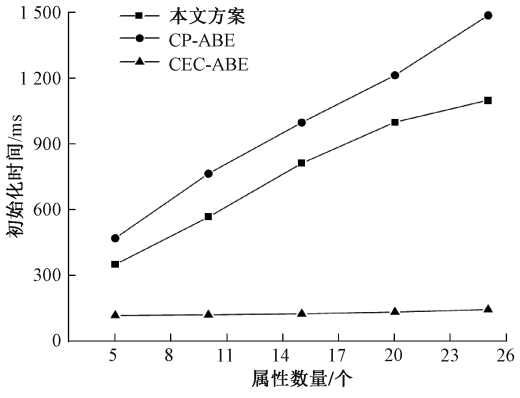

图 2　系统初始化时间比较

Figure 2　Comparison of system initialization time

加密时间的比较如图 3 所示,本文 BC-DMAC 方法使用的 CP-ABE 并没有直接对原数据进行加密,而是先进行 AES 对称加密,同时为了保持加密时间效率,利用 IPFS 存储方案,在加密中仅使用密钥加密,减少了文件大小,但 ABE 算法的访问机构

越复杂,细粒度访问程度越高。与CEC-ABE方案[9]相比,本文方案的计算成本平均降低了47.6%。

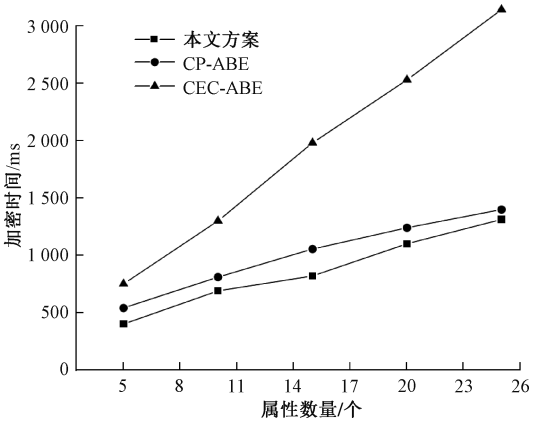

图3 加密时间比较

Figure 3 Comparison of encryption time

用户解密时间的比较如图4所示,解密时间随着访问控制策略中的属性个数的增加而增加,而本文方法所消耗的解密时间基本是恒定的,这是因为本文BC-DMAC方法在解密阶段数据分为解密令牌发放和令牌解密密文,用户只需持有令牌即可解密。因此耗时较少。仿真结果表明,本文方案在访问控制时产生较少的计算开销。

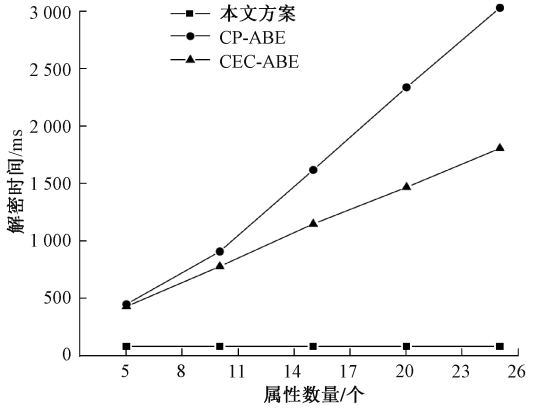

图4 用户解密时间比较

Figure 4 Comparison of user decryption time

密文更新时间的比较如图5所示。因密文中撤销的属性数量,直接关联到密文构件更新的范围,密文中含有的撤销属性数量越多,需要更新的密文越复杂。对比传统CP-ABE方法和CEC-ABE方法,本文BC-DMAC方法的密文更新时延在正常范围内,由此说明本文方法能在访问控制中实现属性撤销功能。

在正式解密之前增加了一个令牌授予过程,减少了用户方面解密时间,理论分析和实验结果表明,本文所提出的方法在保证安全的同时,能够提高访问效率。

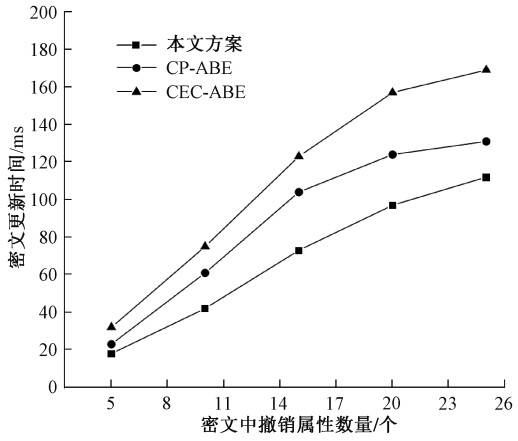

图5 密文更新时间比较

Figure 5 Comparison of ciphertext update time

4 结语

本文在传统属性加密访问控制方法的基础上,提出了一种基于区块链的去中心化多授权机构访问控制方法,相较于传统的属性加密访问控制,所提方法借助智能合约和分布式账本,安全地记录用户记录、权限记录和访问日志,从而实现访问授权和多方仲裁,且提高了访问授权效率,并通过安全分析和仿真分析证明了本文所提方法的有效性、安全性。下一步将重点考虑如何促进开放网络环境中动态灵活的访问授权。

参考文献:

[1] LI E, CLARKE J, ASHRAFIAN H, et al. The impact of electronic health record interoperability on safety and quality of care in high-income countries: systematic review[J]. Journal of medical internet research, 2022, 24(9): e38144.

[2] BONOMI L, HUANG Y X, OHNO-MACHADO L. Privacy challenges and research opportunities for genomic data sharing[J]. Nature genetics, 2020, 52(7): 646-654.

[3] HUANG C, LIU D X, NI J B, et al. Achieving accountable and efficient data sharing in industrial Internet of Things[J]. IEEE transactions on industrial informatics, 2021, 17(2): 1416-1427.

[4] GUPTA R, SINGH A K. Differential and access policy based privacy-preserving model in cloud environment[J]. Journal of web engineering, 2022, 21(3): 609-632.

[5] 董江涛, 闫沛文, 杜瑞忠. 雾计算中基于无配对CP-ABE可验证的访问控制方案[J]. 通信学报, 2021, 42(8): 139-150.

DONG J T, YAN P W, DU R Z. Verifiable access con-

trol scheme based on unpaired CP-ABE in fog computing [J]. Journal on communications, 2021, 42(8): 139-150.

[6] ZHENG T F, LUO Y C, ZHOU T Q, et al. Towards differential access control and privacy-preserving for secure media data sharing in the cloud[J]. Computers & security, 2022, 113: 102553.

[7] 陈英杰, 沈济南, 梁芳, 等. 医疗云环境下访问控制增强模型[J]. 郑州大学学报(理学版), 2022, 54(5): 49-56.
CHEN Y J, SHEN J N, LIANG F, et al. Access control enhancement model in the medical cloud environment [J]. Journal of Zhengzhou university (natural science edition), 2022, 54(5): 49-56.

[8] ZHANG W, ZHANG Z S, XIONG H, et al. PHASHEKR-CP-ABE: partially policy-hidden CP-ABE with highly efficient key revocation in cloud data sharing system[J]. Journal of ambient intelligence and humanized computing, 2022, 13(1): 613-627.

[9] JIANG Y, XU X L, XIAO F. Attribute-based encryption with blockchain protection scheme for electronic health records [J]. IEEE transactions on network and service management, 2022, 19(4): 3884-3895.

[10] JIN H, LUO Y, LI P L, et al. A review of secure and privacy-preserving medical data sharing [J]. IEEE access, 2019, 7: 61656-61669.

[11] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
LIU M D, CHEN Z N, SHI Y J, et al. Research progress of blockchain in data security [J]. Chinese journal of computers, 2021, 44(1): 1-27.

[12] 刘炜, 盛朝阳, 佘维, 等. 基于智能合约的分类分级属性访问控制方法[J]. 计算机应用研究, 2022, 39(5): 1313-1318.
LIU W, SHENG Z Y, SHE W, et al. Classified and hierarchical attribute access control method based on smart contract[J]. Application research of computers, 2022, 39(5): 1313-1318.

[13] 巩坪, 王九如, 宋万水, 等. 基于智能合约的物联网权限传递访问控制模型[J]. 郑州大学学报(理学版), 2023, 55(3): 28-33.
GONG P, WANG J R, SONG W S, et al. Access control model of Internet of Things based on smart contract[J]. Journal of Zhengzhou university (natural science edition), 2023, 55(3): 28-33.

[14] 牛淑芬, 陈俐霞, 李文婷, 等. 基于区块链的电子病历数据共享方案[J]. 自动化学报, 2022, 48(8): 2028-2038.
NIU S F, CHEN L X, LI W T, et al. Electronic medical record data sharing scheme based on blockchain[J]. Acta automatica sinica, 2022, 48(8): 2028-2038.

[15] LIU H, HAN D Z, LI D. Fabric-iot: a blockchain-based access control system in IoT[J]. IEEE access, 2020, 8: 18207-18218.

[16] WANG Y T, SU Z, ZHANG N, et al. SPDS: a secure and auditable private data sharing scheme for smart grid based on blockchain[J]. IEEE transactions on industrial informatics, 2021, 17(11): 7688-7699.