·热点与综述·　　文章编号：1000-3428(2023)08-0037-09　　文献标志码：A　　中图分类号：TP309.2

联盟链高效存储访问控制方案

黄保华，郑慧颖，屈　锡，陈宁江

（广西大学 计算机与电子信息学院，南宁 530004）

摘　要：联盟链平台上的超级账本Hyperledger Fabric提供了通道机制对数据进行隔离保护，但通道内部节点可随意获取链上数据且存在管理中心化的问题，使得联盟链面临数据泄露、访问权限无法更新等安全问题。为了解决以上问题，提出基于密文-策略属性基加密算法的联盟链高效存储访问控制方案。针对访问策略及节点权限更新问题，创建数据链和属性集链，实现数据链上所有节点的属性更新，利用数据库进行访问策略更新并存储访问策略的历史修改记录。修改Hyperledger Fabric提供的Fabric-CA组件，提高节点属性私钥生成与分发过程中的安全性。设计星际文件系统的存储数据分块优化和数据请求协商机制，并使用SM4算法加密数据，实现数据的高效安全存储。测试结果表明，与TABE-DAC方案相比，该方案的访问控制和数据存储时间分别降低了100~200 ms和1~2 s，在保证较高安全性的同时具有更高的运行效率。

关键词：联盟链；属性基加密；星际文件系统；访问控制；SM4算法

开放科学（资源服务）标志码（OSID）：

中文引用格式：黄保华，郑慧颖，屈锡，等.联盟链高效存储访问控制方案[J].计算机工程，2023，49(8)：37-45.

英文引用格式：HUANG B H，ZHENG H Y，QU X，et al.Efficient storage access control scheme for alliance chain[J].Computer Engineering，2023，49(8)：37-45.

Efficient Storage Access Control Scheme for Alliance Chain

HUANG Baohua，ZHENG Huiying，QU Xi，CHEN Ningjiang

（School of Computer and Electronic Information，Guangxi University，Nanning 530004，China）

【Abstract】The alliance chain platform Hyperledger Fabric provides a channel mechanism to isolate and protect data，but the nodes inside the channel can retrieve data on the chain at will and management is centralized，which means alliance chain faces security problems such as data leakage，confusion of node access rights，inability to update access rights，and centralization of data storage.To address the above issues，an efficient storage access control scheme for alliance chain based on Ciphertext-Policy Attribute-Based Encryption（CPABE）algorithm is proposed. To address the issue of updating access policies and node permissions，a data chain and attribute set chain are created to achieve attribute updates for all nodes on the data chain. A database is used to update access policies and store historical modification records of access policies.By modifying the Fabric-CA component provided by Hyperledger Fabric，the security of node attribute private key generation and distribution process is improved.In this scheme，the storage data partitioning optimization mechanism and data request negotiation mechanism of the Inter Planetary File System（IPFS）are designed，and the SM4 algorithm is used to encrypt the data，achieving efficient and secure storage of the data.The test results show that compared with the efficient Traceable Attribute-Based Encryption scheme with Dynamic Access Control based on blockchain（TABE-DAC）scheme，the access control and data storage time of this scheme are reduced by 100-200 ms and 1-2 s，respectively，ensuring greater security while maintaining higher operational efficiency.

【Key words】alliance chain；Attribute-Based Encryption（ABE）；Inter Planetary File System（IPFS）；access control；SM4 algorithm

DOI：10. 19678/j. issn. 1000-3428. 0064936

0　概述

区块链是一种多方参与、按照时间序列存储的分布链式结构的数据库，降低了信任成本，有效避免了中心化服务器单点崩溃风险，但在区块链上所有交易数据是公开的，可能导致用户隐私信息泄露。

基金项目：国家自然科学基金（61962005）。

作者简介：黄保华（1973—），男，副教授、博士，主研方向为信息安全、区块链技术；郑慧颖、屈　锡，硕士研究生；陈宁江，教授。

收稿日期：2022-06-09　　**修回日期：**2022-12-05　**E-mail：**bhhuang66@gxu.edu.cn

计算机工程 www.ecice06.com

为了确保隐私数据不被非授权者使用，须对区块链上的数据实施灵活的访问控制。超级账本Hyperledger[1]是一个由Linux基金会发起的区块链开源项目，致力于推进区块链数字技术和交易验证。Hyperledger Fabric提供了建立通道的功能，通过通道技术实现不同通道中数据的相互隔离，然而在这种机制下的区块链仍然存在安全风险。因为对于通道内的节点而言，链上数据是公开透明的，无法阻止数据的泄露，对于一些只能在小范围内公开的数据，Hyperledger[1]中利用数据对称加密上链、授权组织节点进行传递明文数据的解决方案仍存在密钥分发存储困难、访问控制粒度过粗等问题。若创建多个通道实现节点间的隔离，则会大幅增加通信时间消耗，降低获取数据的灵活性；若数据访问策略发生更改，则会增加通道内节点加入退出的时间消耗。

联盟链是由多个组织共同维护的小范围内公开的区块链系统。联盟链虽然限制了参与维护节点的范围，但是并不是所有数据都能够被所有节点访问。在实际应用中，各组织间不能达成互信，组织内员工的权限也是分级的且会发生变化，数据的访问权限也会发生变化。这使得数据的访问权限也须进行详细划分且支持更新，同时需要更快速高效的算法来提升工作效率。目前，联盟链访问控制方案采用的访问控制方案主要有传统和基于区块链的联盟链访问控制方案两种。传统联盟链访问控制方案主要包括基于角色的访问控制（Role-Based Access Control，RBAC）、基于属性的访问控制（Attribute-Based Access Control，ABAC）、基于使用控制（Usage CONtrol，UCON）模型的访问控制和基于权能的访问控制（Capability-Based Access Control，CapBAC）方案。基于区块链的联盟链访问控制方案有传统访问控制模型与区块链技术的结合方案、基于组策略的访问控制方案和基于智能合约的访问控制方案。但上述方案存在数据泄露、节点访问权限无法更新、数据存储中心化等安全问题。此外，星际文件系统（Inter Planetary File System，IPFS）也存在解析和下载瓶颈[2]、I/O操作高延迟等问题。

针对联盟链超级账本目前存在的访问控制、数据存储等问题，本文结合IPFS和联盟链，从优化IPFS存储性能和联盟链访问控制方法两方面出发，提出一个联盟链高效存储访问控制方案，根据部署在区块上的访问策略与访问节点的属性进行权限验证，利用IPFS实现数据分布式存储。

1 相关技术

1.1 区块链

区块链[3]使用加密技术保障信息安全，是一种由点对点网络（Peer to Peer，P2P）、加解密、分布式存储等技术融合而来的技术。根据区块链参与方数量和范围进行分类，区块链可以分为公有链、联盟链和私有链。联盟链是介于公有链和私有链之间的一种特殊的区块链类别，可以看作是特殊的私有链，是由多个组织共同维护的小范围内公开的区块链系统，为多个组织机构提供区块链服务。链上数据只能由这些组织控制的节点记录并获取，使得数据在可控范围内共享，且由于参与节点数较公有链少很多，因此交易速度较快。

JEMEL等[4]利用属性基加密（Attribute-Based Encryption，ABE）算法，通过节点验证访问者，在引入有生命周期的访问授权的同时不增加更新成本。YAN等[5]提出ANAC机制，利用授权用户与数据拥有者之间的关系来控制访问，设计门限秘密共享方案和通用访问结构，实现公证和自治。GAO等[6]采用策略和属性隐藏，通过ElGamal实现CP-ABE密钥获取中的隐私保护。徐俊伟等[7]通过优化Hyperledger Fabric联盟链平台超级账本中的Fabric-CA模块，实现CP-ABE中节点属性密钥的动态生成，对属性密钥使用非对称加密实现安全分发。汪金苗等[8]采用多授权中心的ABE方案，各授权中心负责生成部分属性对应私钥构件，且由多个节点轮流担任授权中心。然而，上述方案没有考虑用户属性更改后的数据访问权限更改问题，不支持属性更新。

YU等[9]使用一个可编辑的密钥链和一个标准的数据链，实现数据存储和访问控制管理的解耦，将变色龙哈希（Chameleon Hash，CH）集成到区块链，提出一种新的验证方案。邱云翔等[10]将访问策略与所有节点属性通过智能合约部署在区块中，解决权限集中的问题。上述方案针对区块链的访问控制问题，通过属性基加密方法实现细粒度访问控制，然而仍存在双链结构过于复杂、区块过多降低系统效率等问题。

1.1.1 Fabric-CA

Fabric-CA是实现Fabric中成员服务的组件，主要功能为：1）给各实体注册和登记身份；2）给各实体发放身份证书；3）给各交易发布交易证书；4）更新和撤销证书。

1.1.2 Fabric交易流程

Fabric交易流程如图1所示，具体步骤如下：

1）客户端（Client）调用成员服务注册、登记，获取身份证书。

2）客户端向区块链发送一个交易提案，将本次交易用到的合约相关参数和签名等信息发送给背书节点（Endorse Peer）。

3）背书节点在收到提案后，验证交易提案上的节点签名，并确定提交者是否有权限（此处调用访问控制方案），同时按照背书策略模拟执行，发送给客户端签名后的模拟结果。

4）客户端判断签名后的模拟结果与预期结果是否相同并确定是否根据该结果执行交易提案。如果结果不相同，则终止提案，否则继续将收到的结果打包签名发送给排序节点（Orderer）。

计算机工程 www.ecice06.com

5）排序节点验证背书节点签名，之后对交易进行排序，按照区块的生成策略，打包成区块，然后发给提交节点（Committer Peer）。

6）提交节点在收到区块后，校验区块中的交易，检查交易依赖的ReadSet和WriteSet是否与区块链世界状态一致，若一致，则将区块上链，并修改最新状态（所有键的最新值）。

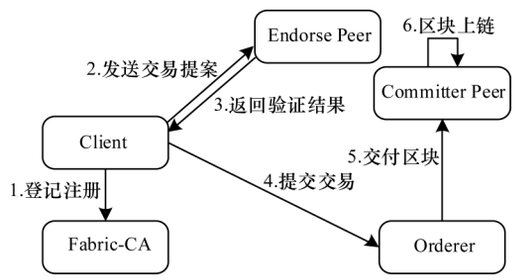


图1　Fabric交易流程

Fig.1　Fabric transaction process

1.2　属性基加密

ABE算法将属性集与访问策略加入用户私钥和密文中，解密过程就是属性集与访问策略匹配的过程，匹配成功即完成解密。ABE算法的优势为：与传统公钥加密算法不同，不需要留存每个用户的公钥，然后在加密得到各自的密文后分别发送给对应用户，这极大地减少了存储和计算时间。

ABE方案分为密钥策略属性基加密（Key-Policy ABE，KP-ABE）和密文策略属性基加密（Ciphertext-Policy ABE，CP-ABE）。KP-ABE方案对策略进行一系列的计算生成密钥，通过访问策略得到解密密钥。CP-ABE通过访问策略加密明文，对属性进行一系列的计算生成密钥，当且仅当访问策略与属性集相符时完成解密。因为在CP-ABE中，数据拥有者可以预设访问策略，使拥有对应属性的数据使用者才能访问数据，并提供属性级的访问控制粒度及数据加密存储与数据细粒度共享，适用于公有云环境。CP-ABE方案流程一般包括初始化、私钥生成、加密、解密等4个步骤，公式化描述如下：

1）$\mathrm{Setup}(1^{\lambda})\rightarrow(\mathrm{PK},\mathrm{MK})$：初始化函数，输入随机选取的安全参数，输出公共参数PK和主密钥MK。

2）$\mathrm{KeyGen}(A,\mathrm{MK},\mathrm{PK})\rightarrow(\mathrm{ABE}_{\mathrm{SK}})$：私钥生成函数，输入节点属性集$A$、主密钥MK和公共参数PK，输出节点属性私钥$\mathrm{ABE}_{\mathrm{SK}}$。

3）$\mathrm{Encrypt}(\mathrm{PT},P,\mathrm{PK})\rightarrow(\mathrm{CT})$：加密函数，输入明文PT、访问策略$P$和公共参数PK，输出密文CT。

4）$\mathrm{Decrypt}(\mathrm{CT},\mathrm{PK},\mathrm{ABE}_{\mathrm{SK}})\rightarrow(\mathrm{PT})$：解密函数，输入密文CT、公共参数PK和节点属性私钥$\mathrm{ABE}_{\mathrm{SK}}$，输出明文PT。

1.3　星际文件系统

IPFS由BENET[11]在2014年提出。DANIEL等[12]、HUANG等[13]和JOVOVIĆ等[14]对IPFS架构进行详细描述。VAGHELA等[15]将IPFS的存储地址存入区块链，保证数据的可信度和不可篡改性。IPFS在区块链中的应用可以减小区块链中存储的数据规模，将文件存储在无须信任的多个节点中，具备文件去重和查看文件历史版本的功能，有效避免了中心化存储存在的一些安全问题和限制，提升了服务效率，降低了服务成本。

IPFS的优势为：1）哈希值作为内容标识符（Content Identifier，CID）很容易实现数据完整性校验和检索；2）根据CID查找到数据后，直接计算数据哈希值，避免数据篡改；3）数据哈希值与数据是一一对应的，可以用来去除重复，减少存储浪费；4）多节点共同参与，避免单点故障，保护数据不易被丢失和损坏。

文献[16]使用面向代理的方法将IPFS和区块链相结合，并通过问答系统进行实现。文献[17]提出一个以患者为中心的框架，患者使用私钥解密病历记录，无须所有节点都存储完整的区块链，利用SHA-256获取文件在IPFS上的存储地址。文献[18]利用以太坊智能合约和代理重加密实现分布式的多方授权，引入声誉机制对节点进行行为评级，通过IPFS为代理提供加密的对称密钥和数据。文献[19]使用ABE、MA-ABE、IPFS和以太坊构建B-BOX存储系统，定义组织网络和区块链网络，一个组织可以加入组织网络并成为IPFS系统的一部分，具备去中心化、数据安全性、数据不可篡改性、对用户公开透明等特点。文献[20]利用IPFS保证数据安全存储，将具有多值属性的与门作为访问结构，可验证关键字搜索，提高搜索效率并跟踪病历来源，但不能撤销过期用户。文献[21]提出一种基于IPFS的区块链大数据存储方法，通过将大于100 MB的数据存储在IPFS上，解决区块链中大型文本数据的交易性能低下问题。文献[22]为医护人员提供了可在急救时获得患者病历的紧急访问机制，并利用IPFS存储URL和节点用于安全通信的公钥。文献[23]使用修改后的IPFS软件来强制执行预定义的访问控制列表，结合PKI和区块链技术来共享公钥和私钥。文献[24]提出设计准则以评估所考虑的不同技术的充分性，可辅助研发人员设计新的分布式系统。文献[25]提出一个基于超级账本的PCHDM框架，利用IPFS提高了可伸缩性和互操作性。但上述方案都只是对IPFS的应用，并没有提出对IPFS性能等缺陷的改进方法。

文献[26]研究IPFS结构，表明该结构在健壮性和抵抗Sybil攻击方面具有较大优势，但在性能和查询隐私方面有待改进。文献[27]阐述IPFS在隐私保护方面的局限性，用户可以付费使用IPFS提供的Pinning服务以固定重要数据来实现数据持久性，同时提高了数据检索速度。文献[28]评估IPFS在专用网络上的读写操作的性能和影响因素，指出影响写性能的因素主要是I/O磁盘操作，影响读性能的因素有网络通信、对接收到的数据块的本地处理和IPFS查找节点的时间，IPFS在大文件上的读写性能

计算机工程 www.ecice.com

有待进一步改进。文献[29]介绍IPFS核心特性,结合多种网络协议和P2P,为实现去中心化云存储奠定了基础,并指出IPFS尚未解决访问控制、激励、内容持久性和复制等问题。针对IPFS数据持久性和安全性保障机制的不足,文献[30]利用IPFS对文件访问控制进行优化,IPFS通过以太坊提供的接口发起交易,加入用户组来管理系统中的用户,利用目录管理文件更新,但该改进方案效率不高。

2 存储访问控制方案

所提方案通过优化CP-ABE算法实现联盟链的访问控制,并扩展实现属性更新、访问策略更新和密钥分发,进一步提升数据安全性。使用数据所有者(Data Owner,DO)预设的访问策略加密数据的相关信息,实现细粒度的数据访问控制,利用双层区块链架构的属性集链进行属性更新,对数据访问策略进行版本控制及数据库记录进行访问策略更新,修改Fabric-CA组件实现节点属性私钥的安全生成或分发。另外,所提方案利用IPFS实现数据存储,组建IPFS专有网络,编写智能合约,创建分块和协商机制实现对IPFS磁盘I/O效率和CPU时间等方面的性能优化。

IPFS存储原始数据密文,区块链上仅存储被CP-ABE算法加密后的原始数据的文件地址和数据哈希值。背书节点执行智能合约时,可向通道锚节点申请数据使用者(Data User,DU)的属性集对CT进行解密计算,若满足访问策略,则解密成功获取数据。

2.1 相关符号定义

相关符号定义如下:

1)$P=\{A\}=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}=(A,\rho)$,表示访问策略。

2)A,表示所有属性的属性集。

3)$A_i=(A_i,\rho)$,表示节点i的属性集。

4)$(i,(A_i,\rho))$,表示标识节点i或有相同权限等级的节点的元组。

5)KM,表示主密钥。

6)PK,表示系统公共参数。

7)$\mathrm{ABE}_{\mathrm{SK},i}$,表示属性为$A_i$的节点$i$的私钥。

8)m,表示DO上传的原始数据。

9)SK,表示加密原始数据的对称密钥。

10)$E_{\mathrm{sk}}(m)$,表示m被SK加密后的密文。

11)PT,表示待加密的消息明文。

12)CT,表示消息被加密后的密文。

13)A_{all},表示待更新节点属性集的集合。

14)Ucert,表示节点证书。

15)$\mathrm{Ucert}_{\mathrm{DO}}$,表示节点DO的证书。

16)P',表示更新的访问策略。

17)CT′,表示访问策略更新后的密文。

18)$(\mathrm{key}_{\mathrm{CT}},\mathrm{CT}')$,表示数据$m$对应的交易键值对。

19)Block,表示数据上链后的区块。

20)$\mathrm{Block}_{\mathrm{data}}$,表示更新了访问策略的区块。

21)$\mathrm{Block}_{\mathrm{attr}}$,表示更新了属性集的区块。

22)Tx(CT)和Tx(CT′),分别表示访问策略更新前后数据上链发送请求的交易。

23)$\mathrm{Tx}(\mathrm{CT}_{\mathrm{A}})$,表示属性集上链发送请求的交易。

24)CT_{A},待更新节点属性集的集合密文。

2.2 系统模型

访问控制方案的系统模型如图2所示。各节点的属性由联盟链中的管理节点组成的属性授权中心(Attribute Authority,AA)通过对属性集链的更新进行分配和管理。DO在上传数据到区块链上时,设定访问该数据的访问策略,将数据用SM4算法加密后存储在IPFS中,再使用CP-ABE算法对数据的对称密钥SK、哈希值和数据存储地址URL_m进行加密,计算密文。DO将密文通过调用智能合约上链,管理节点充当背书节点,对密文数据进行验证,并最终同步到各节点。DU使用智能合约从属性集链锚节点处,获取属性集链上的DU属性集,使用CP-ABE算法中的解密函数,判断DU的属性是否满足该数据的访问策略,若满足则DU解密得到相应的数据明文,否则不能得到数据明文。

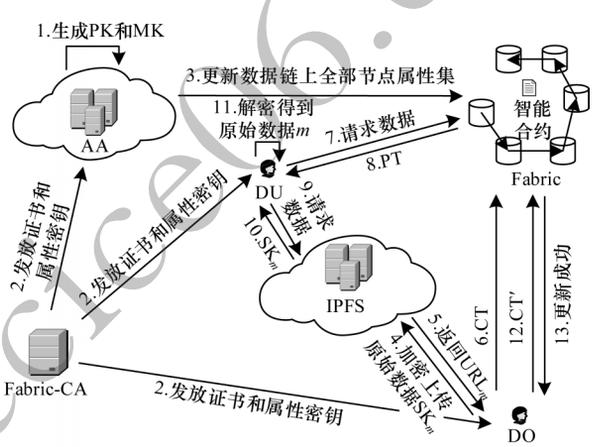


图2 访问控制方案的系统模型

Fig.2 System model of access control scheme

由Fabric-CA初始化生成并分发对应的证书,并且通过修改后的CA组件来生成和分发节点属性私钥。为每个组织创建一个成员服务提供者(Membership Service Provider,MSP),多个MSP共同组成Fabric-CA,避免成员管理中心化。对称加密后的数据存储在IPFS中,数据链上只存储被CP-ABE算法加密后的对称密钥、数据存储地址和数据哈希值,属性集的更新可以和数据链同步进行。

2.3 属性集及策略定义

为每一个组织创建一个MSP,多个MSP共同组成Fabric-CA。设计属性集结构为{组织,部门,小组,职位/工号},其中,职位/工号的选择由具体访问策略决定,将访问粒度控制在一小部分人或者一个人上。根据组织间和组织内部的合作情况定义某数

www.ecice06.com 计算机工程

据的访问策略，具体设置为：1）组织内用户均可访问该数据；2）某一组织的某个职位可以访问该数据；3）不同组织的特定小组可以访问该数据。

2.4　方案构造

访问控制方案主要分为初始化、数据加密上链、数据存储、访问控制、访问策略更新、属性集更新等6个阶段。

1）初始化阶段。该阶段调用Setup函数，由AA和Fabric-CA生成CP-ABE算法中的系统公共参数PK和算法主密钥MK，并根据节点登记注册请求生成节点证书Ucert和各节点的私钥$ABE_{SK,i}$，如图3所示。

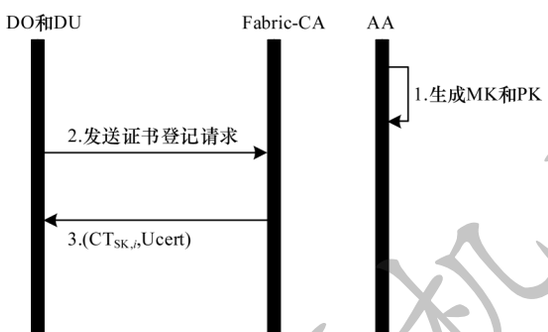


图3　初始化阶段流程

Fig.3　Process of initialisation phase

首先，节点向Fabric-CA发送证书请求，申请登记注册，在Fabric-CA收到请求后，生成该节点的证书Ucert和CBCP-ABE算法中所需的节点密钥$ABE_{SK,i}$。然后，使用Ucert中节点的公钥对节点属性私钥$ABE_{SK,i}$加密得到$ABE_{SK,i}$的密文$CT_{SK,i}$，返回(Ucert, $CT_{SK,i}$)给节点。最后，在节点收到(Ucert, $CT_{SK,i}$)后，用Ucert中的私钥进行解密，获得$ABE_{SK,i}$。

2）数据加密上链阶段。该阶段主要是DO与区块链系统进行交互，DO将原始数据m加密后上传到IPFS上，IPFS返回m的存储地址URL_m，然后指定访问策略P，使用CP-ABE加密函数将$PT=URL_m \| Hash(m)$加密后上链，如图4所示。

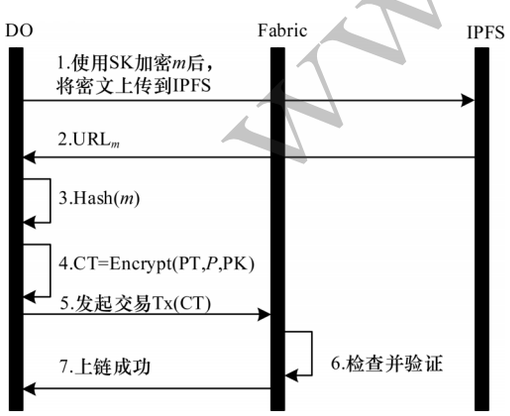


图4　数据加密上链阶段流程

Fig.4　Process of data encryption upload phase

3）数据存储阶段。该阶段主要是联盟链上DO和DU与IPFS网络之间的交互，DO将数据存储在IPFS上，IPFS使用分块机制，当数据大于50 MB且小于1 000 MB时将每10%的数据分为1个块，当数据大于1 000 MB时将每1%的数据分为1个块，用Merkle DAG生成数据最终的存储地址，并将存储地址发送给DO上链。DU从链上获得数据m经SM4算法加密后的密文$E_{SK}(m)$的存储地址后向IPFS网络请求$E_{SK}(m)$，IPFS节点向周围节点发送数据请求，拥有数据的节点返回响应，IPFS节点向最近的节点请求，对方返回$E_{SK}(m)$，IPFS节点将得到的$E_{SK}(m)$发送给DU。数据存储阶段流程如图5所示。

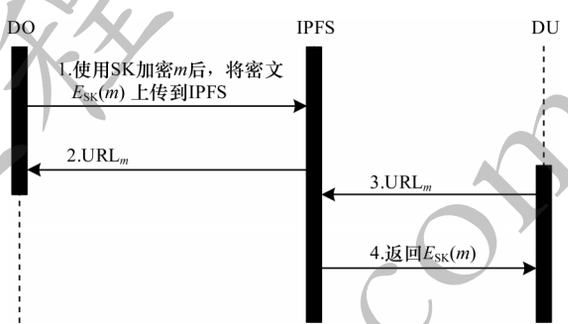


图5　数据存储阶段流程

Fig.5　Process of data storage phase

4）访问控制阶段。该阶段由DU与Fabric网络交互完成，通道内全部节点对新的交易进行同步后，DU向Fabric网络请求存储在区块链上的交易密文CT，先用证书私钥对$CT_{SK,i}$解密得到CP-ABE算法属性密钥$ABE_{SK,i}$，再调用Decrypt函数使用$ABE_{SK,i}$对密文CT进行解密。如果符合DO预设的访问策略P，则DU得到PT，从而获取存储在IPFS上的数据m的存储地址和对称密钥，实现细粒度的访问控制。访问控制阶段流程如图6所示。

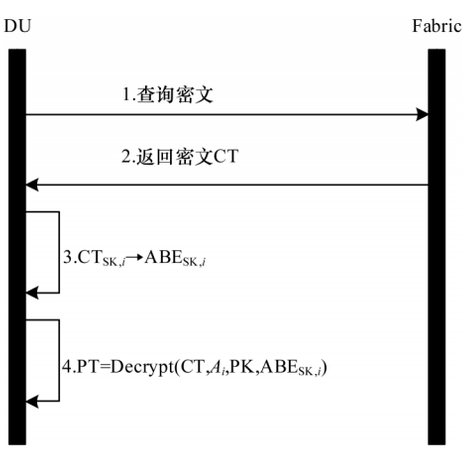


图6　访问控制阶段流程

Fig.6　Process of access control phase

5）访问策略更新阶段。该阶段是DO与数据链的交互，DO向数据链发送数据m的访问策略更新交易，数据链通过对状态数据库、历史状态数据库和账

计算机工程 www.ecice06.com

本索引数据库的更改，实现数据 m 的访问策略的更新，如图7所示。

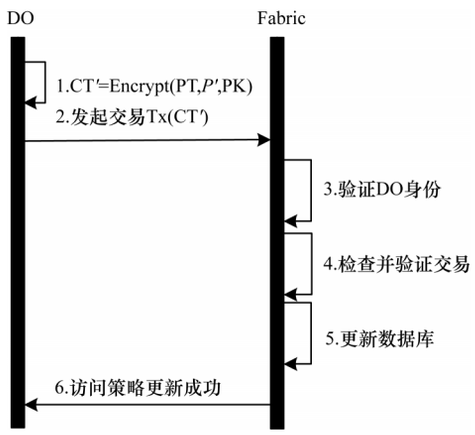


图7 访问策略更新阶段流程

Fig.7 Process of access policy update phase

6)属性集更新阶段。该阶段由联盟链中的管理节点与Fabric网络的交互实现，AA为管理节点组成的机构，通过为管理节点单独创建一条通道来管理数据链上节点的属性，如图8所示。

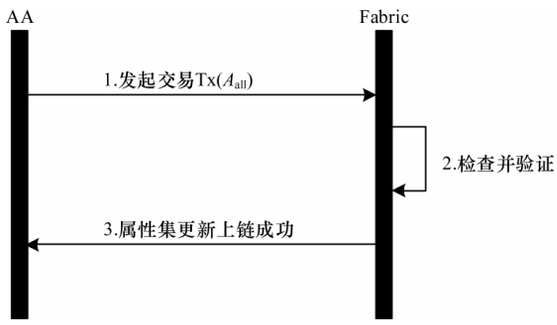


图8 属性集更新阶段流程

Fig.8 Process of attribute set update phase

原始数据 m 由DO经过SM4算法加密后存储至IPFS。智能合约从锚节点获取DU的属性集 A_i，利用 A_i 调用CP-ABE算法的解密函数计算CT。若能够获取区块上的数据CT，则DU的属性集 A_i 与该区块的访问策略匹配成功，获取原始数据的对称密钥SK、存储地址 URL_m 和哈希值，同时向 URL_m 指向的资源库请求数据，解密后获得原始数据 m 并与哈希值对比验证数据。数据访问控制流程如图9所示，其中，B为区块Block。

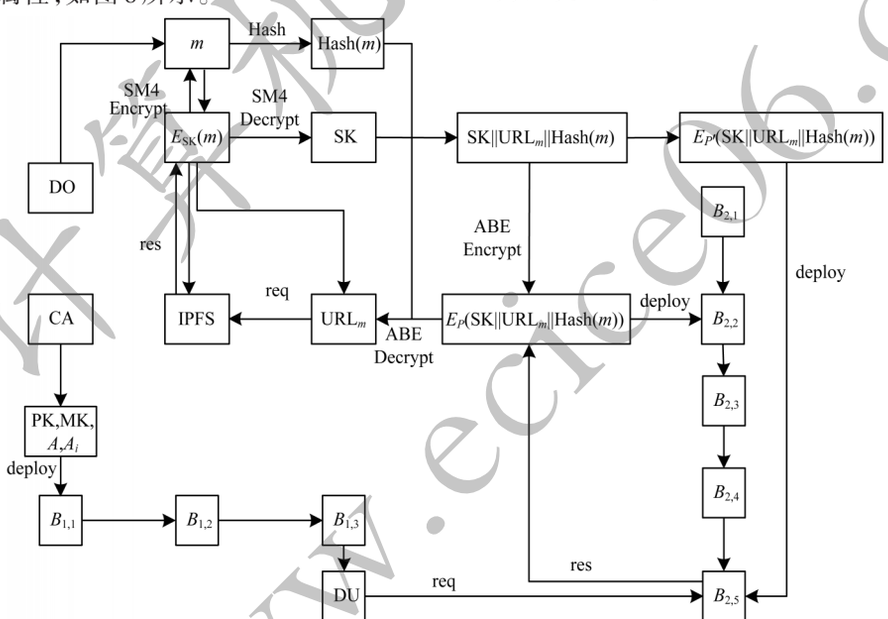


图9 数据访问控制流程

Fig.9 Process of data access control

3 安全性分析与性能测试

3.1 安全性分析

所提方案具有去中心化、不可篡改、数据隐私保护等安全特性。

1)去中心化

针对联盟链提出一个细粒度访问控制方案，利用智能合约将该方案部署至区块链，并使用IPFS进行数据分布式存储。联盟链由多个组织共同维护，具有弱中心化分布式的特点，结合IPFS的去中心化架构，有效降低了传统的集中式服务器单点故障和权限管理风险。

2)不可篡改

共同维护联盟链的多个组织拥有各自不同的需求，节点属性集单独上链由管理节点共同管理，结合区块链共识机制，如实用拜占庭容错(Practical Byzantine Fault Tolerance，PBFT)算法，当恶意节点小于(N−1)/3时，可以保持数据一致，防止节点属性被篡改等情况导致的安全隐患。联盟链上存储数据的哈希值和IPFS内容寻址哈希，获取数据后可以进行内容校验，保证数据不可篡改。

3)数据隐私保护

加密存储节点上链的原始数据，且IPFS采用分

www.ecice06.com 计算机工程

布式存储,利用分布式哈希表提升数据的处理效率,存储原始数据的密文,存储地址是该密文的哈希值,保证了密文的不可篡改和唯一性。为联盟链的节点创建一个专用IPFS网络,保证了只有在该专用网络中的节点才能获取IPFS中存储的数据,且保护了数据隐私。选取节点接入IPFS主网络,存在IPFS上的数据是由SM4算法加密后的数据,只有获取密钥才能得到明文数据,保障数据安全。

节点属性集的更新通过增加新通道,由管理节点负责更新,实现对属性集更小范围的访问,避免将属性集暴露给所有节点。访问策略更新过程和数据上链过程类似,通过存储数据的更新记录来实现访问权限的更新,每次访问数据查找到的都是最新版本的数据,保证了数据访问权限更新的实时性。

加密数据存储地址和原始数据的哈希值经过优化后的CP-ABE算法加密后上传至联盟链,只有属性符合访问策略的节点才能获得访问权限,在节点属性发生改变后节点无法凭借历史属性集继续访问数据,保证了数据的安全性和隐私性,实现了细粒度的访问控制。访问策略更新提升了链上数据的安全性,利用Fabric的交易流程进行改进,可减少区块链的处理消耗和存储压力。

4)节点属性私钥的安全分发

Fabric-CA组件是由超级账本提供的模块,使用的算法是安全可信的,对Fabric-CA组件进行修改优化,在完成对节点的登记注册操作的同时为节点生成属性私钥$ABE_{SK,i}$。利用节点生成过程中协商得到的公钥对属性私钥$ABE_{SK,i}$进行加密后安全传输给节点,节点使用对应的私钥获取$ABE_{SK,i}$,保证只有拥有对应私钥的节点才能成功解密得到明文数据,由此通过使用非对称密码算法,保证属性密钥的安全分发。

3.2　性能测试

实验包括数据上链、数据下载、访问策略更新、属性更新等4个功能模块的性能测试。实验操作系统Linux Centos 7.8,内存8 GB,以Hyperledger Fabric 1.0作为联盟链开发平台。系统所有节点运行在VMware Workstation的虚拟机上,在模拟实验中设置6个节点,由不同端口代表不同节点进行通信,在测试中记录了所提方案中数据上链、数据下载、访问策略更新、属性更新等4个功能模块的时间消耗。

数据使用者始终拥有自己上链数据的访问权限,在设置好数据的访问策略后将数据上链,此时不调用IPFS中的数据,而是直接从本地存储中获取数据。数据使用者向数据链发送请求,从IPFS网络中获取数据。

数据规模设定为1、10、100 MB,数据上链和下载的实验结果如图10、图11所示。数据上链和下载的时间主要受到数据规模的影响,随着数据规模的增加而增加。在实际应用中,需要根据数据规模调整分块机制以尽可能降低时间消耗。由图10、图11可以看出:所提方案相比于文献[30]方案上链时间消耗较少,且随着数据规模的增加,时间消耗差距加大;所提方案在数据规模较小时下载时间消耗较少,当数据规模为100 MB时接近于文献[30]方案的时间消耗。

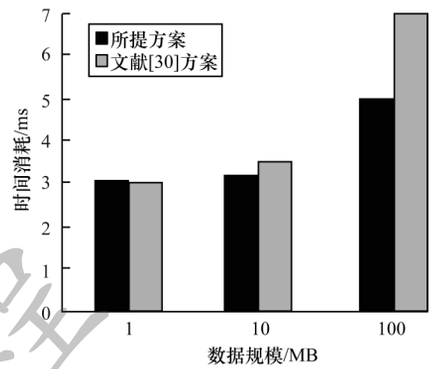


图10　数据上链的实验结果

Fig.10　Experimental result of data upload

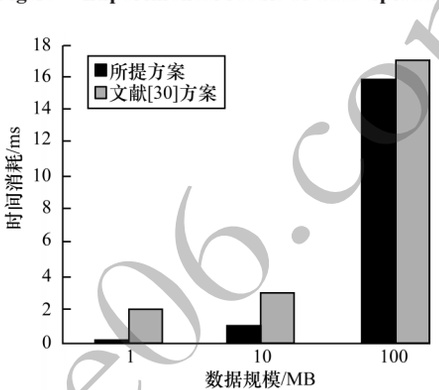


图11　数据下载的实验结果

Fig.11　Experimental result of data download

访问策略更新的实验结果如图12所示,通过新的访问策略加密将数据加解密的对称密钥SK、数据在IPFS上的存储地址URL_m和数据哈希值进行上链。由于处理的是固定长度的数值,因此主要受带宽、环境、距离等因素的影响。更新时间一般为1 100~2 100 ms,与数据链的读写时间类似。由图12可以看出,与TABE-DAC方案[31]相比,本文方案消耗时间较少。

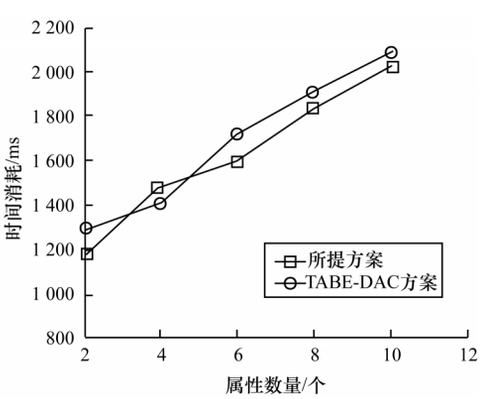


图12　访问策略更新的实验结果

Fig.12　Experimental result of access policy update

计算机工程 www.ecice06.com

所提方案将所有节点属性集单独存放在另一条链即属性集链上，属性更新就是将节点属性集加密后上链到属性集链的过程。属性集链由管理节点共同维护，与数据进行分离，因为每次访问数据都是访问最新区块的属性集，一般不进行溯源操作，所以省去了操作时间，同时也极大地方便了对节点属性的更新。属性更新分为属性集加密和属性集上链两部分。通过模拟属性集更新过程的各项指标的时间消耗如图13所示，在属性集链网络中节点个数为6，所有节点属性集规模分别设置为1 000、2 000、4 000、6 000、8 000时，属性集加密并上链过程的时间消耗在2 000 ms内，读取并解密的时间消耗在20 ms以内，时间消耗随着属性集规模线性提升。与文献[7]方案将属性数据部署在同一条链上相比，所提方案减少了算法加解密时间和属性集的查找时间，增加了与另一条链上锚节点获取属性集的通信时间，但是属性集链与数据链的更新可以同步进行，提高了方案整体效率。

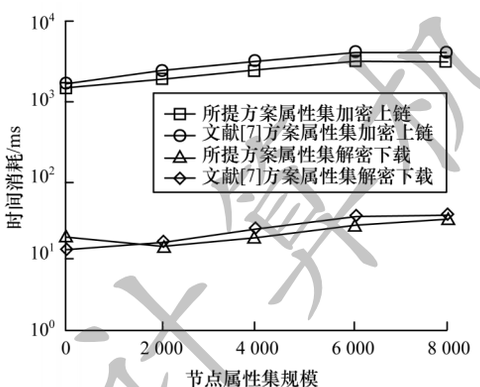


图13 属性集更新的实验结果

Fig.13 Experimental result of attribute set update

根据对联盟链数据存储访问控制系统4个主要功能的实验结果表明，随着数据规模的增加，数据上链下载时间会随之增加，当数据规模为100 MB时所提方案的时间消耗为5 s和16 s，而文献[30]方案在数据规模为100 MB时的上链下载到IPFS的时间消耗为7 s和17 s，由此得出所提方案数据存储时间降低了1~2 s、控制时间降低了100~200 ms。此外，访问策略和属性更新的数据规模都较固定，因此时间消耗变化不大。

综上所述，所提方案相比于现有方案考虑的问题更加全面，能够同时实现属性更新、密钥分发、访问策略更新和安全存储等功能，并且从链上和链下两方面出发，与Fabric功能特性结合更紧密，灵活性较强，适用于大部分应用场景。

4 结束语

本文提出一个联盟链高效存储访问控制方案。基于Hyperledger Fabric提供的联盟链架构，结合Fabric-CA组件实现密钥安全分发，并将节点属性集部署至区块链，达到快速处理恶意节点访问权限的目的。利用数据库记录版本更新实现访问策略更新，使用对称密码算法加密原始数据后存储至IPFS，并设计IPFS分块和协商机制及智能合约对数据进行细粒度的访问控制，保证数据隐私安全和提升数据存储效率。安全性分析与性能测试结果表明，该方案在保证数据安全访问存储的前提下，通过属性更新和访问策略更新实现灵活的联盟链上的数据访问控制。后续将从改进区块链处理速度、IPFS效率等方面出发，进一步提升对称密钥安全性和方案整体效率。

参考文献

[1] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the 13th EuroSys Conference. New York, USA: ACM Press, 2018: 1-15.

[2] SHEN J J, LI Y, ZHOU Y F, et al. Understanding I/O performance of IPFS storage: a client's perspective[C]// Proceedings of International Symposium on Quality of Service. New York, USA: ACM Press, 2019: 1-10.

[3] 张志威，王国仁，徐建良，等. 区块链的数据管理技术综述[J]. 软件学报，2020，31(9)：2903-2925.
ZHANG Z W, WANG G R, XU J L, et al. Survey on data management in blockchain systems[J]. Journal of Software, 2020, 31(9): 2903-2925. (in Chinese)

[4] JEMEL M, SERHROUCHNI A. Decentralized access control mechanism with temporal dimension based on blockchain[C]//Proceedings of the 14th International Conference on E-Business Engineering. Washington D. C., USA: IEEE Press, 2017: 177-182.

[5] YAN Z, GAN G H, RIAD K. BC-PDS: protecting privacy and self-sovereignty through blockchains for OpenPDS[C]// Proceedings of IEEE Symposium on Service-Oriented System Engineering. Washington D. C., USA: IEEE Press, 2017: 138-144.

[6] GAO S, PIAO G R, ZHU J M, et al. TrustAccess: a trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5784-5798.

[7] 徐俊伟，袁景凌，向广利. 可更新属性的链上数据访问控制方法[J]. 小型微型计算机系统，2023，44(2)：429-434.
XU J W, YUAN J L, XIANG G L. Data access control based on updatable attributes encryption[J]. Journal of Chinese Computer Systems, 2023, 44(2): 429-434. (in Chinese)

[8] 汪金苗，谢永恒，王国威，等. 基于属性基加密的区块链隐私保护与访问控制方法[J]. 信息网络安全，2020(9)：47-51.
WANG J M, XIE Y H, WANG G W, et al. A method of privacy preserving and access control in blockchain based on attribute-based encryption[J]. Netinfo Security, 2020(9): 47-51. (in Chinese)

[9] YU G S, ZHA X, WANG X, et al. Enabling attribute

revocation for fine-grained access control in blockchain-IoT systems[J]. IEEE Transactions on Engineering Management, 2020,67(4):1213-1230.

[10] 邱云翔,张红霞,曹琪,等. 基于CP-ABE算法的区块链数据访问控制方案[J]. 网络与信息安全学报,2020,6(3):88-98.
QIU Y X, ZHANG H X, CAO Q, et al. Blockchain data access control scheme based on CP-ABE algorithm[J]. Chinese Journal of Network and Information Security, 2020,6(3):88-98. (in Chinese)

[11] BENET J. IPFS-content addressed, versioned, P2P file system [EB/OL]. [2022-05-11]. https://arxiv. org/abs/1407. 3561.

[12] DANIEL E, TSCHORSCH F. IPFS and friends: a qualitative comparison of next generation peer-to-peer data networks[J]. IEEE Communications Surveys & Tutorials, 2022,24(1):31-52.

[13] HUANG H W, LIN J R, ZHENG B C, et al. When blockchain meets distributed file systems: an overview, challenges, and open issues[J]. IEEE Access, 2020, 8: 50574-50586.

[14] JOVOVIĆ I, HUSNJAK S, FORENBACHER I, et al. 5G, blockchain and IPFS: a general survey with possible innovative applications in industry 4. 0[C]//Proceedings of the 3rd EAI International Conference on Management of Manufacturing Systems. Dubrovnik, Croatia: EAI Press, 2018:157-158.

[15] VAGHELA A, SUTHAR A. A review of bigdata analysis using smart contract[EB/OL]. [2022-05-11]. https://www. researchgate. net/publication/350048650_A_REVIEW_OF_BIGDATA_ANALYSIS_USING_SMART_CONTRACT.

[16] TENORIO-FORNÉS A, HASSAN S, PAVÓN J. Open peer-to-peer systems over blockchain and IPFS: an agent oriented framework [C]//Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. New York, USA: ACM Press, 2018:19-24.

[17] REEN G S, MOHANDAS M, VENKATESAN S. Decentralized patient centric e-health record management system using blockchain and IPFS[C]//Proceedings of IEEE Conference on Information and Communication Technology. Washington D. C. , USA: IEEE Press, 2020: 1-7.

[18] BATTAH A A, MADINE M M, ALZAABI H, et al. Blockchain-based multi-party authorization for accessing IPFS encrypted data[J]. IEEE Access, 2020, 8: 196813-196825.

[19] PHAM V D, TRAN C T, NGUYEN T, et al. B-BOX: a decentralized storage system using IPFS, attributed-based encryption, and blockchain [C]//Proceedings of RIVF International Conference on Computing and Communication Technologies. Washington D. C. , USA: IEEE Press, 2020: 1-6.

[20] SUN J, YAO X M, WANG S P, et al. Blockchain-based secure storage and access scheme for electronic medical records in IPFS[J]. IEEE Access, 2020, 8: 59389-59401.

[21] TANG J, JIA T, CHEN H B, et al. Research on big data storage method based on IPFS and blockchain [C]// Proceedings of the 2nd International Conference on Video, Signal and Image Processing. New York, USA: ACM Press, 2020: 55-60.

[22] SABERI M A, ADDA M, MCHEICK H. Break-glass conceptual model for distributed EHR management system based on blockchain, IPFS and ABAC [J]. Procedia Computer Science, 2022, 198(C): 185-192.

[23] UDDIN M N, HASNAT A H M, NASRIN S, et al. Secure file sharing system using blockchain, IPFS and PKI technologies [C]//Proceedings of the 5th International Conference on Electrical Information and Communication Technology. Washington D. C. , USA: IEEE Press, 2022: 1-5.

[24] TENORIO-FORNÉS Á, HASSAN S, PAVÓN J. Peer-to-peer system design trade-offs: a framework exploring the balance between blockchain and IPFS [J]. Applied Sciences, 2021, 11(21): 10012.

[25] MANI V, MANICKAM P, ALOTAIBI Y, et al. Hyperledger healthchain: patient-centric IPFS-based storage of health records[J]. Electronics, 2021, 10(23): 3003.

[26] HENNINGSEN S, FLORIAN M, RUST S, et al. Mapping the interplanetary file system [C]//Proceedings of IFIP Networking Conference. Washington D. C. , USA: IEEE Press, 2020: 289-297.

[27] GUIDI B, MICHIENZI A, RICCI L. Data persistence in decentralized social applications: the IPFS approach[C]// Proceedings of the 18th Annual Consumer Communications & Networking Conference. Washington D. C. , USA: IEEE Press, 2021: 1-4.

[28] LAJAM O A, HELMY T A. Performance evaluation of IPFS in private networks [C]//Proceedings of the 4th International Conference on Data Storage and Data Engineering. New York, USA: ACM Press, 2021: 77-84.

[29] DOAN T V, PSARAS Y, OTT J, et al. Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations[J]. IEEE Internet Computing, 2022, 26(6): 7-15.

[30] LIN Y F, ZHANG C Y. A method for protecting private data in IPFS[C]//Proceedings of the 24th International Conference on Computer Supported Cooperative Work in Design. Washington D. C. , USA: IEEE Press, 2021: 404-409.

[31] GUO L F, YANG X L, YAU W C. TABE-DAC: efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain[J]. IEEE Access, 2021, 9: 8479-8490.

编辑 陆燕菲

计算机工程 www.ecice.com