基于策略和属性隐藏的区块链访问控制方法研究

杨志谋[1]，文　强[1]，张　帅[1]，张功国[2]，孙　锐[2]

（1. 中国人民解放军 31202 部队，广东　广州　510510；
2. 重庆邮电大学　通信与信息工程学院，重庆　400065）

摘　要：针对访问控制过程中缺乏对用户隐私保护的问题，提出了一种基于策略和属性隐藏的区块链访问控制方案。首先，基于 Hyperledger Fabric 平台编写访问请求、属性管理和策略管理链码，搭建基本的基于属性的访问控制模型，实现了细粒度的访问控制。其次，使用 AES 对称加密算法和属性基加密算法将资源进行加密存储，再将存储地址和资源哈希上传到区块链上，确保数据的安全性和完整性。最后，使用 Paillier 同态加密算法将用户属性和访问策略加密并上传到区块链上，确保访问过程中用户的隐私安全。通过方案对比和仿真实验说明了本文方案能够有效保护用户的隐私。

关键词：区块链；访问控制；隐私保护；加密算法

中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097－1788. 2023. 10. 007

引用格式：杨志谋，文强，张帅，等. 基于策略和属性隐藏的区块链访问控制方法研究［J］. 网络安全与数据治理，2023，42(10)：40－48.

Research on blockchain access control methods based on policy and attribute hiding

Yang Zhimou [1]，Wen Qiang [1]，Zhang Shuai [1]，Zhang Gongguo [2]，Sun Rui [2]

(1. 31202 Unit of People's Liberation Army，Guangzhou 510510，China；2. School of Communication and Information Engineering，Chongqing University of Posts and Communications，Chongqing 400065，China)

Abstract：Aiming at the lack of privacy protection in the process of access control，an access control scheme based on blockchain policy and attribute hiding is proposed. Firstly，access request，attribute management and policy management chain codes are written based on Hyperledger Fabric platform，and basic attribute based access control model is built to achieve fine-grained access control. Secondly，the AES symmetric encryption algorithm and attribute-based encryption algorithm are used to encrypt resources for storage，and then the storage address and resource hash are uploaded to the blockchain to ensure the security and integrity of the data. Finally，the Paillier homomorphic encryption algorithm is used to encrypt and upload user attributes and access policies to the blockchain，ensuring the privacy of users during access. Through comparison of schemes and simulation experimental results，it is proved that this scheme can effectively protect user privacy.

Key words：blockchain；access control；privacy protection；encryption algorithm

0　引言

随着通信技术、云计算和物联网等技术的飞速发展，大量的数据产生并存储在了互联网上，这些数据可能涉及用户的个人隐私，一旦泄露将会对用户安全造成巨大的威胁[1-2]。访问控制技术作为保护数据安全的重要技术之一[3]，其通过预设的访问策略能够有效防止未经授权的访问和不当的使用。目前主流的访问控制方案分为基于角色的访问控制（Role Based Access Control，RBAC）[4]、基于权能的访问控制（Capability Based Access Control，CapBAC）[5]、基于属性的访问控制（Attributes Based Access Control，ABAC）[6]和基于属性基加密（Attribute Based Encryption，ABE）[7]的访问控制。其中，属性基加密以属性作为决策要素，通过与、或、非和门限操作能够制定细粒度的访问控制策略，实现从一对一加密到一对多加密的提升，使得它在数据发布和数据共享方面具有良好的应用前景。

属性基加密将密文和密钥与访问控制结构和属性联系起来，根据不同的两两对应关系，属性基加密又被分

为密钥策略属性基加密（Key-Policy Attribute-Based Encryption，KP-ABE）[8-9]和密文策略属性基加密（Ciphertext-Policy Attribute-Based Encryption，CP-ABE）[10-11]。在KP-ABE中，访问控制策略是嵌套在密钥中，该策略由一组属性组成，只有拥有与密钥策略匹配的属性集合的用户才能解密和访问数据。这种方法通常用于数据发布场景，例如医疗数据、社交网络数据等数据发布场景。在CP-ABE中，访问控制策略嵌套在密文中，当数据被加密时，需要指定与访问控制策略匹配的属性集合。只有拥有该属性集合的用户才能解密和访问数据。因为访问控制策略是嵌套在密文中的，只要用户拥有对应的属性集合就能解密，因此一般应用于数据共享场景，例如云存储、云计算等数据共享场景。总而言之，CP-ABE被认为是更加适合于数据共享中的访问控制。

然而，传统的访问控制方案都依赖于一个可信的第三方来决策，意味着所有的权限分配都由可信实体进行，这导致整个系统容易发生单点故障且透明度较低的问题。为了解决这一问题，不少研究提出以区块链取代中心化机构进行访问控制。区块链作为一个去中心化的分布式账本，最早由中本聪[12]于2008年在文章《比特币：一个点对点的电子现金系统》中提出。区块链根据去中心化程度的不同被分为公有链、私有链和联盟链三类，而联盟链因其能够兼具去中心化和交易速度快这两个优点而得到更加广泛的使用。

除此之外，在CP-ABE方案中访问策略往往是以明文进行存储的，其涉及了用户的隐私。其他用户可以通过访问结果来推测出用户的属性，这将间接地造成用户的隐私泄露。而且，传统的CP-ABE加密算法中，随着属性值的增多和文件大小的增大，公钥的大小和算法的复杂度也将增大，这将不利于现实场景下的应用。

本文提出了一种基于属性和策略隐藏的区块链访问控制方案。首先，通过Hyperledger Fabric联盟区块链平台来解决传统CP-ABE方案中依赖中心实体造成的单点故障问题。然后，针对区块链的透明性会造成用户隐私泄露的问题，提出通过同态加密算法将访问策略和属性进行加密，再使用区块链上的智能合约进行验证，以确保访问结果的可靠性和隐私的安全性。针对CP-ABE方案中公钥随着文件的增大而增大的问题，提出先用对称加密算法加密明文数据，再使用CP-ABE加密对称密钥，以此来提高加解密效率。最后，通过分析系统的性能，证明了本文方案的可行性和高效性。

1 相关工作

访问控制技术通过提前制定访问控制策略来预防不符合要求的访问请求，防止数据遭到窃取。但是，越来越复杂的网络环境给访问控制技术带来了新的挑战，如何提高访问控制技术以适应当今时代的发展受到了研究人员的关注。

文献［13］中，作者通过以太坊平台实现了去中心化的访问控制模型，并通过智能合约实现了高效的用户角色和角色权限管理，还设计了威胁和安全模型来抵抗攻击。文献［14］中，作者通过以太坊平台实现了RBAC模型，并以智能合约技术实现了跨组织的角色利用。文献［15］中，作者提出一种基于分散权能的访问控制框架（IOT Consortium Capability-based Access Control Model，IOT-CCAC），使用区块链技术解决传统方案中集中式的问题，并减少了授予和撤销权能时的时间损失。文献［16］中，作者为了解决访问控制系统仍然存在容易混淆权能授权主体、不灵活的权能授予和撤销、不安全的权能转移和缺乏权能验证等问题，提出了基于能力、区块链的细粒度和灵活的访问控制，定义了新的能力授权规则，并设计了具有能力撤销列表的授权树，以满足能力撤销的灵活性和及时性的需要。文献［17］中，作者为物联网系统提出了一种基于属性的访问控制方案，由属性认证机构根据身份或能力发布属性，通过区块链记录属性分布，并简化了访问控制协议。文献［18］中，作者提出了基于急救属性的访问控制方案，该方案能够在治疗期间快速授予急性护理团队访问权限，同时在治疗结束后立即撤销，以便在急性护理生命周期期间与适当的医疗保健专业人员共享患者数据。RBAC、CapBAC和ABAC这三类模型均能在一定程度上实现有效快速的访问控制，但是在这三种访问模型中数据均以明文形式进行存储，用户对数据的掌控有所欠缺。

在属性基加密（Attribute-Based Encryption，ABE）的过程中，数据均由数据拥有者制定访问策略并进行加密处理，极大地提高了用户对数据的掌控力度。因此，大量的研究人员在基于属性基加密的访问控制方向进行研究。文献［19］中，作者提出了使用半可信云服务器来完成复杂的、开销较大的解密计算工作的方案。该方案使得资源受限的设备能够利用计算消耗很大的ABE机制的优势。该过程依赖于从用户的密钥生成转换后的密钥，然后由半可信云服务器使用。在文献［20］中，作者提出了一种用于物联网环境的具有三因素身份验证的细粒度匿名用户访问控制方案，支持多权限ABE，并限定密文和密钥的大小来降低存储压力。

除此之外，为了解决方案中的中心化问题，提出引用区块链技术来实现去中心化的访问控制。文献［21］中，作者提出一种结合基于属性的加密和Hyperledger区

块链网络技术的架构，以提供对数据的细粒度访问控制。在文献［22］中，作者为了减少用户端的计算开销，整个访问过程被分为链上和链下两部分。链上部分负责处理用户的访问请求，进行预解密（返回由对称密钥加密的中间密文），确保解密的正确性。为了鼓励用户通过区块链发起访问，作者还设计了一个信誉计算模块。链下部分根据预解密结果继续解密从而获得最终的明文。在文献［23］中，作者通过 shamir 加密算法来解决属性管理中单点故障的问题。通过 shamir 秘密分享算法将属性交给多个机构共同管理，同时通过区块链网络来解决各个属性管理机构间的交互问题，保证了访问控制过程中的安全性和可靠性。

为了解决访问控制过程中的隐私泄露问题，在文献［24］中，作者提出了一种策略隐藏的访问控制方法，在区块链中进行参数生成、密钥验证和访问控制，并通过混淆的方法实现策略隐藏。文献［25］中，作者提出通过隐藏向量加密定义最小授权集，在方案中添加了一个名为“转换步骤”的额外步骤，增加了一些计算成本。

综上所述，在目前的 RBAC、CapBAC 和 ABAC 三种模型中，属性、访问策略和数据均以明文形式进行存储，尽管能够实现快速的访问控制，但是缺乏对用户隐私的保护，给用户信息安全造成了巨大的威胁。而在基于属性基加密的访问控制过程中虽然实现了对数据的加密，但是属性和访问策略仍以明文形式进行存储验证。尽管在文献［24］和文献［25］中对属性和策略进行了加密处理，但效率较低。因此，针对以上问题，本文提出结合同态加密算法和 CP-ABE 加密算法将用户属性、访问策略和数据进行加密，实现了安全、高效的访问控制。

2　系统框架

本方案的系统架构如图 1 所示，主要分为五个部分，分别是资源拥有者、资源请求者、区块链网络、存储机构和属性认证机构。

资源拥有者：资源拥有者是指持有数据资源的实体。资源拥有者若想要分享自己的资源可以设置基于属性的访问策略，只有匹配该访问策略的资源请求者才能获得该数据。访问策略被保存在区块链网络中。在具体的访问策略中，属性值和访问策略均经过加密处理。

资源请求者：资源请求者是指对某个数据拥有者所持有的某个数据发起访问请求的实体。资源请求者本身具有一系列的属性，再通过区块链网络发起访问请求后，

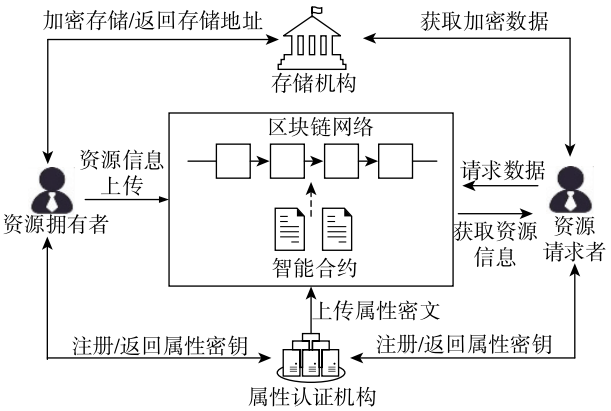


图 1　系统框架

区块链上的智能合约根据访问策略对其属性进行验证，决定是否授权访问。

区块链网络：区块链网络由多个对等的节点搭建而成。区块链网络定义了相关的智能合约，资源拥有者调用智能合约上传自己设置好的访问策略，资源请求者调用智能合约请求访问数据。区块链上记录了所有的交易信息，整个过程是公开透明的。同时，区块链上所存储的访问策略和属性值均经过加密处理，其他用户无法获得访问策略和属性信息。

属性认证机构：属性认证机构是一个受信任的实体，向区块链中的资源拥有者、资源请求者的属性提供认证并进行加密上传到区块链。同时，其还根据用户属性产生用户的私钥来解密数据。

存储机构：存储加密后的资源数据，返回存储地址。

3　工作流程

3.1　策略和属性隐藏的访问请求流程

在大多数现有的基于区块链的 CP-ABE 方案中，访问策略和属性一般以明文的形式进行存储，只有满足访问策略的请求者才能获得对应的资源数据。但是，由于区块链透明的特性，直接在区块链上储存属性和访问策略将会造成隐私的泄露。这是因为除了属性，访问策略中同样隐含了用户的隐私，若访问策略能够被任何人随意获取，无论自身属性是否满足访问策略要求，同样可以从中获取一定的信息。例如，某患者将自己的医疗数据进行存储并将访问策略设置为 ID：abc or 职称：主任 and 科室：神经科。该策略表示只有神经科中 ID 为 abc 或职称为主任的医生能够访问该数据。从这个访问策略中就可以间接推导出该患者可能有精神方面的疾病。为了防止属性和访问策略被他人获取从而导致用户的隐私泄露，本方案采用部分隐藏的策略对属性值和访问策略进行加密处理，具体访问流程如图 2 所示。

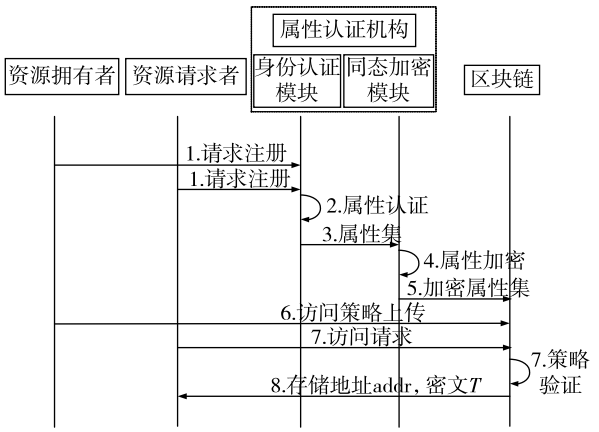


图 2　访问请求流程

（1）用户向属性认证机构发起注册请求，属性认证机构首先通过身份认证模块验证用户身份，并为其分配属性值，再通过同态加密模块加密用户属性集。同态加密模块首先计算属性值的哈希值 H，再通过 Paillier 加密算法加密哈希值 H 得到 H_{pk}，例如，用户具有如下的属性集合：

$$S=[(\text{position}),(\text{age}:B),(\text{ID}:C)] \tag{1}$$

经过加密之后上传到区块链上的属性集如下所示：

$$H(S)_{\text{pk}}=[(\text{position}:H(A)_{\text{pk}}),(\text{age}:H(B)_{\text{pk}}),(\text{ID}:H(C)_{\text{pk}})] \tag{2}$$

其中，$H()$ 表示哈希计算，$()_{\text{pk}}$ 表示 Paillier 同态加密。

（2）属性认证机构完成加密后，调用属性管理链码中的 AddAttribute 接口将用户的身份 ID 和加密后的属性值储存到区块链上。

（3）资源拥有者预设访问策略，并在本地进行加密，实现访问策略的隐藏。访问策略同样以同态加密算法进行加密并以布尔表达式的形式进行存储。访问策略的加密方式与属性的加密方式类似，对访问策略中的属性计算哈希值再使用 Paillier 加密算法加密。例如，下列的访问策略：

$$P=(\text{position}:A)\ \text{AND}\ ((\text{age}:B)\ \text{OR}\ (\text{ID}:D)) \tag{3}$$

经过加密处理后上传到区块链上的访问策略如下：

$$[H(P)+1]_{\text{pk}}=\{\text{position}:[H(A)+1]_{\text{pk}}\}\ \text{AND}\ \{\{\text{age}:[H(B)+1]_{\text{pk}}\}\ \text{OR}\ \{\text{ID}[H(D)+1]_{\text{pk}}\}\} \tag{4}$$

将访问策略加密后，资源拥有者调用策略管理链码中的 AddPolicy 接口将资源元信息和访问策略上传到区块链网络中，其中资源元信息包括资源 ID、资源哈希值、资源存储地址等。

（4）资源请求者按照资源 ID 调用属性验证链码中的 CheckAccess 接口发起访问。访问请求合约在收到访问请求后，会通过相应的接口获取到加密后的属性值和访问策略，根据访问策略中的属性名称找到用户的对应属性，利用加密算法的加性同态性质计算差值，如下所示：

$$\text{Res}=\{[H(A)+1]-H(A)\}_p\ \text{AND}\ \{[H(B)+1]-H(B)\}_p\ \text{OR}\ \{[H(D)+1]-H(C)\}_p \tag{5}$$

其中 AND 左右两边值相等且均为 $H(1)_p$ 时为 True，OR 则需要其中一边值为 $H(1)_p$ 时返回 True，否则返回 False。若验证通过则返回资源储存地址 addr 和密文 T，否则返回错误信息。至此，通过对属性和访问策略的加密，以及加密情况下的策略验证确保了整个访问请求流程中用户的隐私安全。

3.2　数据加密流程

该流程中资源拥有者通过 AES 对称加密算法将数据进行加密，再使用 CP-ABE 算法加密 AES 算法的密钥，这样通过 CP-ABE 算法加密的数据大小始终为 key 的长度，在加密较大的数据时性能也不会下降，最后将数据存储地址和加密后的 AES 密钥等上传到区块链。具体的数据加密流程如图 3 所示。

（1）运行初始化算法，向生成器中输入安全参数 k 来获得一组参数 (G_0, G_1, p, g)，其中，G_0 和 G_1 为阶数为 p 生成元为 g 的乘法循环群，p 为素数，e 为双线性映射 $e: G_0 \times G_0 \to G_1$。然后随机选择两个数 $\alpha, \beta \in Z_p$，另外对于每个属性 $i \in U$，随机选择 $h_1, h_2, \cdots h_U \in G_0$，最后通过式（6）和式（7）计算公钥 PK 和主密钥 MK。

$$\text{PK}=g,\ g^{\beta},\ e(g,g)^{\alpha},\ h_1,\ h_2,\ \cdots,\ h_U \tag{6}$$

$$\text{MK}=g^{\alpha} \tag{7}$$

（2）资源拥有者运行 AES 加密算法生成对称密钥 key 对数据 M 进行加密，得到密文 $T=\text{Enc}_{\text{AES}}(M)$。

（3）资源拥有者运行 CP-ABE 中的 LSSS 方案，设置访问策略 P 并将其转化为一个 $l \times n$ 的矩阵 $\boldsymbol{A}$，随机选择向量 $\vec{\nu}=(s, y_2, \cdots, y_n)$，对 $\boldsymbol{A}$ 的每一行 $\boldsymbol{A}_i$ 计算 $\lambda_i=\boldsymbol{A}_i \cdot \vec{\nu}$，最后得到密文 CT 如式（8）所示：

$$\text{CT}=\begin{pmatrix} C=\text{key}\cdot e(g,g)^{\alpha s},\ C'=g^{s}, \\ (C_1=g^{\beta\lambda_1}h_{\rho(1)}^{-r_1},\ D_1=g^{r_1}), \\ \cdots, \\ (C_l=g^{\beta\lambda_l}h_{\rho(l)}^{-r_l},\ D_l=g^{r_l}) \end{pmatrix} \tag{8}$$

其中，$r_1, r_2, \cdots, r_l \in Z_p$；$y_2, \cdots, y_n \in Z_p$；$\rho$ 表示一个映射函数，将 $\boldsymbol{A}_i$ 映射为对应的属性，等于 λ_i；s 为秘密值。

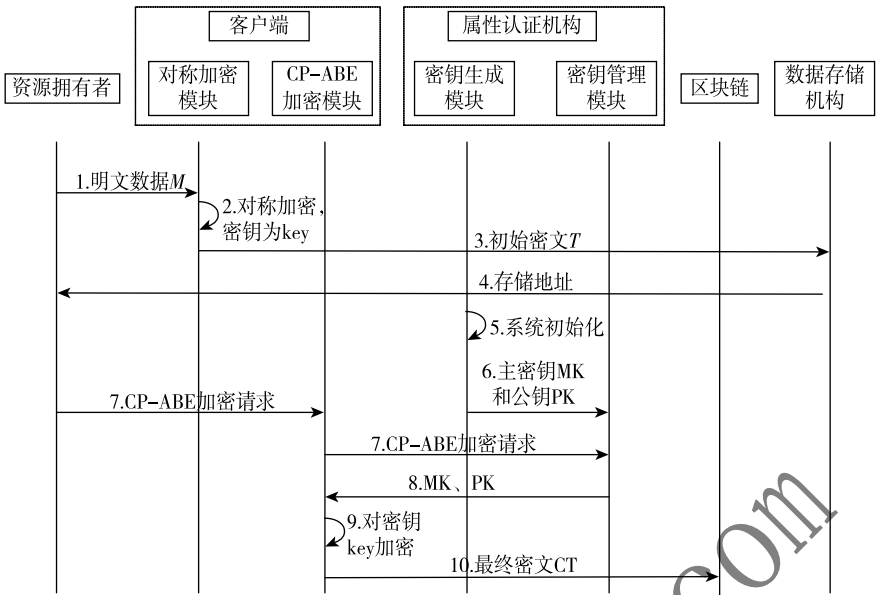


图 3　数据加密流程

（4）资源拥有者首先将 CT 存储到数据存储机构中，然后调用 AddFile 接口将加密后的访问策略 P、数据存储地址 addr 以及资源标识 id 等文件元信息上传存储到区块链上。

3.3　数据解密流程

资源请求者在通过访问请求流程获得了数据存储地址 addr 和密文 T 后，根据自身的属性获得对应的私钥 SK，通过 SK 解密 CT 得到对称密钥 key，再使用 key 解密 T 得到明文 M。具体解密流程如图 4 所示。

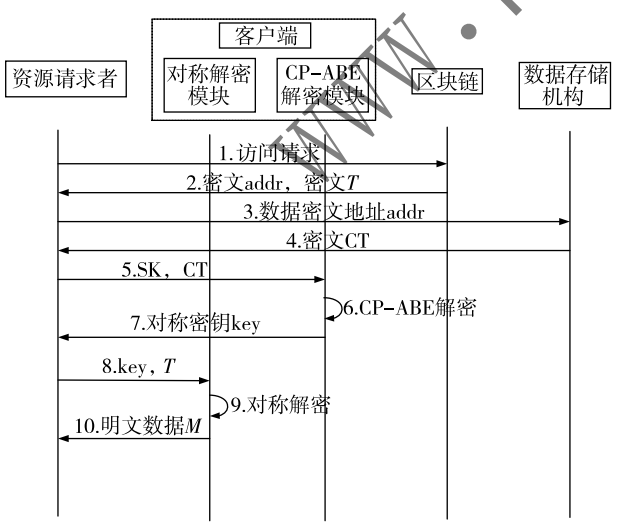


图 4　数据解密流程

（1）数据请求者向属性认证机构请求获得私钥 SK。

（2）属性认证机构根据资源请求者的属性集 S 通过式（9）计算得到私钥 SK：

$$\mathrm{SK}=\left(K=g^{\alpha}g^{\beta t},\ L=g^{t},\ \left\{K_x=h_x^{t}\right\}_{x\in S}\right) \tag{9}$$

其中，$t\in Z_p$；x 对应着属性集合里某一个属性，这个属性也可以用 $\rho(i)$ 表示。

（3）数据请求者根据访问请求流程中获得的存储地址 addr 获取密文 CT。

（4）数据请求者根据私钥 SK 解密 CT 得到对称密钥 key，如式（10）所示。得到密钥 key 之后，使用 AES 解密算法得到明文数据 M。

$$\mathrm{key}=C/e(g,g)^{\alpha s}=C/e(C',K)/\left(\prod_{i\in I}\left(e(C_i,L)\cdot e\left(D_i,K_{\rho(i)}\right)\right)^{\omega_i}\right) \tag{10}$$

其中，$\boldsymbol{\omega}_i$ 为一个向量使得 $\sum_{i\in I}\boldsymbol{\omega}_i\lambda_i=s$；$I\subset\{1,2,\cdots,l\}$ 且 $I=\{i:\rho(i)\in S\}$。

4　链码设计

链码是一个可以对账本数据进行操作的可开发的组件，可以通过编写不同的链码来实现业务逻辑。本文设计了策略管理链码、访问请求链码和属性管理链码三个链码来实现基于属性的访问控制，确保访问控制过程中的隐私保护和细粒度。

（1）策略管理链码（Policy Management Chaincode，PMC）：本文采用策略管理链码实现文件元信息和加密后的访问策略的上传、更新、删除和查询的功能。在策略管理链码中主要设计了以下四个接口来实现对应的功能：

AddPolicy：该接口将传入的资源存储地址 addr、资源哈希值 H（file）、资源 ID 和加密后的访问策略 P 储存到区块链中等待调用。

UpdatePolicy：该接口接收资源 ID 和新的访问策略

P，并根据资源 ID 和新接收的访问策略对旧的进行覆盖，以达到访问控制策略更新的效果。

DeletePolicy：该接口根据传入的资源 ID 删除对应的访问策略。

QueryPolicy：该接口根据传入的资源 ID 返回对应的访问策略，同时该接口被设置为无法由用户调用。

（2）访问请求链码（Access Request Chaincode，ARC）：访问请求链码将根据访问策略验证资源请求者的属性，并根据验证结果决定是否返回对应的文件元信息。该链码设计有如下接口：

CheckAccess：该接口根据传入资源 ID 和资源请求者的身份 ID 调用 QueryPolicy 和 GetAttribute 接口，分别获得访问控制策略和资源请求者的属性，然后逐一判断属性和策略是否匹配，若匹配则返回对应文件元信息给请求者，否则返回错误信息。

（3）属性管理链码（Attribute Management Chaincode，AMC）：主要负责接收属性认证机构发送的加密后的属性集，并储存到区块链上。该链码设计有如下接口：

AddAttribute：该接口会接收来自属性授权机构的用户 ID 和加密的属性集，并将其储存到区块链网络上。

UpdateAttribute：该接口会根据接收的用户 ID 和新的加密的属性集对旧的进行覆盖，以达到属性更新的效果。

DeleteAttribute：该接口将根据接收的资源 ID 删除对应的属性集。

QueryAttribute：该接口将接收用户 ID，并返回对应的属性集。

5　实验与分析

为了验证本文提出的基于区块链的策略和属性隐藏的访问控制方案的可行性，本文使用 Docker 技术和 Hyperledger Fabric 框架搭建了区块链平台。Fabric 区块链中包含两个组织，每个组织中各有一个排序服务节点和 Peer 节点。同时，使用两台主机分别担任数据拥有者和数据请求者。另外，实验中使用 JPBC2.0 库来实现 CP-ABE 的加密和解密流程。

5.1　系统性能

本文统计了策略管理链码、访问请求链码、属性管理链码在不同并发请求下的不同接口的时延情况，如图 5 所示，其中图（a）代表了策略管理链码中不同接口的时延，图（b）代表了属性管理链码中不同接口的时延，图（c）代表了访问请求链码中不同接口的时延。并发请求数被设置为 100、200、300、400 和 500。

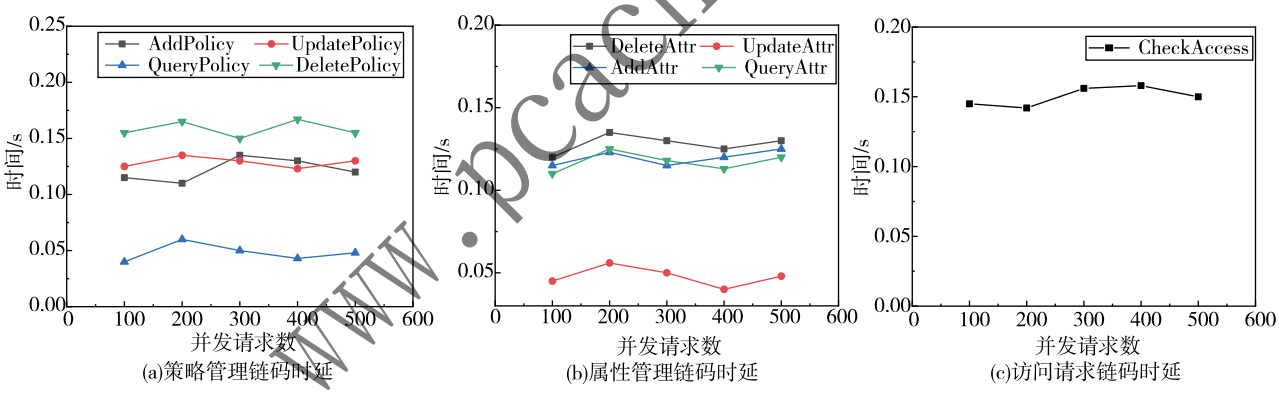


图 5　链码时延

其中，用户注册流程由属性管理链码实现，资源元信息上传流程由策略管理链码实现，访问请求流程则由访问请求链码实现。其中时延最高的两个接口分别是 CheckAccess 和 DeletePolicy 接口，平均时延在 0.15 s 以上，其余接口平均时延均在 0.15 s 以下。并且可以发现 AddPolicy、DeletePolicy、AddAttribute、DeleteAttribute 等写和删除操作的接口相较于 QueryPolicy、QueryAttribute 等读接口花费的时间更多。这是因为读、写和删除操作尽管都要通过索引值来获取数据，但是读操作在获取到数据后就可以将数据返回给用户，而写和删除则要对数据进行修改，修改后的数据将在通道内进行共享确保通道内节点间账本的一致性。

针对区块链上的访问流程对效率的影响进行实验。在本方案中，数据请求者需要通过区块链实现策略验证才能获得对应的密文和存储地址等。本文设计方案一进行对比，在方案一中访问请求者可以直接从区块链平台获得数据存储地址，而不用进行策略验证。如图 6 所示，本文方案在保护了用户隐私的同时在区块链上进行了策略验证，访问请求时延较方案一有一定的增加，但是仍在可接受范围内，且性能较为稳定。

5.2　方案对比

为了说明本文方案的优势，本文从存储开销、计算

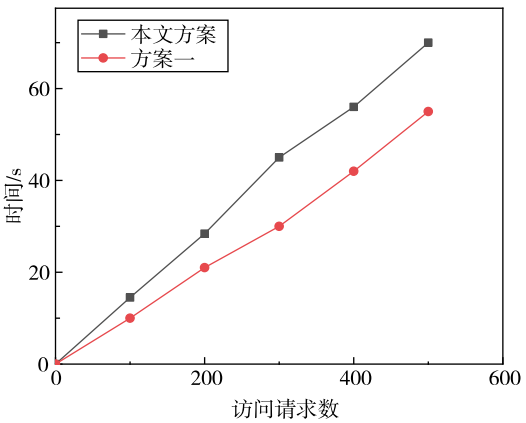


图 6　访问时延对比

开销、访问控制判决开销、面对不同大小文件和不同属性个数时的时延这几个方面与其他文献进行对比。

首先，本文将从数据加密存储、细粒度的访问控制、访问策略隐藏、是否依赖中央机构这四方面进行对比，结果如表 1 所示。

表 1　方案对比

方案	数据加密	细粒度	策略隐藏	区块链
文献［23］	√	√	×	√
文献［24］	√	√	√	√
文献［25］	√	√	√	√
本文	√	√	√	√

文献［23］通过 shamir 秘密分享算法将属性交给多个机构共同管理，解决了属性机构单点故障的问题，但是未考虑区块链环境下属性和策略隐藏的问题。文献［24］和文献［25］中所提出的方案实现了策略隐藏和去中心化。但是，文献［24］中采用了混淆的方法来实现策略隐藏，增加了计算的消耗。文献［25］中通过隐藏向量加密定义最小授权集，在方案中添加了一个名为“转换步骤”的额外步骤，增加了一些计算成本。本文方案以区块链取代中心化机构，对属性和访问策略进行同态加密，并在区块链上进行储存验证，确保了用户的隐私保护和访问控制中的安全性。

其次，为了说明本文方案在存储开销的优势，本文将比较本文方案与其他方案在 PK、MK、SK、CT 四部分中的存储开销，如表 2 所示。其中 PK、MK、SK、CT 分别表示公钥、主密钥、私钥和密文。本文使用 L_G、L_{G_i}、L_Z 来分别表示群 G、群 G_1 和 Z_N 的元素长度，使用 n 表示属性的数量，n_i 表示第 i 个属性的取值个数，使用 i 表示访问策略中的属性数量，I 表示用户的属性集合。通过横向比较可以看到，在获得相关安全特征的前提下，本文方案在 PK、MK、SK 和 CT 这四方面的存储开销均小于文献［24］和文献［25］。

然后，为了说明本文方案的计算开销，本文将本文方案与文献［24］和文献［25］在密钥生成、加密和解密方面进行对比，结果如表 3 所示。其中，e_0、e_1 表示在 G_0 和 G_1 上的指数运算，e 表示双线性对映射运算。从表 3 中可以看出，本文方案在密钥生成、加密和解密方面的计算复杂度均小于其他两个方案。

为了进一步说明本文方案在访问控制判决中的优势，本文对访问判决时的计算开销进行对比，结果如表 4 所示。其中 B 代表区块链共识开销，k 表示指数运算。

从表 4 可以看出，在不考虑区块链共识时延的影响下，文献［24］和文献［25］中的方案在进行访问控制判决时，要进行双线性对映射运算。而本文方案通过同态加密算法对属性和策略进行加密，在进行访问判决时只需要进行指数运算，计算消耗远小于其他两个方案，故本文方案能够实现高效的访问控制。

表 2　存储开销比较

方案	PK	MK	SK	CT
文献［24］	$(7+2n)L_G+2L_{G_1}$	~	$(I+2)\ L_G$	$(t\cdot n+1)\ L_G+L_{G_1}$
文献［25］	$(n+2)L_G+L_{G_1}$	$2L_Z+n\cdot L_G$	$10I\cdot L_G$	$3t\cdot L_G+L_{G_1}$
本文	$(n+2)L_G+L_{G_1}$	L_G	$(I+2)\ L_G$	$(2t+1)\ L_G+L_{G_1}$

表 3　计算开销比较

方案	密钥生成	加密	解密
文献［24］	$(I+2)\ e_0$	$(t\cdot\sum_{i=1}^{n}n_i+1)e_0+e_1$	$[1+t(\sum_{i=1}^{n}n_i+1)]e+[2+t(\sum_{i=1}^{n}n_i+1)]e_1$
文献［25］	$10I\cdot e_0$	$(5t+2)\ e_0+e_1$	$(2t+2)\ e+e_1$
本文	$(I+2)\ e_0$	$(2t+1)\ e_0+e_1$	$(2t+1)\ e+e_1$

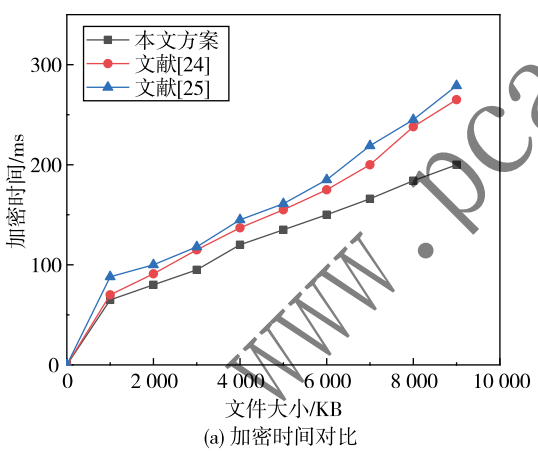
表 4　访问控制判决计算开销对比

方案	访问控制计算开销
文献［24］	$(1+t+t\cdot I)\ e+(2+t+t\cdot I)\ e_1+B$
文献［25］	$(3\sum_{i=1}^{n} i+\sum_{i=1}^{I} i)e+(1+\sum_{i=1}^{t} i)e_1+B$
本文	$k+B$

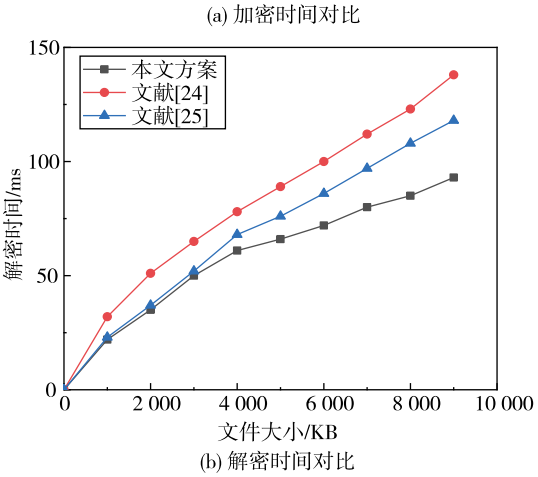
最后，为了说明本文方案在面对不同数据大小情况下的优势，本文方案将与文献［24］和［25］不同大小文件的加密和解密时延进行对比，并控制 3 种方案的属性个数不变，均设为 3 个属性，结果如图 7 所示。

从图 7 可以看出，本文方案在文件大小较小时加解密时延与文献［24］和［25］中的方案相差不大，但随着文件大小继续增大，本文方案的加密和解密时间更低，明显小于文献［24］和［25］中的方案。

为了说明访问策略中的属性个数对加解密时延的影响，将文件大小固定为 1 000 KB，本文方案与文献［24］以及文献［25］方案加密和解密时间对比，实验结果如图 8 所示。实验结果表明，3 种方案的加/解密时间均逐步增加，但本文方案的加密与解密消耗的时间最少。

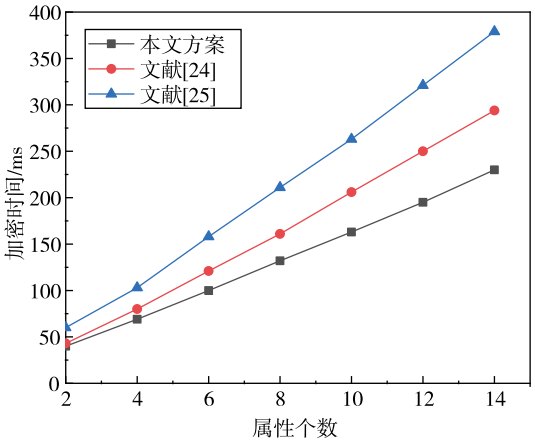


(a) 加密时间对比

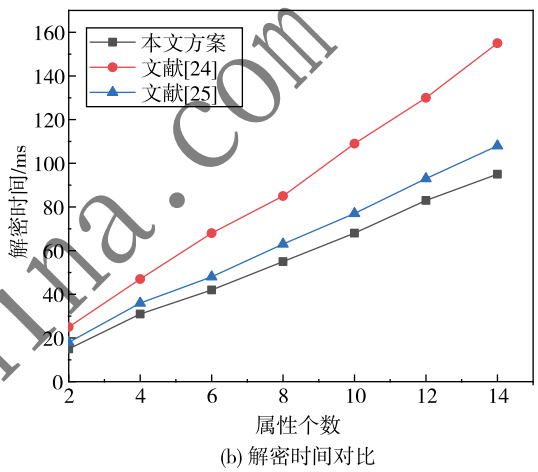


(b) 解密时间对比

图 7　不同文件大小的加/解密时间对比



(a) 加密时间对比



(b) 解密时间对比

图 8　不同属性数量下的加/解密时间对比

6　结论

本文针对传统的 CP-ABE 方案中存在的问题，利用区块链去中心化的特点，提出以区块链取代传统的中心化机构，使用同态加密算法保护用户隐私，并结合 AES 算法和 CP-ABE 算法降低系统开销。详细描述了所提出模型的系统框架、工作流程以及隐私保护措施。最后，基于 Hyperledger Fabric 框架和 JPBC 库实现了整个系统模型，并通过仿真实验和方案对比分析说明了本方案的可行性。

参考文献

［1］LIN J，YU W，ZHANG N，et al. A survey on internet of things：architecture，enabling technologies，security and privacy，and applications［J］. IEEE Internet of Things Journal，2017，4（5）：1125－1142.

［2］PALATTELLA M R，DOHLER M，GRIECO A，et al. Internet of things in the 5G era：enablers，architecture，and business models［J］. IEEE Journal on Selected Areas in Communications，2016，34（3）：510－527.

［3］史锦山，李茹. 物联网下的区块链访问控制综述［J］. 软件学报，2019，30（6）：1632－1648.

[4] FERRAIOLO D, CUGINI J, KUHN D R. Role-based access control (RBAC): features and motivations [C]//Proceedings of 11th Annual Computer Security Application Conference, New Orleans, 1995: 241 – 248.

[5] GUSMEROLI S, PICCIONE S, ROTONDI D. A capability-based security approach to manage access control in the internet of things [J]. Mathematical and Computer Modelling, 2013, 58 (5 – 6): 1189 – 1205.

[6] HU V C, FERRAIOLO D, KUHN R, et al. Guide to attribute-based access control (abac) definition and considerations (draft) [Z]. NIST special publication 800 – 162, 2013: 1 – 54.

[7] SAHAI A, WATERS B. Fuzzy identity-based encryption [C]// Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2005: 457 – 473.

[8] WANG C, LUO J. An efficient key-policy attribute-based encryption scheme with constant ciphertext length [J]. Mathematical Problems in Engineering, 2013, 2013: 1 – 7.

[9] HAN J, SUSILO W, MU Y, et al. Privacy-preserving decentralized key-policy attribute-based encryption [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23 (11): 2150 – 2162.

[10] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C]// SP'07: 2007 IEEE Symposium on Security and Privacy, 2007: 321 – 334.

[11] WANG H, ZHENG Z, WU L, et al. Adaptively secure outsourcing ciphertext-policy attribute-basedencryption [J]. Journal of Computer Research and Development, 2015, 52 (10): 2270 – 2280.

[12] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [J]. Decentralized Business Review, 2008: 21260.

[13] KAMBOJ P, KHARE S, PAL S. User authentication using Blockchain based smart contract in role-based access control [J]. Peer-to-Peer Networking and Applications, 2021, 14 (5): 2961 – 2976.

[14] SHARMA A, PILLI E S, MAZUMDAR A P, et al. Towards trustworthy Internet of Things: a survey on trust management applications and schemes [J]. Computer Communications, 2020, 160: 475 – 493.

[15] BOURAS M A, XIA B, ABUASSBA A O, et al. IoT-CCAC: a blockchain-based consortium capability access control approach for IoT [J]. PeerJ Computer Science, 2021, 7: e455.

[16] CHEN Y, TAO L, LIANG B, et al. Capability-&blockchain-based fine-grained and flexible access control model [J]. IEEE Network, 2023: 1 – 8.

[17] DING S, CAO J, LI C, et al. A novel attribute-based access control scheme using blockchain for IoT [J]. IEEE Access, 2019, 7: 38431 – 38441.

[18] DE OLIVEIRA M T, VERGINADIS Y, REIS L H A, et al. AC-ABAC: attribute-based access control for electronic medical records during acute care [J]. Expert Systems with Applications, 2023, 213: 119271.

[19] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of abe ciphertexts [C]//USENIX Security Symposium, 2011 (3): 34.

[20] BANERJEE S, ROY S, ODELU V, et al. Multi-authority CP-ABE-based user access controlscheme with constant-size key and ciphertext for IoT deployment [J]. Journal of Information Security and Applications, 2020, 53: 102503.

[21] ALNIAMY A, TAYLOR B D. Attribute-based access control of data sharing based onhyperledger blockchain [C]// Proceedings of the 2020 the 2nd International Conference on Blockchain Technology, 2020: 135 – 139.

[22] QIN X, HUANG Y, YANG Z, et al. LBAC: a lightweight blockchain-based access control scheme for the Internet of Things [J]. Information Sciences, 2021, 554: 222 – 235.

[23] QIN X, HUANG Y, YANG Z, et al. A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing [J]. Journal of Systems Architecture, 2021, 112: 101854.

[24] 林莉，储振兴，刘子萌，等. 基于区块链的策略隐藏大数据访问控制方法 [J]. 自动化学报，2022，49 (5)：1031 – 1049.

[25] ZHANG Z, ZHANG J, YUAN Y, et al. An expressive fully policy-hidden ciphertext policy attribute-based encryption scheme with credible verification based on blockchain [J]. IEEE Internet of Things Journal, 2021, 9 (11): 8681 – 8692.

（收稿日期：2023 – 07 – 06）

作者简介：

杨志谋（1979 – ），男，博士研究生，高级工程师，主要研究方向：运筹学、数据挖掘分析、数据信息安全、物联网安全等。

文强（1981 – ），男，硕士研究生，工程师，主要研究方向：目标分析、数据挖掘、数据信息安全等。

张帅（1993 – ），男，硕士研究生，工程师，主要研究方向：运筹学、数据挖掘分析、物联网安全等。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部