计算机科学
COMPUTER SCIENCE

基于区块链的云上数据访问控制模型研究

童飞, 邵冉冉

引用本文

童飞, 邵冉冉. 基于区块链的云上数据访问控制模型研究[J]. 计算机科学, 2023, 50(9): 16-25.

TONG Fei, SHAO Ranran. Study on Blockchain Based Access Control Model for Cloud Data [J]. Computer Science, 2023, 50(9): 16-25.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230500239

基于区块链的云上数据访问控制模型研究

童　飞[1,2,3]　邵冉冉[1,2]
1 东南大学网络空间安全学院　南京 211189
2 教育部计算机网络和信息集成重点实验室(东南大学)　南京 211189
3 紫金山实验室　南京 211111

摘　要　区块链和基于密文策略的属性加密(Ciphertext Policy Attribute Based Encryption,CP-ABE)相结合的方案已经被广泛应用于云上共享数据的访问控制,但是这些方案中数据用户的隐私保护问题并未得到妥善解决。一些研究引入分布式多属性授权中心的基于属性的签名方案(Distributed Multi-Authority Attribute Based Signature,DMA-ABS)来保护数据用户的隐私,但当数据用户多次访问数据时需要进行重复的权限验证,这会带来多余的时间消耗问题。并且,在数据用户的属性和访问控制策略保持相对稳定的情况下,数据用户无限制地重复访问共享数据,会导致系统过载,影响正常的请求处理。这可能会引起云端数据的泄露,给云端数据的安全带来隐患。为了解决这些问题,文中提出了一个基于区块链的云上个人隐私数据访问控制方案。该方案首先将智能合约和多属性授权中心的 CP-ABE 方案结合,实现了云上个人隐私数据的细粒度访问控制,并引入 DMA-ABS 方案完成了对数据用户的匿名性身份验证,保护了数据用户的身份隐私;其次,基于比特币 UTXO(Unspent Transaction Output)机制,设计了一种数字令牌 token,实现了一次授权、多次访问的功能,即缩短了访问时间,又限制了访问次数;最后,在 Hyperledger Fabric 上进一步实现了访问控制流程,并与现有方案进行了访问时间开销的比较。实验结果表明,所提方案能够有效降低访问时间开销,提高访问效率。

关键词:区块链;访问控制;基于密文策略的属性加密方案;访问令牌;智能合约
中图法分类号　TP18

Study on Blockchain Based Access Control Model for Cloud Data

TONG Fei[1,2,3] and SHAO Ranran[1,2]
1 School of Cyber Science and Engineering,Southeast University,Nanjing 211189,China
2 Key Laboratory of Computer Network and Information Integration of Ministry of Education(Southeast University),Nanjing 211189,China
3 Purple Mountain Laboratories,Nanjing 211111,China

Abstract　The combination of blockchain and ciphertext policy sttribute based rncryption(CP-ABE) schemes has been widely used in the access control of sharing data on the cloud,but the privacy protection of data users in these schemes has not been solved. Some studies introduce distributed multi-authority attribute based signature schemes(DMA-ABS) to protect the privacy of data users,but when the data user accesses the data multiple times,it is necessary to perform repeated permission verification,which will cause unnecessary time consumption. And when the attributes and access control policies of data users are relatively unchanged,data users can access shared data repeatedly and infinitely,system overload and affect normal request processing. This may cause the leakage of cloud data, posing a hidden danger to the security of cloud data. At the same time,the behavior of data users changes dynamically. A data user who once perform well may have some malicious behaviors such as frequent access to data,illegal access to data,which brings hidden dangers to data security. Firstly,the smart contract is combined with the CP-ABE scheme of multi-attribute authority center to realize the fine-grained access control of personal privacy data in the cloud,and the distributed multi-authority attribute based signature scheme is introduced. The anonymous identity verification of data users is completed to protect the identity privacy of data users. Secondly,based on the idea of unspent transaction output(UTXO) of Bitcoin,the digital token is designed to realize once authorization and multiple access. Finally,this scheme implements an access control process based on hyperledger fabric,and compares it with existing schemes in terms of access time overhead. The results indicate that the proposed scheme can effectively reduce access time overhead and improve access efficiency.

到稿日期:2023-05-31　返修日期:2023-07-09
基金项目:国家自然科学基金(61971131);东南大学“至善青年学者”项目(2242021R41157)
This work was supported by the National Natural Science Foundation of China(61971131) and “Zhishan” Scholars Programs of Southeast University(2242021R41157).
通信作者:童飞(ftong@seu.edu.cn)

Keywords　Blockchain，Access control，Ciphertext policy attribute based encryption，Access token，Smart contract

1　引言

随着网络技术的快速发展，个人数据量迅速增长，云计算技术为个人数据的存储和共享提供了有效的方法，人们习惯将珍贵的照片、重要的文档等存储在云端。截至目前，全世界的数据信息存储量在飞速上升[1]，每时每刻都有大量的新数据存储在云端，云存储可以实现海量、低成本、低能耗的共享存储资源，但用户和云服务器之间缺乏信任，云服务器可能会泄露或篡改云上数据，同时云服务器也可能会受到攻击，存储在云上的个人隐私数据更易遭到窃取。例如，2019 年 7 月，美国资讯安全公司 Capital One 的云服务器被黑客攻击[2]，导致超过 1 000 万 Capital One 客户的个人信息遭窃，包括姓名、联系信息以及信用卡申请记录等；2022 年 7 月，日本 Kokikai Yasue 医院数据库被未经授权的计算机访问[3]，泄露了 111 191 名患者的姓名、地址、电话号码和医疗记录等隐私信息。云上海量个人隐私数据在存储和共享过程中的安全问题亟待解决。访问控制技术是保护数据隐私的重要技术之一，可以保证只有授权用户才有权限访问系统或者数据，防止数据被非法篡改或泄露。因此，如何实现安全、灵活的访问控制系统，以保障云上个人隐私数据的安全成为重要研究内容。

基于属性的加密方案（Attribute-Based Encryption，ABE）可以提供数据加密和细粒度访问控制方法[4-5]，来保证数据的机密性。ABE 中发送者设置访问策略加密数据，只有符合属性要求的接收者才能解密密文，得到数据。但是 ABE 方案无法支持灵活的访问控制策略。因此，一些学者在 ABE 方案的基础上提出了以下两类加密方案：基于秘钥策略的属性加密（Key Policy Attribute Based Encryption，KP-ABE）和基于密文策略的属性加密（Ciphertext Policy Attribute Based Encryption，CP-ABE）。其中 KP-ABE 将访问控制策略嵌入在密钥中，将文件属性嵌入到密文中，即密钥对应于一个访问控制策略，密文对应于一个属性集合。KP-ABE 中会为接收到消息的接收者分配一个特定的访问策略，因此 KP-ABE 多适用于静态场景，如付费视频网站和日志加密管理等；CP-ABE[6] 中的密文对应于一个访问策略，密钥对应于一个属性集合，所以数据发送者可以设置密文的访问策略，当接收者的属性满足此访问策略时才能解密成功，获得共享数据。这种设计更接近于现实中的应用场景，适合于消息分发和共享场景，更适合本文研究的云上个人隐私数据共享场景。

CP-ABE 可以保证存入云上的数据被加密，并且数据共享者只需要设置访问策略，执行一次加密即可。当用户拥有的属性符合加密者所描述的策略时，用户就可以解密。由此，实现了一对多的云上数据访问控制，解决了对称加密传输带来的密钥泄露问题，提高了数据共享效率。但是单一属性授权中心 CP-ABE 方案[7] 中需要一个可信第三方管理属性和属性密钥，这会带来单点故障问题。因此，研究者[8-9] 引入多个属性授权中心来代替单一的属性授权中心，提出了多属性授权中心的 CP-ABE 方案，解决了单一属性授权中心带来的单点故障问题。但是仍存在以下问题：数据用户（Data User，DU）在属性和策略不变的情况下，可以无限制地访问共享数据，导致系统过载，影响正常的请求处理；需要一个集中式服务器来完成访问控制处理和授权，易产生单点故障问题；数据所有者（Data Owner，DO）将数据上传到云端后就无法完全控制 DU 对数据的访问。

具有去中心化、不可篡改和可追溯等特性的区块链技术[10]，可以在多个属性授权中心（Attribute Authorization Center，AA）之间构建信任，并取代集中式服务器，实现去中心化的访问控制和管理，从而提高访问控制的安全性和灵活性。同时，区块链是公开透明的，因此可以利用 CP-ABE 加密数据存储在区块链上，保护数据的隐私，实现用户可控的细粒度访问控制系统。

本课题的主要意义在于对基于区块链的云上个人隐私数据访问控制系统进行研究，结合区块链和多属性授权中心的 CP-ABE 方案，设计了一个云上数据共享更安全、更灵活的访问控制模型。

2　相关工作

2.1　基于 CP-ABE 的访问控制研究

为了实现云上数据的安全共享，实现对加密数据的高效访问控制以及云上共享的个人隐私数据的保护，研究者们提出了基于 CP-ABE 的访问控制技术。

文献[11]将共享医疗数据用 CP-ABE 加密后存储在云端，只有具有符合访问策略的属性的用户才可以解密密文，保护了数据安全，并实现了细粒度访问控制。文献[12]将 CP-ABE 的加解密操作外包给可信云服务器进行计算，依赖于云服务器的可信性，一旦云服务器被攻击或者存在恶意行为，则可能会导致数据泄露或者其他安全问题。这些 CP-ABE 方案中存在单一的属性授权中心，这会带来单点故障问题，并且在实际应用中可能会涉及许多属性。由单一属性授权中心统一管理不符合实际，因此一些研究将单个属性授权中心的工作划分给多个属性授权中心，解决了系统性能瓶颈问题。文献[13]设计了多属性授权中心，以减轻单一属性授权中心的压力，并在设计方案中实现了外包加解密和属性撤销功能。

但在这些研究中，DO 一旦将数据共享到云端就失去了对数据的控制权，并不了解数据的被访问情况，且上传到云端的数据可能会被篡改，无法保证其数据完整性。并且这些方案需要一个集中式服务器来完成访问控制处理和授权，易产生单点故障问题。

2.2　基于区块链的访问控制研究

区块链技术的可追溯性、不可篡改性和公开性为云上个人隐私数据的安全共享提供了新方法。

目前已经有许多将区块链技术和 CP-ABE 加密机制结合的研究。文献[14]改进了 CP-ABE 算法，引入审计员，利用区块链实现分布式数据共享和公开审计方案。但其引入了可信代理服务器，带来了单点故障的风险。文献[15]将电子医疗数据存入云服务器，将索引保存在联盟链上以保护云上数据的完整性，并结合属性加密和内容提取签名来实现数据的

隐私保护。文献[16]利用智能合约分发私钥，避免 DO 和 DU 之间的直接交互，使用区块链避免可信第三方依赖，但所有数据都在区块链上公开可见，未能保护数据用户隐私。文献[17]将 CP-ABE 方案中的属性映射到属性令牌中，具有相应属性令牌的用户在消耗属性令牌后被授予对加密数据的访问和解密权限，但是在系统框架中存在可信第三方承担了属性私钥生成功能，存在单点故障问题。文献[18]为避免不可信属性授权中心由数据拥有者生成密钥，利用智能合约分发、管理密钥，但这又会给 DO 带来巨大的计算负担。因此这些方案并不能保证数据用户的身份隐私。

为保护数据用户的隐私和匿名性，文献[19]提出了一种无中央机构的分布式多属性授权中心的基于属性的签名方案(Distributed Multi-Authority Attribute Based Signature, DMA-ABS)，可以在验证方不知道签名者具体身份属性的情况下，验证签名者的身份属性是否满足具体的访问策略，保护数据用户身份属性隐私。文献[20]将 CP-ABE、DMA-ABS 和区块链相结合，实现细粒度访问控制并保护了数据用户隐私，但是该系统中所有的属性均由单个属性授权中心管理，存在单点故障风险。文献[21]将 Multi-authority CP-ABE、DMA-ABS 和区块链相结合，保护数据的完整性、机密性和可访问性，由多属性授权中心代替单一属性授权中心。但在这些研究中 DU 每次访问数据都要基于 DMA-ABS 对 DU 的身份进行验证，这会带来较多的时间开销，并且当属性和访问策略相对不变时，DU 可以无限制访问共享数据，导致系统过载，可能造成系统崩溃，带来数据安全问题。

综上所述，目前较少研究综合考虑 DU 身份属性隐私保护、动态授权 DU 访问权限、控制 DU 访问次数等问题。

3 预备知识

3.1 访问控制结构

1996 年，Beimel[22]定义了访问控制结构，即设 $P=\{P_1, P_2, \cdots, P_n\}$是一个由 n 个参与者组成的集合，访问控制结构 $A\subseteq 2^P$是 P 的非空子集组成的集合，在集合中的元素为已授权的集合，不在集合中的元素为非授权集合。现在关于 CP-ABE 的研究中，大多采用访问控制树或者线性秘密共享来表示访问控制结构。

3.1.1 访问控制树

在 CP-ABE 的访问控制树中，树形结构可以表示访问控制策略，访问控制树隐藏加密密钥，树的内部节点表示与、或、门限操作，叶子节点表示 DO 的属性和属性值。

生成访问控制树需要经过以下步骤。

1)访问控制策略建模：DO 根据需要的访问控制策略，构造一个访问控制属性表达式。

2)属性-节点映射：针对访问控制属性表达式，根据一定的映射规则，将属性映射成访问控制树上的节点。

3)访问控制树构建：构建访问控制树，并将属性节点嵌入树中。

4)树节点加密：从根节点开始，对于每个非叶子节点，根据其属性表达式生成一组公私钥对，将公钥嵌入到该节点中。

5)对于每个叶子节点，用其属性生成一个私钥，并将其与访问控制树中的所有公钥结合进行加密。

当 DU 请求访问加密数据时，需要经过以下步骤。

1)访问请求构造：DU 构造一个包含自己属性的访问请求。

2)访问控制树遍历：DU 从根节点开始，依次遍历访问控制树，并根据自己的属性信息选择对应的子节点。

3)解密：当 DU 到达叶子节点时，使用该节点的私钥结合所有已选中的其他节点进行解密。

3.1.2 线性秘密共享方案

访问控制结构还可以由线性秘密共享方案(Linear Secret Sharing Scheme, LSSS)构造。LSSS 可以将秘密分割成多个部分并分配给多个参与者，并确保只有在满足特定条件时才能重构秘密。LSSS 可以保护敏感信息不被恶意攻击者访问，同时确保数据的可用性和完整性。

本文将使用 LSSS 访问矩阵来实现访问策略，具有一些参与者 P 的秘密共享方案 Π 在满足以下两个条件时是线性的：

1)每个参与者在 Z_p 上形成一个向量。

2)存在一个 m 行 d 列的共享矩阵 $\boldsymbol{A}$ 与访问结构$(\boldsymbol{A},\rho)$相关联。$\boldsymbol{A}$ 中的第 i 行由参与者 $\rho(i)$签名，其中 ρ 表示从$\{1, 2, \cdots, m\}$到 P 的映射函数，该映射函数将矩阵 $\boldsymbol{A}$ 的每一行映射到一个属性，$i=1, \cdots, m$。设列向量 $\boldsymbol{v}$ 表示为$(s, y_2, \cdots, y_d)$，其中 $s\in Z_p$ 表示要共享的秘密值，$y_2, \cdots, y_d$ 是 Z_p 中的多个随机数。然后，根据 $\boldsymbol{A}$ 计算 $\boldsymbol{A}\cdot\boldsymbol{v}$ 来分享秘密值 s，即通过映射函数 $\rho(i)$，每个参与者 $p_i\in P$ 都拥有一个共享组成 $\lambda_i=(\boldsymbol{A}\cdot\boldsymbol{v})_i$。

每个 LSSS 可以按照以下方式进行线性重构。假设存在与访问结构$(\boldsymbol{A},\rho)$相关联的 LSSS 矩阵 $\boldsymbol{A}$。S 表示一个授权集合，$I\subset\{1, \cdots, m\}$可以定义为 $I=\{i:\rho(i)\in S\}$。可以构造多个常数$\{w_i\in Z_p\}$，满足 $\sum_{i\in I} w_i\boldsymbol{A}_i=(1, 0, \cdots, 0)$。如果$\{\lambda_i\}$是根据$(\boldsymbol{A},\rho)$的任意秘密值 s 得到的有效份额，那么就可以通过 $\sum_{i\in I} w_i\lambda_i=s$ 重构秘密值 s。

3.2 CP-ABE

传统的 CP-ABE 方案中存在一个单一 AA，它负责管理所有的属性并生成相关属性密钥。DO 设置访问策略加密文件生成密文后，将密文上传到云服务提供商(Cloud Service Provider, CSP)中，DU 可以从 CSP 上获得密文。此时，满足访问策略的 DU 就可以用其属性私钥解密获得 DO 共享的文件，但是该方案中存在单点故障问题。且在实际工作中，属性很多，单个访问结构难以管理。因此，本文参考 2020 年 Okamoto 提出的多属性授权中心 CP-ABE 方案[23]，通过引入多个 AA，来代替单个 AA 管理用户属性，以解决上述问题。多属性授权中心 CP-ABE 方案由以下 5 个函数组成。

1)$GlobalSetup(\lambda)\rightarrow GP$：给定安全参数 λ，生成全局公共参数 GP。

2)$AuthoritySetup(GP, AA_{id}, i)\rightarrow(APK_i, ASK_i)$：输入全局公共参数 GP、AA 在系统中的唯一标识为 AA_{id} 和每个 AA 管理的属性 i，生成自己的公钥 APK_i 和私钥 ASK_i。

3)$Encrypt(GP, M, (\boldsymbol{A},\rho), \{APK_i\})\rightarrow CT$：输入全局公共参数 GP 以及要加密的共享数据 M，访问结构$(\boldsymbol{A},\rho)$以及

管理访问控制策略中属性相关的访问结构的公钥集合$\{APK_i\}$，输出加密的密文CT。

4)$ABE.KeyGen(GP,U_{id},i,\{ASK_i\})\rightarrow ABE.SK_i$：输入全局公共参数$GP$、DU的唯一标识符$U_{id}$，DU符合访问控制策略的相关属性$i$和相关AA的私钥$\{ASK_i\}$，输出属性密钥$ABE.SK_i$。

5)$Decrypt(GP,U_{id},CT,\{ABE.SK_i\})\rightarrow M$：输入公共参数$GP$，DU的唯一标识符$U_{id}$、密文$CT$和DU相关的属性密钥$\{ABE.SK_i\}$，若DU的属性集合满足密文对应的访问策略，则解密成功，输出加密的数据M。

3.3　基于属性的签名

基于属性的签名(Attribute-Based Signature，ABS)是一种数字签名方案，可以通过将签名关联到访问控制策略来实现对数据的细粒度访问控制。ABS不是针对具体的签名对象进行签名，而是针对满足一定属性条件的签名者进行签名，可以保证在不泄露签名者具体身份信息的前提下验证该签名者符合特定的访问控制策略，保护签名者的身份隐私。多属性授权中心的基于属性的签名(Multi-Authority Attribute Based Signature，MA-ABS)是对传统的ABS签名方案的一种扩展，它采用了多个AA协同工作来实现属性的发放和管理，避免了单一AA带来的单点故障问题，提高了系统的灵活性和可扩展性。

因此，本文参考文献[21]提出的多属性授权中心的基于属性的签名方案DMA-ABS。DMA-ABS方案由以下6个函数组成。

1)$GlobalSetup(\lambda)\rightarrow GP$：给定安全参数$\lambda$，生成全局公共参数$GP$。

2)$AuthoritySetup(GP,AA_{id},i)\rightarrow(APK_i,ASK_i)$：输入全局公共参数$GP$、AA在系统中的唯一标识$AA_{id}$和每个AA管理的属性$i$，生成自己的公钥$APK_i$和私钥$ASK_i$。

3)$CreateUser(GP,U_{id})\rightarrow(UPK,USK)$：输入公共参数$GP$、DU的唯一标识符$U_{id}$，输出DU的公钥$UPK$和私钥$USK$，私钥用来签名。

4)$ABS.KeyGen(GP,U_{id},i,ASK_i,UPK)\rightarrow ABS.SK_i$：输入公共参数$GP$、DU的唯一标识符$U_{id}$、相关属性$i$和相关访问结构的私钥$ASK_i$和用户公钥UPK，输出DU的签名密钥$ABS.SK_i$。

5)$Sign(GP,M,(A,\rho),USK,U_{id},\{ABS.SK_i\})\rightarrow\sigma$：输入公共参数$GP$、要签名的消息$M$、访问结构$(\boldsymbol{A},\rho)$、DU私钥$USK$、DU唯一标识符$U_{id}$和DU相关签名密钥集$\{ABS.SK_i\}$，输出签名$\sigma$。

6)$Verify(GP,U_{id},\sigma,(A,\rho),M,\{APK_i\})\rightarrow 0/1$：输入公共参数$GP$、DU的唯一标识符$U_{id}$、签名$\sigma$、访问结构$(\boldsymbol{A},\rho)$、签名的消息$M$以及出现在访问策略上所有属性对应的访问结构的公钥集合$\{APK_i\}$，验证签名。如果签名合法则输出1，否则输出0。

3.4　区块链

3.4.1　区块链概念和结构

区块链是一种由多方共同维持、使用加密技术保证信息传输和访问安全、按照时间序列存储的分布链式结构数据库。严格来讲，区块链技术是加密解密技术、点对点网络、分布式存储技术等多项技术的交叉融合，具有去中心、不可篡改、可追溯和公开透明等特性。区块链是由区块构成的逐渐延展的链式数据结构，包含由区块头和交易信息构成的区块体。其中区块头包含上一区块的哈希Hash、Merkle根、时间戳、难度值和随机数Nonce等内容，每个区块通过哈希链接到上一区块并为区块链提供完整性。区块链的四大核心技术为分布式账本、共识机制、密码学和智能合约。

3.4.2　区块链分类

根据区块链系统中参与者的不同，可以将区块链分为公有链、私有链和联盟链。

1)公有链。公有链通常被认为是“完全去中心化”的，所有数据公开透明，不需要任何集中的组织，允许所有节点自由加入或退出。任何节点都可以参与使用和维护公有链，常见的公有链有比特币和以太坊。

2)私有链。私有链仅对单独的组织或者个人开放，信息不对外公开，因此私有链交易速度快、成本低、不易被攻击且隐私保护强。

3)联盟链。联盟链是介于公有链和私有链之间的一种系统，是“部分去中心化”的，由多个组织合作共同维护一条区块链，共同根据共识机制参与整个系统的管理和运作。联盟链只允许授权节点加入到区块链网络中，常见的联盟链有Hyperledger Fabric。

本文引入多个AA取代传统CP-ABE方案中的单一AA，来避免单点故障问题。联盟链的“部分去中心化”、不可篡改等安全特性，能很好地与多属性授权中心的访问控制方案结合，因此本文利用联盟链在多个AA之间构建信任，由多个AA共同维护区块链，构建安全的访问控制框架。

3.4.3　UTXO概述

比特币中引入了交易的概念，用于在地址之间传输加密货币。每笔交易都由发送方使用私钥签名并提交给区块链。比特币通过hash机制，把涉及同一枚比特币的所有交易串联在一起，防止重复付款的欺诈行为。UTXO是中本聪最早在比特币中用于解决重复交易问题的技术。

3.4.4　Hyperledger Fabric

Hyperledger Fabric提供了一个可扩展的、可配置的、安全的、高性能的区块链平台。它支持使用Java，Node.js，Go等通用编程语言来编写智能合约。Fabric的核心设计理念是模块化和可插拔性，它主要由Peer节点、Orderer节点、CA(Certificate Authority)、链码和Fabric账本(Ledger)构成。

4　系统框架

本文方案的整体架构如图1所示，其由5个实体组成：AA、联盟链、DO、DU和CSP。

1)AA：将单个AA的工作划分给多个AA，解决单个AA系统中的性能瓶颈问题。各个AA管理对应的属性并向DU分发属性私钥和签名私钥。在本文方案中，一个AA可以管理多个属性，但是一个属性仅能由一个AA管理。

2)联盟链：联盟链节点由各个AA维护，联盟链上存储交易以及共享数据的元数据metadata，元数据中包含云上加密

数据的哈希值，当 DU 从 CSP 上下载加密数据后可以验证哈希值，以保证云上数据的完整性。

3)DO：DO 在本方案中会设置访问策略加密共享数据，然后将密文上传到 CSP，并将密文相关元数据上传到区块链。DO 还可以利用智能合约验证 DU 的授权请求，验证通过后向 DU 分发代表访问权限的访问令牌 token，在整个方案系统中 DO 可以掌控共享数据的被访问情况。

4)DU：DU 想要访问共享数据，就必须先向 DO 进行访问权限申请，DU 获得访问权限即访问令牌 token 后可以向 CSP 请求下载加密的共享数据，获得加密数据后，满足访问控制策略的 DU 可以解密获得数据，然后比较哈希值来验证云上数据的完整性。

5)CSP：CSP 是半可信的，即 CSP 会诚实地执行用户的命令，但仍然对用户的数据和信息好奇，CSP 可能会篡改、丢失甚至泄露云上存储的数据。在本节中 CSP 存储加密的共享数据，并处理 DU 的访问请求，在验证 DU 的访问权限的有效后向 DU 分发密文。

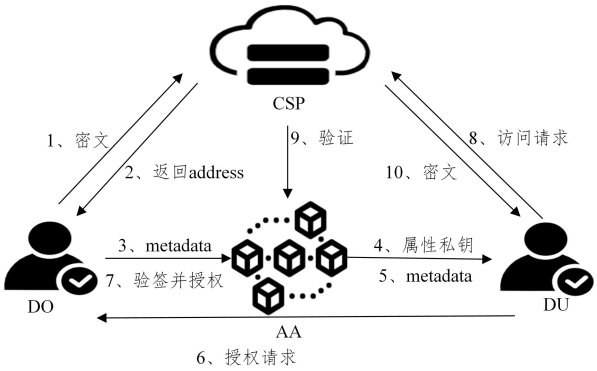

图 1 系统框架

Fig. 1 System framework

为实现细粒度授权和访问过程分离，以及一次授权、多次访问的功能，本文基于比特币 UTXO 数据结构，开发了一种代表数据用户访问权限的数字令牌，用于访问控制，其被称为 token，token 的各字段如表 1 所列。

表 1 token 结构

Table 1 token structure

字段	名称	描述
Basic	TX_{id}	交易号
	Timestamp	交易提交时间
	Script	当前交易名称
	$Sig(token)_{DO}$	发送者对 token 的签名
In	SenderId	发送者的 id
	Subject	DO 对 DU 的签名
Out	RecipientId	接收者 id
	Quantity	token 数量

本文方案设计的 token 设置有 3 个字段，分别为 Basic，In 和 Out。

Basic 字段中，TX_{id} 是用于标识交易的唯一值，只有在该交易被成功验证并存储在区块链中时，才会生成唯一的标识交易号。Timestamp 代表交易提交时间；Script 标识交易操作类型，包括 transfer，consume 和 query 这 3 种操作。transfer 操作用于授权阶段，DO 向身份验证通过的 DU 授予相应数量的 token；consume 操作用于有访问权限的 DU 向 CSP 发起访问，每访问一次消耗一个 token；query 操作用于访问请求阶段 CSP 验证 DU 的访问权限。$Sig(token)_{DO}$ 是 DO 对该访问令牌 token 的签名，是 DO 用私钥提供的签名。

In 字段中的 SenderId 是发送者在系统中的唯一标识，是发送者 id。Subject 字段是只读字段，不可以更改，是 DO 对授权 DU 的签名，可以表示为 $Sig(DU)_{DO}$。它可以证明当前 token 仅可由授权 DU 用来访问该 DO 的共享数据，不可以被授权 DU 转移给非授权用户访问该 DO 的共享数据，或者被授权 DU 重用该 token 以访问其他 DO 的数据。例如，DO 授权给 DU_1 一定数量的 token，token 字段的 Subject 字段为 $Sig(DU_1)_{DO}$，代表 DO 对 DU_1 的签名。DU_1 若将该 token 转移给非授权用户 DU_2，对于 DU_2 来说，其无法使用该 token。因为若 DU_2 想使用该 token 则需要填充 token 的关键字段，其中 In 字段中的发送方为 DU_2，Subject 字段为只读字段，仍为 $Sig(DU_1)_{DO}$。DU_2 没有 DO 的私钥，无法改变 Subject 字段的签名。在访问阶段验证该交易时，用 DO 公钥验签，验签结果为 DU_1，与 DU_2 比对不通过，验证失败。假设 DU_1 要用该 token 访问其他 DO，如 DO_1，同理在访问阶段验证该交易时，用 DO_1 的公钥验签会失败，这保证了访问控制系统的安全性。

Out 字段中的 RecipientId 是接收者在系统中的唯一标识，是接收者 id。Quantity 表示 DO 授予给 DU token 的个数，DU 每执行一次 consume 交易，交易成功后 Quantity 的数量减一。

5 系统流程

整体方案的系统流程包括系统初始化、加密、属性私钥获取、授权和访问这 5 个阶段。

5.1 系统初始化阶段

系统初始化主要包括全局参数的生成以及 AA 和 DU 的注册，所有的 AA，DU 和 DO 都必须在区块链网络中进行注册并拥有唯一标识符。

区块链系统中，首先由 Fabric-CA 执行链下函数 $Global\text{-}Setup(\lambda)\rightarrow GP$，该函数由区块链 CA 执行，以安全参数 λ 为输入参数，生成公共参数 GP，然后调用智能合约将公共参数 GP 存在区块链中，以便于 DU，DO 和 AA 在访问控制过程中使用。

1)AA 注册：AA 从区块链中获得公共参数 GP 后，生成其公私钥对 (APK, ASK)，并调用智能合约将其公钥 APK 存在区块链中，以便 DO 加密密文和验证 DU 权限时使用。

2)DU 注册：DU 从区块链中获得公共参数 GP 后，生成其公私钥对 (UPK, USK)，并将其公钥 UPK 存在区块链中，以便 AA 在属性私钥生成阶段将生成的属性私钥加密存储到区块链上，保护属性私钥的安全。

5.2 加密阶段

为了提高加密效率，DO 从密钥空间中随机选择一个对称密钥 K 来加密共享数据 Data，生成密文 CT_1。然后 DO 利用链下函数 $Encrypt(GP, M, (A, \rho), \{APK_i\})\rightarrow CT_2$ 将对称密钥 K 加密，生成密文 CT_2。该函数输入包括公共参数 GP、要加密的对称密钥 K、DO 设置的访问策略 $(\boldsymbol{A}, \rho)$ 和相关 AA

的公钥$\{APK_i\}$，输出为加密密文CT_2。然后，DO将密文$CT=\{CT_1,CT_2\}$打包存储到CSP，得到CSP中数据的存储地址address。最后DO调用智能合约将共享数据的元数据$metadata=\{address,(\boldsymbol{A},\rho),H(CT)\}$上链存储，组成元目录，其中$(\boldsymbol{A},\rho)$是DO设置的访问结构，$\rho$将访问矩阵$\boldsymbol{A}$中的行与相应属性的散列值映射，$address$是CSP中数据的存储地址，$H(CT)$是密文$\{CT_1,CT_2\}$的哈希值，以验证云上数据未被篡改。

5.3　属性私钥获取阶段

DU从AA处获得其属性私钥，即属性密钥和签名密钥。属性密钥用来解密密文，DU属性符合密文的访问策略即可解密成功；签名密钥用来对授权请求做签名，便于DO验证DU的身份属性是否满足访问策略。一个DU有多个属性，不同的属性由不同的AA管理。举例来说，若DU属性有{区块链实验室，A大学}，其要获得相关的属性私钥，则分别需要从“A大学”和“区块链实验室”处获得。这将带来一些通信开销，并且DU属性越多，通信开销就越大。

为减少DU通信开销，DU可以通过与智能合约交互来获取属性私钥，以减少DU和AA之间的交互。DU完成注册后将自己的公钥UPK存入区块链后，相关的AA将提前运行链下函数$ABE.KeyGen(GP,U_{id},i,\{ASK_i\})\rightarrow ABE.SK_i$。该函数输入包括公共参数$GP$、DU的唯一标识符$U_{id}$、DU符合访问控制策略的相关属性$i$和相关$AA$的私钥$\{ASK_i\}$，输出DU的属性密钥$ABE.SK_i$。接着AA运行链下函数$ABS.KeyGen(GP,U_{id},i,ASK_i,UPK)\rightarrow ABS.SK_i$，该函数输入包括公共参数$GP$、DU唯一标识符$U_{id}$、相关属性$i$、相关AA的私钥$ABE.SK_i$和用户公钥$UPK$，输出DU的签名密钥$ABS.SK_i$。AA生成DU的属性密钥$ABE.SK_i$和签名密钥$ABS.SK_i$后，用DU的公钥$UPK$加密这两个密钥，得到DU加密后的属性私钥$SK_i$，然后调用智能合约将其存储到区块链上。因为区块链是公开透明的，所以用DU的公钥UPK加密其属性私钥可以保证其属性私钥的隐私和安全。之后DU可以通过算法1与智能合约交互请求，以获取其属性集合attributes对应的属性私钥集合SK_{uid}，减少通信开销。

算法1　属性私钥获取智能合约

输入：(U_{id}，attributes，i)
输出：属性私钥集合SK_{uid}
1. /* 属性私钥获取 */
2. if 数据用户U_{id}身份有效 then
3.　for i in attributes do
4.　获得属性私钥SK_i；
5.　$SK_i\rightarrow SK_{uid}$；
6.　end for
7.　return SK_{uid}；
8. else
9.　return false；
10. end if

5.4　授权阶段

授权阶段为DU请求获得DO共享数据的访问权限，授权流程如图2所示，首先，DU从区块链上查找元目录，获得DO共享数据的元数据metadata(第1－2步)。metadata包括CSP中数据的存储地址address、DO设置的访问结构$(\boldsymbol{A},\rho)$、密文的哈希值$H(M)$。然后，DU执行链下函数$Sign(GP,M,(\boldsymbol{A},\rho),USK,U_{id},\{ABS.SK_i\})$生成签名信息$\sigma$，该函数输入包括公共参数$GP$、DU唯一标识符$U_{id}$、签名的消息$M(M$为$\{U_{id},DO_{id}\}$，$DO_{id}$为DO的唯一标识符)、DU的属性私钥$USK$和DU相关签名密钥集合$\{ABS.SK_i\}$，输出对授权请求的签名信息$\sigma$。

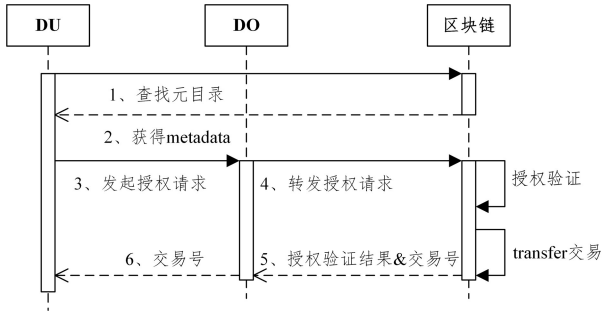

图2　授权流程

Fig. 2　Authorization process

接着，DU向DO发送授权请求，授权请求包括签名的消息M和签名信息σ。DO将该授权请求、访问结构$(\boldsymbol{A},\rho)$和没有交易号的token(用于执行transfer操作)广播到区块链网络中(第3－4步)，触发智能合约，调用链上函数$Verify(GP,U_{id},\sigma,(\boldsymbol{A},\rho),M,\{APK_i\})$对DU进行授权验证。该函数输入包括公共参数$GP$、DU唯一标识符$U_{id}$、签名$\sigma$、访问结构$(\boldsymbol{A},\rho)$、签名的消息$M$以及出现在访问策略上所有属性对应的AA的公钥集合$\{APK_i\}$。如果签名合法则输出1，否则输出0。

验证结果若为1则表示验证通过，触发transfer交易。区块链成功背书共识后，将会得到一个有效的交易号TX_{id1}存储到区块链上，然后将授权验证结果和交易号TX_{id1}返回给DO做响应(第5步)。最后，DO将交易号TX_{id1}返回给DU做授权响应(第6步)，之后DU可以利用这些token对DO共享数据发起访问。DU利用token向DO的共享数据发起访问，因此DO可以循环利用授权给DU的token，即当DU的访问令牌耗尽再次发起授权请求时，DO可以将这些从DU处收到的token再次授权给DU。

DO对DU发起的transfer交易所对应的token结构如表2所列。Basic部分中，TX_{id1}为实际交易号；time为瞬时时间戳的值；transfer为操作名称；$Sig(token)_{DO}$为DO对当前token的签名。In部分中DO_{id}表示DO的唯一标识$Sig(DU)_{DO}$，即Subject值，为只读字段，是DO对DU的签名，表示该token仅可由DU使用并且仅可用来访问DO的共享数据。Out部分中，U_{id}表示DU的唯一标识；Quantity为DO授权DU token的数量。

表2　transfer交易token结构

Table 2　token structure of transfer

字段	值
Basic	$\langle TX_{id1},time,transfer,Sig(token)_{DO}\rangle$
In	$\langle DO_{id},Sig(DU)_{DO}\rangle$
Out	$\langle U_{id},Quantity\rangle$

5.5 访问阶段

访问流程如图3所示，首先DU获得DO授权的token后向CSP发起访问请求{U_{id}，DO_{id}，Sig(DU)，address，TX_{id1}，没有交易号的token}，访问请求包括访问者DU的唯一标识U_{id}、被访问者DO的唯一标识DO_{id}、DU的签名Sig(DU)、访问密文在CSP上的存储地址address、DO授权给DU相应数量token的交易号TX_{id1}和一个没有交易号的token，这个token用来发起consume交易(第1步)。

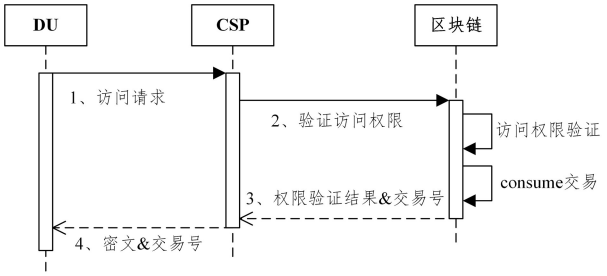

图3 访问流程

Fig. 3 Access process

然后，CSP收到访问请求后，利用请求中的交易号TX_{id1}执行query操作，验证交易真实性来判断DU访问权限是否有效。若访问权限有效，则触发consume交易，将没有交易号的token提交给区块链。区块链节点达成共识后返回给DU两个交易号，其中一个交易号表示DU此次可以访问DO的数据，消耗一个token，因此DU对DO的数据访问权限减一。另一个交易号TX_{id2}代表DU剩余token，由DU之后发起访问请求(第2步)。接着，区块链将访问权限验证结果和交易号TX_{id2}返回给CSP做响应(第3步)。最后，CSP将密文和交易号TX_{id2}返回给DU做访问请求的响应(第4步)。DU收到密文后可以执行链下函数 $Decrypt(GP, U_{id}, CT_2, \{ABE.SK_i\})$解密获得对称密钥$K$。该函数以公共参数$GP$、DU唯一标识符$U_{id}$、密文$CT_2$和DU相关的属性密钥$\{ABE.SK_i\}$为输入。若DU的属性集合满足密文对应的访问矩阵，则可以解密成功，输出加密阶段加密的对称密钥K，然后用对称密钥解密密文CT_1获得共享数据Data。

DU对DO发起的consume交易所对应的token结构如表3所列。Basic部分中，TX_{id1}为实际交易；time为瞬时时间戳的值；consume为操作名称；$Sig(token)_{DU}$为DU对当前token的签名。In部分中U_{id}表示交易发送方DU的唯一标识；$Sig(DU)_{DO}$即Subject值，为只读字段，是DO对DU的签名，表示该token仅可由DU使用并且仅可用来访问该DO的共享数据。Out部分中，该交易有两个未花费的交易输出，一个是DU转给DO的一个用作访问的token，DO_{id}表示交易接收者DO的唯一标识，1为DU此次访问DO共享数据消耗的访问令牌数，DU转给DO的token之后可被循环利用授权给DU；另一个代表DU剩余的token数量。

表3 consume交易token结构

Table 3 token structure of consume

字段	值
Basic	〈TX_{id1}，time，consume，$Sig(token)_{DU}$〉
In	〈U_{id}，$Sig(DU)_{DO}$〉
Out	〈DO_{id}，1〉〈U_{id}，Quantity-1〉

6 实验分析及讨论

6.1 安全分析

6.1.1 防分布式拒绝服务攻击

分布式拒绝服务攻击(Distributed Denial of Service，DDoS)可以使很多计算机在同一时间遭受到攻击，使攻击目标无法使用，即利用合理的请求造成资源过载，导致服务不可用，从而造成服务器拒绝正常流量服务。

本方案中DU只有获得DO授权相应数量的token以后，才可以发起访问请求。在DU向CSP发起访问请求后，CSP可以验证交易的有效性，未授权用户即使发起访问请求，但因其未获得访问令牌，CSP不会处理其请求。这就防止了未授权用户向CSP发起大量请求，避免系统瘫痪。

6.1.2 数据完整性

本方案中共享数据被加密存储在云存储器上，由于云是半可信的，云可能会出于利益而篡改用户存储在云上的加密数据，导致访问数据的用户获得错误的共享数据，无法解密成功。本方案设计利用区块链的不可篡改性，将存储在云上的共享数据的哈希值存在区块链上。DU从云上获取加密数据后，可以计算密文哈希值，然后与其从区块链上获得的元数据中的密文哈希值做对比，验证证存储在云上的加密数据是否被篡改。若哈希值相同则说明密文未被篡改，以此来保证加密数据的完整性。

6.1.3 数据用户隐私保护

本方案引入DMA-ABS方案对DU的身份属性进行验证，可以在不知道DU具体身份属性的情况下对DU进行验证，保护了DU的属性安全。

6.1.4 抵赖攻击

本方案中，DU发起授权或者访问请求时，将调用智能合约进行权限验证，将在链上记录一个可信且不可更改的访问日志，恶意DU的任何非法访问都会被记录在链，无法抵赖。

6.1.5 重放攻击

在重放攻击中，授权DU将已使用过的token重放发起访问，但是在本文方案中，token具有交易号、时间戳和签名等属性，授权DU使用token需经智能合约验证，使用之后即被记录为已使用，因此重复的交易号需经由智能合约验证拒绝。

6.1.6 中间人攻击

恶意DU入侵到授权DU和DO的通信中，并发送伪造的consume请求。本文方案中，引入DMA-ABS算法对DU的授权请求进行属性权限认证，即使恶意DU发起授权请求，但也可经由智能合约验证其属性不满足DO设置的访问策略，DO并不会授权其token。

假设攻击者恶意发送伪造的consume请求，但是在本文方案中，consume请求中应包含DU的唯一标识和其token代表的交易号TX_{id}，该交易号在发送之前就已经记录在区块链账本上，经由访问智能合约认证，被修改或者伪造的consume请求都可以被智能合约检测到，被认为是无效访问请求。

6.2 功能分析

为了比较本方案的访问控制模型设计和现有方案之间的差异，本节将从多属性授权中心、身份隐私、可追溯性和数据

对于 DO 来说可控这 4 个方面进行比较，结果如表 4 所列。

表 4　访问控制方案之间的对比

Table 4　Comparison between access control schemes

文献	[16]	[17]	[20]	[21]	本文方法
多属性授权中心	×	√	×	√	√
身份隐私	×	×	√	√	√
可追溯性	√	√	√	√	√
数据 DO 可控	×	×	×	×	√

6.2.1　多属性授权中心

本文使用的多属性授权中心 CP-ABE 是基于传统的 CP-ABE 算法改进设计的。传统的 CP-ABE 算法中只包含单个属性授权中心，一个 AA 管理着多个不同的属性，存在单点故障问题，并且由多个 AA 管理多个属性更加符合实际的云存储环境。文献[16]和文献[20]采用了传统的 CP-ABE 算法，系统中只包含单个属性授权中心，不适合用户属性过多的场景。

6.2.2　身份隐私

基于属性的签名算法可以在不泄露 DU 具体身份属性的情况下，保证 DU 签名的消息被验证是否满足特定的访问控制结构。文献[20]、文献[21]和本文系统引入了 DMA-ABS 方案，保护了 DU 身份属性隐私。

6.2.3　可追溯性

区块链具有去中心、不可篡改和可追溯的特性。本文系统在整个数据访问控制过程中，token 授权结果和 DU 访问密文的请求存储在区块链上，防止未授权用户恶意访问密文。文献[16-17，20-21]都引入了区块链，将 DU 访问密文的行为记录在区块链上，记录恶意用户的访问行为，并且便于在密文被泄露时锁定恶意用户。

6.2.4　数据 DO 可控

在大多数基于区块链的访问控制系统研究中，DO 仅仅起到一个共享数据存入云端或者区块链的作用。数据共享之后，DO 并不能掌控共享数据的被访问情况。但是在本文系统中，DU 需要获得 DO 的授权，获得 token 之后才能访问共享数据，保证 DO 可以掌控共享数据的被访问情况。

6.3　性能分析

为了评估本方案的性能，本文开发了一个基于开源区块链平台 Hyperledger Fabric V2.2 版本的实验模型，以分析本文所提方案的可行性和性能。并且本文选定文献[21]中提出的访问控制方案做为对比方案进行性能比较，方案[21]也引入了 DMA-ABS 方案来保证数据用户的匿名性验证，但是当 DU 多次访问数据时每次都需要进行访问权限的验证，存在着重复的验证操作，且该访问权限的验证时间消耗较高。

实验运行在操作系统为 Ubuntu 20.04，CPU 为 Intel Core(TM) i5-10400 @2.90GHz，运行内存有 8GB 的计算机上，然后初始化一个由两个组织组成的联盟区块链，每个组织都是一个由独立的可信机构以及 4 个节点组成的局域网。每个 peer 节点上都部署了本文设计的智能合约，智能合约由 Java 编程语言编写。DU，DO 和 CSP 作为客户端应用程序调用智能合约。

6.3.1　访问数据时间消耗对比

1）单个 DU 访问数据时间消耗

本文引入 token，将授权验证结果以访问令牌的形式存储，这样后续 DU 再次访问数据时就不需要再次验证 DU 的访问权限，可以直接查询 token 的有效性并进行验证，实现了授权和访问分离并且减少了 DU 访问时间开销。从图 4 中可以看到，由于引入了 token，本文方案需要执行 transfer 交易，授权 DU 相应数量的 token，因此在第一次访问时的时间开销较大，但与对比方案相比时间开销在可接受范围内。同时随着 DU 访问次数的增加，在本文方案中，DU 之后的每次访问时间消耗远低于文献[21]的时间消耗，大大降低了 DU 的访问时间开销。这是因为本文方案不再需要每次都执行复杂的验签计算，仅需验证 DU 的 token 有效性即可完成对 DU 的访问请求处理。

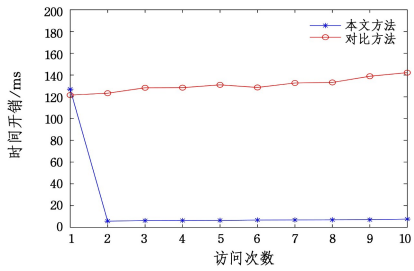

图 4　单个 DU 访问数据时间消耗的对比

Fig. 4　Comparison of time consumption for single DU accessing data

2）多个 DU 访问数据时间消耗

接下来将从多个 DU 访问数据方面入手，对比访问时间开销，验证引入 token 的优势。本部分实验固定每个 DU 发起一次访问请求，考虑了本文方案中存在的 3 种情况：所有发起访问的 DU 都有 token、一半的 DU 有 token 和所有的 DU 都未获得 token。

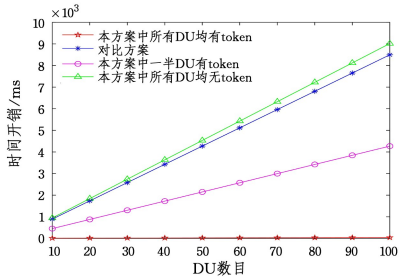

图 5　多个 DU 访问数据时间消耗对比

Fig. 5　Comparison of time consumption for multiple DU accessing data

从图 5 中可以看到，随着 DU 数目的增多，本文方案和对比方案的访问时间开销都约呈线性增长。从图中还可以看到，本文方案在最不理想的情况下，即所有发起访问请求的 DU 都未获得 token，本文方案的时间开销比对比文献[21]略大。本文方案中没有 token 的 DU 需要先获得 token 才能发起访问，但是该时间开销在可接受范围内。

当访问的数据用户中有一半的 DU 有 token 时，时间开销是低于对比方案的，并且当所有 DU 都有 token 时，访问时间开销远远低于对比方案，仅消耗几十毫秒，可以证明本文方案可以有效降低 DU 访问数据的时间开销。

6.3.2　token 数目变化对访问时间消耗的影响

本文方案引入了 token，代表 DU 对 DO 共享数据的访问

权限，实现了一次授权、多次访问。接着，本节将进一步研究token数目变化对DU访问共享数据的时间消耗的影响。

如图6所示，横坐标表示DU在授权阶段获得的token数量，设置为1～10。从图中可以看出，当DU访问次数固定不变时，随着DU获得的访问权限token数量的增加，DU访问共享数据的时间消耗也越小。因此当DU需要多次访问共享数据时，在授权阶段获得的token数量越多，整体平均时间消耗越低。并且当访问次数为1时，可以看出token数量变化对访问时间消耗几乎没有影响。同时从图中也可以看到，当DU获得token数量固定不变时，访问次数越多，时间消耗越大。

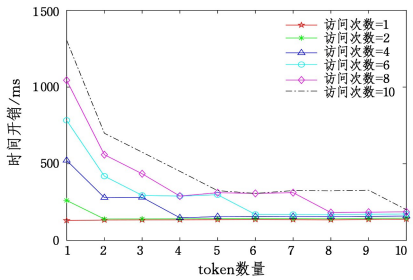

图6 token数量变化下访问时间消耗的对比

Fig. 6 Comparison of access time consumption when the number of tokens changes

6.3.3 属性私钥获取时间消耗

本文方案采用多属性授权中心的CP-ABE方案，引入多个AA代替单个AA，来解决单一属性授权中心的CP-ABE方案中的单点故障问题。由于引入多个AA，不同的AA管理不同的属性，因此DU在获取属性私钥时，需要与不同的AA通信以获得其相关属性的属性私钥，这会给DU带来较大的通信负担。因此，本文方案设计在DU加入整个系统时，AA会将DU相关的属性私钥用DU的公钥加密存储到区块链上，因此DU只需要与区块链进行交互即可获得其属性私钥。

图7中，横坐标为DU的属性数目，使DU分别与2个AA和4个AA交互来获取属性私钥的时间开销。当DU属性数目固定时，DU和AA交互的个数越多，获取属性私钥的时间消耗就越大，本文方案中DU获取属性私钥的时间消耗较低。同时，从图中也可以看出，随着DU的属性个数的增加，DU获取属性私钥的时间消耗也在增加，但是在本方案中，其整体时间消耗在几十毫秒级别，DU是可以接受的。因此，本方案中DU与智能合约交互获得其属性私钥，可以有效降低DU的通信开销和属性私钥获取的时间开销。

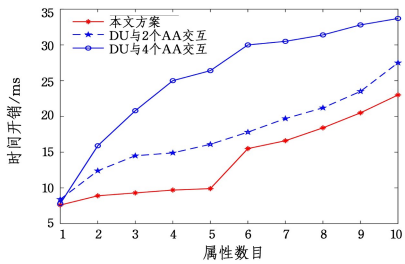

图7 属性私钥获取时间消耗的对比

Fig. 7 Comparison of time consumption for obtaining attribute private keys

6.3.4 交易吞吐量

本文利用性能测试工具tape研究了区块大小和交易到达率对交易吞吐量（单位：每秒交易数（Transaction Per Second，TPS））的影响。区块大小表示同一区块中打包的最大交易的数量，交易到达率（Transaction Arrival Rate）表示同时到达区块链的交易数量。块大小设置为10～60，间隔为10，将交易到达率设置为200～1 000单位，间隔为200。从图8中可以看出，随着区块大小从10变化到40，交易吞吐量显著增加，然后趋于稳定。并且由于所有的交易到达率都远高于系统的处理速率，因此可以看到不同的交易到达率对交易吞吐量几乎没有影响。

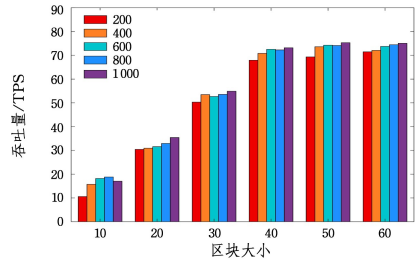

图8 交易吞吐量

Fig. 8 Transaction throughput

结束语 本文提出了一种基于多属性授权中心CP-ABE、DMA-ABS和区块链的云上个人隐私数据共享访问控制模型。本文方案调用智能合约实现链上和链下交互，保证了数据所有者对共享数据的可控性，并引入UTXO数据结构来实现一次授权、多次访问功能，在保护数据用户匿名性验证的前提下减少访问时间开销。但是，本文方案中由于引入了多属性授权中心CP-ABE和DMA-ABS算法，数据所有者和数据用户将承担较高的加解密开销，后期仍需对加解密外包加以研究。

参 考 文 献

[1] SHARMA S. Expanded cloud plumes hiding Big Data ecosystem [J]. Future Generation Computer Systems, 2016, 59: 63-92.

[2] 数安时代GDCA. CapitalOne数据泄露影响1.06亿人[EB/OL]. https://www.sohu.com/a/330584204_604699. 2019-07.

[3] 隐查查. 2022年国内外个人信息泄露大事件盘点[EB/OL]. https://zhuanlan.zhihu.com/p/598514200. 2023-01.

[4] RASORI M, LAMANNA M, PERAZZO P, et al. A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(11): 8269-8290.

[5] LI J G, ZHANG Y C, NING J T, et al. Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT [J]. IEEE Transactionson Cloud Computing, 2022, 10(2): 762-773.

[6] CHEN N Y, LI J G, ZHANG Y C, et al. Efficient CP-ABE Scheme With Shared Decryption in Cloud Storage [J]. IEEE Transactions on Computers, 2022, 71(1): 175-184.

[7] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy Attribute-Based Encryption[C]// 2007 IEEE Symposiumon Security and Privacy. 2007: 321-334.

[8] HUANG K Q. Secure Efficient Revocable Large Universe Multi-Authority Attribute-Based Encryption for Cloud-Aided IoT[J]. IEEE Access, 2021, 9: 53576-53588.

[9] KAMALAKANTA S, ANKIT P, PADMALOCHAN B. PMTER-ABE: a Practical Multi-Authority CP-ABE with Traceability, Revocation and Outsourcing Decryption for Secure Access Control in Cloud Systems[J]. Cluster Computing, 2021, 24(2): 1525-1550.

[10] HIKHA M, ANSHUMAN K, GÜRKAN G, et al. A Survey on Role of Blockchain for IoT: Applications and Technical Aspects [J]. Computer Networks, 2023, 227: 109726.

[11] LSHEHRI S, RADZISZOWSKI S, RAJ R. Secure Access for Healthcare Datain the Cloud Using Ciphertext-Policy Attribute-Based Encryption[C]// 2012 IEEE 28th Iternational Conference on Data Engineering Workshops. 2012: 143-146.

[12] EL GAFIF H, TOUMANARI A. Efficient Ciphertext-Policy Attribute-Based Encryption Constructions with Outsourced Encryption and Decryption[J]. Security and Communication Networks, 2021, 2021(3): 1-17.

[13] LIU Z C, JIANG Z, WANG X, et al. Practical Attribute-Based Encryption: Outsourcing Decryption, Attribute Revocation and Policy Updating[J]. Journal of Network and Computer Applications, 2018, 108: 112-123.

[14] LI T, ZHANG J W, LIN Y X, et al. Blockchain-Based Fine-Grained Data Sharing for Multiple Groups in Internet of Things [J]. Security and Communication Networks, 2021, 12(3): 123-135.

[15] SREENIVASA Y R. A Secure and Efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records Sharing in Cloud Computing[J]. Future Generation Computer Systems, 2017, 67(2): 133-151.

[16] LI S X, LI R X, ZHANG Y, et al. CBI: A Data Access Control System Based on Cloud and Blockchain Integration[C]// 2020 IEEE 22nd International Conferenceon High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems. 2020: 715-721.

[17] ZOU Y P, PENG T, ZHONG W T, et al. Reliable and Controllable Data Sharing Based on Blockchain[C]// First International Conference on Ubiquitous Security. 2021: 448-461.

[18] MALAMAS V, KOTZANIKOLAOU P, DASAKLIS T, et al. A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data[J]. IEEE Access, 2020, 8: 134393-134412.

[19] OKAMOTO T, TAKASHIMA K K. Decentralized Attribute-Based Signatures[C]// International Workshop on PublicKey Cryptography. 2013: 125-142.

[20] ZHANG Y R, HE D B, CHOO K R. BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT [J]. Wireless Communications and Mobile Computing, 2018, 1(11): 1-9.

[21] LI G, SATO H. A Privacy-Preserving And Fully Decentralized Storage and Sharing System on Blockchain[C]// 2019 IEEE 43rd Annual Computer Software and Applications Conference. 2019: 694-699.

[22] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. Technion: Israel Institute of Technology, 1996.

[23] OKAMOTO T, KASUYUKI T. Decentralized Attribute-Based Encryption and Signatures[J]. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2020, E103. A(1): 41-73.

TONG Fei, born in 1987, Ph.D, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include Internet of Things and ubiquitous networking intelligence & security.

（责任编辑：喻藜）