第 12 卷 第 3 期
2023 年 5 月
集 成 技 术
JOURNAL OF INTEGRATION TECHNOLOGY
Vol. 12 No. 3
May 2023

引文格式：
屈靖淇, 李红辉, 崔家昇, 等. 基于区块链的可溯源政务大数据共享方法研究 [J]. 集成技术, 2023, 12(3): 19-33.
Qu JQ, Li HH, Cui JS, et al. Research on blockchain-based traceable government big data sharing method [J]. Journal of Integration Technology, 2023, 12(3): 19-33.

基于区块链的可溯源政务大数据共享方法研究

屈靖淇[1] 李红辉[1,2*] 崔家昇[1] 韩铖山[1] 贾志伟[1]

[1]（北京交通大学计算机与信息技术学院 北京 100044）
[2]（高速铁路网络管理教育部工程研究中心 北京 100044）

摘 要 政务服务跨域协作是政府数字化转型和跨域治理相结合所催生的新型治理模式，是政务服务治理的价值目标。由于政府各部门的具体业务和功能不同，各部门都有一套独立的数据管理系统，且各信息化系统存储多样、数据格式复杂、业务流程各异。如何安全可靠地实现各个部门之间的数据共享已成为一项研究难点。传统政务数据共享通常采用集中式共享模式，该模式容易引发数据隐私泄露、部门权限混乱、单点故障等一系列问题。为解决上述问题，该文提出了一种属性基加密与区块链结合的政务数据共享方案。首先，由数据拥有者制定访问控制策略，对数据请求者的属性进行限制；然后，利用子集覆盖技术，实现数据安全共享中的细粒度访问控制及密钥更新，结合线性秘密共享，以实现访问策略的完全隐藏，采用星际文件系统分布式网络存储对称加密后的密文，以缓解区块链系统的存储压力；最后，利用 Keccak 算法对检索数据密文的哈希值进行重加密，实现数据的完整性验证。通过安全性分析和相关实验可知，该文所提方案在安全性和效率方面均能满足政务数据安全共享的需求，可实现政务数据的高效、安全和可溯源共享。

关键词 区块链；数据溯源；属性基加密；政务数据共享
中图分类号 TP 309 **文献标志码** A doi: 10.12146/j.issn.2095-3135.20221004001

Research on Blockchain-Based Traceable Government Big Data Sharing Method

QU Jingqi [1] LI Honghui[1,2*] CUI Jiasheng[1] HAN Chengshan[1] JIA Zhiwei[1]

[1](*School of Computer and Information Technology*, *Beijing Jiaotong University*, *Beijing* 100044, *China*)
[2](*Research Center for High-Speed Railway Network Management*, *Ministry of Education*, *Beijing* 100044, *China*)
[*]*Corresponding Author*: *hhli@bjtu.edu.cn*

Abstract Cross-domain collaboration of government services is a new governance model, which has

收稿日期：2022-10-04 **修回日期**：2023-02-23
基金项目：国家重点研发计划项目（2019YFB2102500）
作者简介：屈靖淇，硕士研究生，研究方向为区块链；李红辉（通讯作者），教授，研究方向包括大数据技术与工程、人工智能、轨道交通信息技术等，E-mail：hhli@bjtu.edu.cn；崔家昇，硕士研究生，研究方向为区块链；韩铖山，硕士研究生，研究方向为知识图谱、通道耦合；贾志伟，硕士研究生，研究方向为联邦学习。

been spawned by the combination of digital transformation of government and cross-domain governance. This model is aimed at achieving the value goal of governance of government services. However, due to the different specific business and functions of each government department, each department has an independent data management system, and each information system has diverse storage, complex data formats and different business processes. As a result, sharing and utilizing the heterogeneous data between departments in a safe and reliable way has become a challenging research problem. Traditional government data sharing usually adopts a centralized sharing mode, which is prone to a series of issues such as data privacy leakage, departmental authority problems, and single point of failure. To address this issue, this paper proposes a government data sharing scheme that combines attribute-based encryption and blockchain. Firstly, an access control policy is formulated by the data owner to restrict the attributes of data requesters. Subsequently, fine-grained access control as well as key update in secure data sharing is achieved by using subset overlay technology, which is combined with linear secret sharing to achieve complete hiding of the access policy. The inter planetary file system distributed network is used to store the ciphertext after symmetric encryption to relieve the storage pressure of the blockchain system. Finally, the hash of the retrieved data ciphertext is re-encrypted using the Keccak algorithm to achieve data integrity verification. Security analysis and experimental analysis show that the proposed scheme can meet the requirements of secure sharing of government data in terms of security and efficiency, and thus realize the secure and traceable sharing of government data.

Keywords blockchain; data traceability; attribute-based encryption; government data sharing
Funding This work is supported by National Key Rearch and Development Program of China (2019YFB2102500)

1 引 言

近年来，随着我国数字政府的发展，政务数据不断积累，并被广泛存储在不同的政府部门、政府门户平台、政务数据库中。这些数据具有时效性、共享性、机密性，在跨部门业务协作和跨部门服务协作中发挥着关键的作用。然而，目前政务数据共享仍存在一些问题和挑战：(1)单点故障。传统的政务数据集中式存储易遭受单点攻击等网络攻击，一旦被攻击成功，将导致机密数据泄露[1]。(2)数据安全问题严重。个人隐私保护与政务数据共享之间的矛盾突出[2]。(3)数据难以溯源[3]。大多政务数据由各单位的数据库独立存储，容易形成“数据孤岛”，导致共享不畅，此外，当数据共享过程中出现问题时，传统的政务数据共享系统难以实现信息追踪和责任认定。

传统政务数据共享系统一般采用集中式共享模式，但集中式服务器经常面临意外或恶意入侵的威胁，一旦服务器被入侵成功，那么其中存储的大量关于公民、企业和其他组织的重要信息将会尽数泄露，造成严重的安全事故。区块链(blockchain，BC)因其去中心化、可追溯性和安全性等特性而被广泛应用于数据共享等领域。Ge等[4]将医疗系统与BC相结合，提出一种基于BC的医疗数据安全访问模型，用于解决集中式存储可能遇到的隐私问题和安全问题。闫冠辰等[1]将BC与模糊查询技术相结合，实现了电子病历的安全高效共享。郭海洲等[5]将去中心化的BC与电控系统相结合，提出一种电控系统数据共享方案，通过智能合约(smart contract，SC)和分布式

账本进行数据溯源。

BC 因其不可篡改的特性避免了传统集中式共享存在的诸多问题，为跨部门数据共享提供了一个安全可靠的环境。同时，BC 因其公开、透明的特点，在处理较为敏感的业务和隐私数据时较为受限[6]。2005 年，属性基加密(attribute based encryption，ABE)被首次提出，为数据的访问控制和隐私保护结合提供了技术支持[7]。传统的 ABE 方案利用属性描述密文，并将策略嵌入用户的密钥中，当且仅当属性集合满足访问结构时，才能解密成功。因此，BC 与 ABE 技术的结合为海量政务数据的安全可靠大规模共享提供了新思路。张晓东等[3]提出一种基于 ABE 和 BC 的数据共享方案，实现了政务数据的安全共享。Porwal 等[8]提出一种支持任何可调节状态下的 ABE 方案，实现了云计算中的数据共享。杜瑞忠等[9]提出一种基于 BC 的多点授权数据加密访问控制系统，将授权中心和属性权限放入以太坊的智能合约中，实现了细粒度的访问控制。Li 等[10]将 BC 与 ABE 相结合，以实现对数据的去中心化安全共享。Li 等[11]基于 BC 和细粒度访问控制的分散存储系统，提出了一种数据共享框架，但没有考虑到用户隐私的保护。Ma 等[12]提出一种基于 BC、SC 和数据分片存储技术的跨部门协同政务数据共享方案。Piao 等[13]提出一种链上服务方法，该方法可有效识别不同政府部门的数据检索要求，实现了政务数据的安全、可控共享。Shi 等[14]将 BC 和星际文件系统(inter planetary file system，IPFS)相结合，实现了政务数据共享中的隐私保护。

上述研究大多基于 ABE 技术进行数据共享，虽然实现了细粒度的访问控制，但是没有实现访问策略的完全隐藏。此外，利用 BC 实现交易记录和数据溯源时未考虑运行效率和存储开销。上述问题也是目前政务大数据共享中存在的问题。针对政务大数据共享存在的数据孤立、数据安全及数据溯源问题，本文提出了一种 ABE 与 BC 相结合的政务数据共享方法，本文主要创新点有：(1)针对政务大数据共享中存在的数据安全问题，本文提出一种 ABE 与对称加密相结合的混合加密方案，实现了数据安全共享中的细粒度访问控制及密钥更新。由数据拥有者(data owner，DO)制定访问控制策略，对数据请求者(data requester，DR)的属性进行限制，基于子集覆盖技术，保护了数据的机密性。使用线性秘密共享方案(linear secret sharing scheme，LSSS)实现访问策略的完全隐藏[14]，利用 AES 算法加密数据、CP-ABE 算法加密数据哈希路径的混合加密策略，增强了数据管理的灵活性。使用 Keccak(SHA-3)加密算法对检索数据密文的 hash 值进行重加密，实现数据的完整性验证。(2)针对政务大数据共享中存在的单点故障问题，本文提出一种 BC 与 IPFS 相结合的链上链下存储模式，利用 BC 的去中心化、不可篡改的特性及 IPFS 的分布性，实现政务数据的安全分布式存储。针对政务大数据共享中存在的数据难以溯源问题，本文基于 BC 和 SC，实现数据加密和共享过程中的信息跟踪，通过对所有参与者的行为记录上链，实现共享过程中的数据溯源，解决数据滥用和责任认定问题。(3)将本文方案应用于政务大数据跨域互操作与溯源系统中的政务数据跨域共享以及数据溯源模块，以解决政务数据共享中的“数据壁垒”和信息泄露问题，实现政府各部门之间的信息安全有效共享。

2　相关知识

本节将对加解密和安全性验证过程中的相关知识进行介绍。

2.1　双线性映射

令 G_1 和 G_2 为两个 p 阶乘法循环群，G_1 的生成元为 x，若从 G_1 到 G_2 的映射 $e:G_1\times G_1\rightarrow G_2$ 是双线性的，那么应该满足 3 点[15]要求：(1)双线

性：$\forall a,b\in Z_q,\forall x,h\in G_1$，均有 $e\left(x^a,h^b\right)=e\left(x,h\right)^{ab}$ 成立；(2)非退化性：$\exists x,h\in G_1$，使 $e\left(x,h\right)\neq 1$；(3)可计算性：$\forall x,h\in G_1$，均存在有效的算法使 $e\left(x,h\right)\in G_2$。

2.2 判定性困难问题假设

根据系统的安全参数，选择 G_1 和 G_2 为两个 p 阶的乘法循环群，G_1 的生成元为 x，在 Z_p^* 中选取任意的元素 $a,b,c_1,\cdots,c_n$，生成元素(向量)：$\boldsymbol{x},\boldsymbol{x}^b,\boldsymbol{x}^a,\boldsymbol{x}^{a^q},\boldsymbol{x}^{a^{q+2}},\boldsymbol{x}^{a^{2q}},\boldsymbol{x}^{bc_j},\boldsymbol{x}^{a/c_j},\cdots,\boldsymbol{x}^{a^{q+2}/c_j},\cdots,\boldsymbol{x}^{a^{2q}/c_j},\boldsymbol{x}^{abc_k/c_j},\cdots,\boldsymbol{x}^{ba^qc_k/c_j}$。其中，$\forall j\geqslant 1,\forall 1\leqslant j\leqslant q,q\geqslant k,j\neq k$。判定 q-parallel BDHE 假设成立的条件为：不存在一种多项式时间算法能以一个不可忽略的概率 δ 区分 $e\left(x,x\right)^{b^{a^{q+1}}}$ 和 $M\in G_2$，其中，$\delta=e\left(g,g\right)^{s^{a^{q+1}}}\in G_2$。

2.3 线性秘密共享方案

LSSS[16]的定义如下，令所有参与者的集合为 P，其中，$P=\left\{P_i\right\},i=1,2,\cdots,n$，若集合 P 中的一个秘密共享方案 π 具备两个条件，则方案 π 被称为 Z_p 的线性秘密共享方案。其中，判定条件为：(1)参与方的每一个秘密份额因子均构成 Z_p 上的一个向量。(2)存在一个 π 的生成矩阵 $\boldsymbol{M}$，维度为 $m\times n$，对任意 $i=1,2,\cdots,m$，$\boldsymbol{M}$ 的第 i 行被单射函数 ρ 映射为属性 $\rho\left(i\right)$，随机选择 $b_2,b_3,\cdots,b_n\in Z_p$ 构成向量 $\boldsymbol{d}=\left(a,b_2,b_3,\cdots,b_n\right)^{\mathrm{T}}$。其中，秘密值 $a\in Z_p$；$\left(\boldsymbol{M}\cdot\boldsymbol{d}\right)$为秘密共享方案的 m 个份额[17]；每个秘密份额 $\lambda_i=\left(\boldsymbol{M}\cdot\boldsymbol{d}\right)_i$ 属于属性 $\rho\left(i\right)$。

线性秘密共享方案具有线性重构特性[18]。令一个线性秘密共享方案 π 的访问结构也为 LSSS，假定 $S\in N$ 为任意属性授权集合，令 $I=\left\{i:\rho\left(i\right)\in S\right\}$，其中，$I\in\left\{1,\cdots,m\right\}$。若$\left\{\lambda_i\right\}$是方案 π 对任意秘密值的有效秘密共享因子，那么可以在多项式时间内找到一组常数 $\left\{w_i\in Z_p\right\}_{i\in I}$，使等式 $\sum_{i\in I}w_i\lambda_i=s$ 成立[19]。

2.4 密文策略属性基加密

ABE 是一种公钥加密算法，在属性基加密方案中，消息发送方利用一组属性 W 加密消息，消息接收者用一组可以描述身份的属性 W' 与私钥相对应[20]。当且仅当 W' 和 W 的交集个数超出系统设定的门限值 i 时，消息接收者才能解密密文[21]。在 ABE 基础上，Sun 等[22]提出了密钥策略属性基加密(key-policy attribute-based encryption，KP-ABE)机制，将访问策略嵌入密钥，文件属性嵌入密文，接收者收到消息时会为其分配一个特定的访问策略，适用于视频点播、数据库访问。Das 等[23]提出了密文策略属性基加密(ciphertext-policy attribute-based encryption，CP-ABE)机制，将访问策略嵌入密文，用户属性嵌入密钥，使信息拥有者可以规定密文访问策略，适用于消息分发场景。

CP-ABE 利用属性刻画用户的资格，由数据加密方制定密文访问策略，以决定谁可以解密密文。在 CP-ABE 中，用户的私钥与一系列属性相关，只有用户的属性符合密文的访问结构才能解密此密文。CP-ABE 包括 4 个基本步骤：初始化、用户密钥生成、数据加密、数据解密。

2.5 区块链技术

BC 作为一种分布式的点对点网络，具有去中心化、不可篡改、多方维护、可溯源等特性。BC 由链式交易块组成，交易块包括区块头和区块体。其中，区块头包含上一个区块的 hash 值、时间戳、Merkle 根、版本号等，区块体则记录了详细的交易数据。新产生的区块经 BC 网络中的节点验证后，被添加到区块链上，每个在链上的交易块中包含的事务将被永久保存。新区块的产生以及账本的更新离不开共识机制，虽然不同 BC 系统的共识机制各不相同，如工作量证明、权益证明机制、股份授权证明机制、实用拜占庭机制等，但它们都侧重于奖励验证者以维护区块链的状态[20]。目前，区块链的应用模式分为公共区块链、联盟区块链和私有区块链。其中，公共区块链对公众开放，任何人都可参与，其

通过“挖矿”保证系统的分散性，这大大降低了效率；私有区块链的读写权限完全由一个组织拥有，写入权限仅限于组织内部对等方，更适用于组织内部；联盟区块链介于公共区块链和私有区块链之间，它对成员有严格的限制，同行之间相互制约，信任度高，主要适用于组织和机构内部或之间的合作[23]。本文使用 Hyperledger Fabric 联盟链置本地区块链网络，模拟各个政府部门节点之间的安全、有效、可溯源数据共享。

3　基于区块链和密文属性基加密的政务大数据共享方案

3.1　方案模型

本文提出一种基于区块链和 CP-ABE 的政务大数据共享系统方案(BT-GDS)，系统架构如图 1 所示。系统架构包括 DO、IPFS 分布式网络、DR、密钥生成中心(key generator center，KGC)、SC、BC 和可信任的授权服务器(trusted authorization server，TAS)等 7 个组成部分。

其中，DO 是某个政府部门的数据拥有者，如司法局、民政局、水务局等，是联盟链的节点之一。当 DO 想要与其他部门共享数据时，需要调用智能合约，以生成数据的信息描述摘要，然后执行两个任务：(1)制定相应的访问控制策略 p，只有满足访问策略的数据请求者才能访问数据；(2) 对数据进行加密，得到密文数据，并将其上传至 IPFS 分布式网络。IPFS 分布式网络将基于数据内容生成唯一的 hash 标识，并将其发送给 DO，DO 随后将 hash 标识发布至 BC。DR 是政府部门中的数据需求方，也是联盟链中的节点之一，DR 根据 DO 上传的信息摘要，确定数据是否符合其需要。DR 从密钥生成中心 KGC 获得主密钥(master secret key，MSK)，然后使用自己的属性集生成用户属性私钥(secret key，SK)，从 IPFS 分布式网络下载加密数据，并对其进行解密。IPFS 提供了一种点对点分布式存储结构，可存储大量数据文件。IPFS 将内容寻址 hash 存储在分布式 hash 列表中，并删除重复的数据文件[4]。DO 使用属性库对外部共享数据进行加密，然后将密文数据上传至 IPFS 网络，该网络根据密文数据的内容返回唯一的 hash 标识，DR 根据 hash 标识下载数据文件。KGC 作为区块链中的节点，解决了传统密钥生成节点不可信或半可信的问题[14]。KGC 通过预定义所有用户属性，将属性分配给相应的节点，从而构建

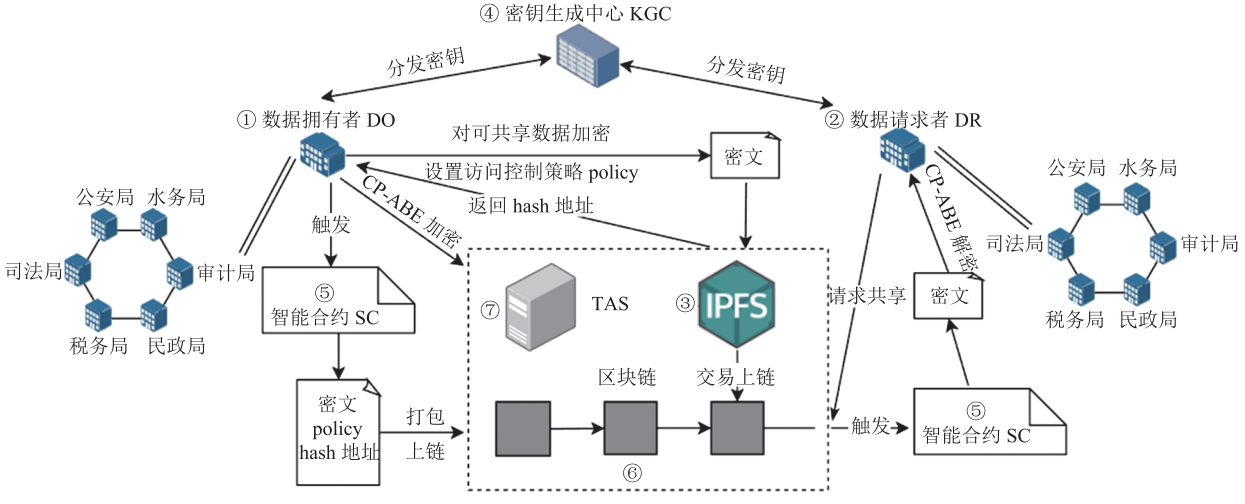

图 1　基于区块链的政务数据共享系统架构

Fig. 1　Government data sharing system architecture based on blockchain

一组节点属性，KGC 根据其属性集计算每个节点的私钥 *SK*。同时，KGC 还负责更新和撤销用户权限，以及撤销属性集。SC 代表两个或多个区块链节点之间的约束协议，其中每一方都必须按照协议履行其义务，因此，智能合约可以充当可信任的第三方[22]。此外，数据共享过程、身份验证等信息通过 SC 记录在 BC 上。本文使用 BC 和 SC 实现数据加密和共享过程中的信息跟踪，对数据加密和共享过程中所有政府部门节点的行为记录上链，方便 DO 和其他节点的审计与追踪，实现共享过程中的数据溯源，从而解决数据滥用和责任认定问题。TAS 调用改进的 CP-ABE 算法将数据拥有者的公钥 *PK* 和访问策略 *p* 作为加密算法 Encrypt 的输入，对检索密文的 hash 值 *hsahi* 进行加密，得到新的加密密文 *CT*。

本文主要参数及其含义如表 1 所示。

表 1 参数以及含义

Table 1 Parameter and meaning

参数	代表含义
λ	系统安全参数
MSK	系统主密钥
PK	系统主公钥
CT	加密数据密文
SK	用户属性私钥
encdata	AES 加密后的加密数据
K	AES 的唯一密钥
hashi	IPFS 返回的唯一 hash 值
p	访问控制策略
hashi'	索引加密后的值
S	属性集合

在本系统中，DO 和 DR 不仅代表政府的各个部门，也代表区块链中的节点，DO 和 DR 通过 CP-ABE 进行数据共享，DO 制定访问控制策略 *p*，DR 通过系统主密钥以及自身属性集生成私钥 *SK*，可有效阻止单点故障的发生。使用线性秘密共享可实现访问策略的完全隐藏，利用 AES 算法加密数据，CP-ABE 算法加密数据哈希路径的混合加密策略，增强了数据管理的灵活性。使用 Keccak 加密算法对检索数据密文的 hash 值进行重加密，实现数据的完整性验证。

3.2 算法流程

政务数据涉及行业机密和公共隐私，因此需要严格的权限管理。在传统的基于大数据中心的共享过程中，每个部门的权力和责任都是模糊的，数据的安全难以得到充分保障[7]。在基于 BC 的数据共享模式下，每个部门可以通过自主授权管理和自行指定其他部门的访问权限，避免权责不清。

每个部门通过智能合约机制自主管理其数据库，包括用户管理、访问控制和授权管理。政府部门根据数据共享的需求编写智能合约(脚本)，指定数据访问权限，然后将合约发布至其系统账户，SC 通过 BC 共识机制进行验证。通过 BC 的账户注册、身份认证和授权管理，可以记录、跟踪整个数据共享流程，保证政务数据共享网络中节点之间的信息有序流动。

综上所述，本文在 CP-ABE 算法的基础上进行改进，提出了 BT-GDS 算法。该算法由系统初始化、密钥生成、数据加密、IPFS 存储、索引加密、CP-ABE 加密、CP-ABE 解密和明文获取 8 个部分组成，如图 2 所示。具体为：(1)系统初始化，$Setup(\lambda)\rightarrow PK,MSK$。给定一个安全参数 λ，通过 Setup 算法将生成公钥 *PK* 和主密钥 *MSK*。(2)密钥生成，$KeyGen(PK,MSK,S)\rightarrow SK$。将属性集合 *S*、公钥 *PK* 和主密钥 *MSK* 作为输入，通过 KeyGen 算法生成用户私钥 *SK*。(3)数据加密，$Enc(data)\rightarrow encdata$，DO 利用唯一的 AES 密钥 *K* 对数据加密，通过 Enc 算法生成加密文件 *encdata*。(4)IPFS 存储，$IPFS(encdata)\rightarrow hashi$，加密数据通过 IPFS 存储返回唯一访问该数据的 hash 值 *hashi*。(5)索引加密，$Keccak(hashi)\rightarrow hashi'$，通过 Keccak 算法将 IPFS 返回的索引 hash 值加密为 *hashi'*。(6)CP-ABE 加密，$Encrypt(PK,hashi,p)\rightarrow CT$。输

入为公钥 *PK*、索引 hash 值 *hashi* 和访问控制策略 p，算法输出为密文 *CT*。(7)CP-ABE 解密，$Decrypt(PK,CT,SK)\rightarrow hashi$。输入为公钥 *PK*、密文 *CT* 和用户密钥 *SK*，算法输出为密文索引 hash 值 *hashi*。(8)明文获取。DR 获取 *hashi* 后，向 IPFS 分布式网络发送命令，从而获取存储在 IPFS 网络中的加密文件 *encdata*，再通过 AES 的唯一密钥 *K* 对加密文件 *encdata* 进行解密运算，得到解密后的明文 *data*。

3.3　访问控制方案

用户管理政务数据共享过程涉及多个用户，有效的用户管理是权限管理的前提。基于属性的访问控制将操作对象的权限转换为属性的权限，实现了细粒度的访问控制，大大降低了系统的复杂性，反映了系统的组织结构[12]。通过为特定用户配置不同的角色，可以为用户分配不同的权限。政府部门的相关人员需要注册 BC 的合法账户，并生成自己的公钥和私钥。当数据共享活动发生时，每个块都需要双方的公钥和私钥才能运行。

因此，本文提出的政务大数据共享方案 BT-GDS 的访问控制流程包括系统初始化、数据加密、数据解密和数据完整性验证 4 个阶段。

3.3.1　系统初始化阶段

本阶段由系统设置和密钥生成两个部分组成。

系统设置：DO 给定一个安全参数 λ，确定一个大素数 q 和对应的生成元、循环群和有限域并得到 (G,G_T,a,b,c)，其中，$G=G_a\times G_b\times G_c$，$G$ 和 G_T 均为双线性群，阶数为 abc，令 $N=abc$。在初始化阶段，DO 运行 Setup 算法生成公钥 *PK* 和主密钥 *MSK*。$Setup(\lambda)$：DO 随机选择 g_a 和 g_c，分别作为群 G_a 和群 G_c 的生成元，DO 随机选取 $R_c\in G_c$、$s_i(i\in U)\in Z_N$ 和 $\alpha,k\in Z_a$，生成系统公钥为 $PK=\left(abc,g_a,g_a^k,e(g_a,g_a)^{\alpha}\right)$，系统主密钥为 $MSK=\left\{\alpha,(s_i)_{i\in U}\right\}$。

密钥生成：该算法由密钥生成中心 KGC 为联盟链中的各个政府部门节点生成对应的密钥。KGC 为每个政府部门节点进行身份和属性认证，并为各个节点分发密钥。以司法局节点为例，KGC 为节点随机选择 $m\in Z_P^*$，对用户属性集 *N* 中的每一个属性

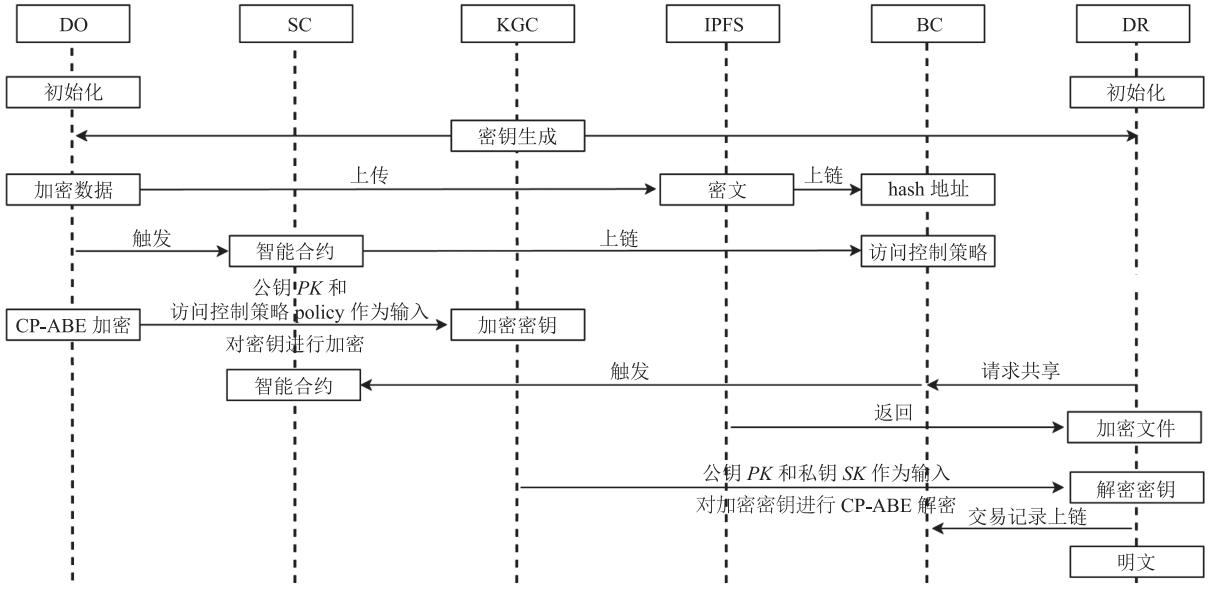

图 2　本方案流程图

Fig. 2　Flow chart of this scheme

n，计算 $L_n=PAI_n^m$，则司法局节点用户私钥 $SK=\left\{L=g^a\times g^{am},L'=g^m,\left\{L_n\middle|n\in N\right\}\right\}$。

3.3.2 数据加密阶段

本阶段由数据加密、索引加密、CP-ABE 加密 3 个部分组成。

数据加密：DO 选择其支持共享的数据（或文件），用 *data* 表示，并调用对称加密算法 AES 生成密钥 K，使用唯一密钥 K 对需要共享的数据（或文件）进行加密并生成密文 *encdata*。具体过程为：AES 算法随机选择参数 $R'_0\in G_c$ 与 $s\in Z_N$，然后计算 $D=K\cdot F^s$ 和 $D_0=B_0^s\cdot R'_0$，其中，$F=e(g_a,g_a)^\alpha$，$R_0,R_{i,j}\in Z_c$，$B_0=g_a\times R_0$，$0<i\leqslant n$，$0<j\leqslant l$，并通过公式（1）计算 $D_{i,j}$。

$$D_{i,j}=\begin{cases}B_{i,j}^s\cdot R'_{i,j}, \text{ if } v_{i,j}\in W_i\\ B_{i,j}^{s_{i,j}}\cdot R'_{i,j}, \text{ otherwise}\end{cases}\tag{1}$$

数据加密算法生成的加密数据（密文）为 $encdata=\left(D,D_0,\left\{D_{i,j}\right\}\right)$。其中，$1\leqslant i\leqslant n,1\leqslant j\leqslant l$。为缓解区块链系统的存储压力，本方案将可共享数据 *data* 的密文 *encdata* 存储在 IPFS 分布式网络中，IPFS 分布式网络将返回唯一用于检索密文的 hash 值 *hashi*，便于后续数据请求者检索密文、索引加密和 CP-ABE 加密。

索引加密：本文利用 Keccak（SHA-3）算法对检索数据密文的 hash 值 *hashi* 进行再加密生成 *hashi'*，用于后续数据的机密性和完整性验证，且索引加密完成时，会触发智能合约将控制策略 p 和加密后的索引 *hashi'* 一起打包上链，方便 DO 和其他节点的审计与追踪。Keccak 算法是 Das 等[23]联合设计的 SHA-3 算法，该算法采用不同于传统 Merkle 结构的新型海绵结构[11]，安全性较好，且擅长在安全强度和处理速度之间取得平衡。该算法提出的新型海绵结构使用有限的状态机，可接受任何长度的输入位以及任何长度的输出位。Keccak 算法的结构如图 3 所示，算法包括吸收模块和挤压模块。吸收模块先使用多重位速率的方式对输入的数据进行填充，$M_1,\cdots,M_n$ 为填充后的数据块，将此数据块依次与 r 位内部状态作异或，用 Keccak 函数作为隐藏层，在新的数据块生成之后进行同样的操作，模式类似深度学习中的多层感知机，循环 n 次后，生成的每一个数据块均被处理完成。挤压模块的主要工作是将数据块拼接为与期望输出长度相匹配的序列，若期望输出小于吸收模块的输出，则直接做截取操作；反之，则用 Keccak 函数将吸收模块的输出拼接，直至两者长度匹配。

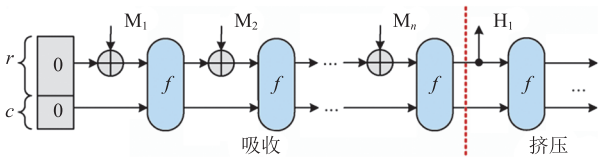

图 3 Keccak 算法结构

Fig. 3 Keccak algorithm structure

CP-ABE 加密：本文以联盟链中的交易作为载体，对整个数据共享流程进行记录和管理，由 DO 选定可共享的数据（或文件），设置特定的访问控制策略 p，当且仅当 DR 的属性集合满足 DO 所定义的特定策略时，DR 才能访问成功。DO 使用 $\boldsymbol{x}$ 表示与访问控制策略 p 关联的向量，DR 使用 $\boldsymbol{y}$ 表示与其节点属性相关的向量，当 $\boldsymbol{x}\cdot\boldsymbol{y}=0$ 时，即 DR 的属性集满足 DO 制定的访问控制策略时，DR 成功解密。在上述索引加密后，可信任的授权服务器 TAS 调用改进的 CP-ABE 算法，将数据拥有者的公钥 *PK* 和访问策略 p 作为加密算法 Encrypt 的输入，对检索密文的 hash 值 *hashi* 进行加密，得到新的加密密文 *CT*。

访问策略 $p=(\boldsymbol{O},\rho)$，其中，$\boldsymbol{O}$ 为 $m\times n$ 维的矩阵，ρ 为矩阵 $\boldsymbol{O}$ 的行指定属性，O_a 表示矩阵 $\boldsymbol{O}$ 的第 a 行（$1\leqslant a\leqslant m$）。设需要进行属性基加密的密文为 u，定义向量 $\boldsymbol{v}=(u,z_2,z_3,\cdots,z_n)$，选择随机数 $z_j\in Z_a,j=2,3,\cdots,n$，分别计算 $I_a=O_a\times\boldsymbol{v}$，

$C_c=g^s$, $C_f=\left(g^{v\times\rho(x)}\right)^{Z_j}$, $C_g=g^{a\times I_a}\times H_1\left(\rho\left(x\right)\right)^{v_i}$, $C_t=\left\{C_c,C_f,C_g\right\}$的值，最终得到密文$CT=\left((\boldsymbol{O},\rho),C_t\right)$。

3.3.3 数据解密阶段

此阶段为 DR 解密密文后获取 DO 共享数据的过程。DR 向 BC 发送共享数据请求，BC 触发 SC（query），DR 获取共享文件在 IPFS 网络中检索密文的 hash 值 *hashi'* 以及访问控制策略 *p*，随后可信任的授权服务器 TAS 利用公钥 *PK*、密文 *CT* 和用户私钥 *SK* 作为输入，调用解密算法的 Decrypt，若用户私钥的属性集满足 DO 制定的访问策略，那么解密成功，得到检索密文的 hash 值 *hashi*；否则提示权限不足，解密失败[24]。DR 获取 *hashi* 后，向 IPFS 分布式网络发送命令 *ipfs get ipfshash*，获得存储在 IPFS 网络中的加密文件 *ipfsfile*，其中 $ipfsfile=\left\{encfile\middle|encdata\right\}$。DR 利用 AES 的唯一密钥 *K* 对加密文件 *encdata* 进行解密运算，得到解密后的文件 *data*。

3.3.4 数据完整性验证阶段

在上述数据解密阶段中，当 DR 调用解密算法 Decrypt 并解密成功后，将会获得在 IPFS 分布式网络中唯一检索密文的 hash 值 *hashi*，DR 利用 Keccak（SHA-3）算法对 hash 值 *hashi* 进行重加密得到 *verhashi'*，比较索引加密的 hash 值与重加密 CP-ABE 解密后的密文得到的 hash 值是否相同。若相同，那么数据共享成功，将共享成功的交易写入 BC，说明文件在整个共享流程中没有被篡改，数据的完整性和机密性得到保证；否则，共享失败，提示数据可能被恶意节点篡改。

4　安全性分析

4.1　数据安全性

本节将从数据安全可信共享、隐私保护、机密性、数据完整性、可溯源等 5 个方面进行数据安全性分析。

（1）数据安全可信共享。本文提出的 BT-GDS 方案中的数据共享依赖于区块链结构，区块链作为一种链式存储结构，将数据区块按照时间顺序以链条的形式连接起来，非创世区块上都存有上一区块和下一区块的 hash 值，保证数据不可伪造、不可篡改。若某一恶意节点想要篡改区块数据，那么需要对所有区块链上的历史区块进行攻击。设恶意节点每秒生成区块的概率为 *v*，数据共享系统中的区块链每秒生成区块的概率为 *s*，恶意节点需要攻击的区块高度为 *h*，在此条件下，恶意节点在 *t* s 内生成 *x* 次区块，其他诚实节点生成 *y* 次区块[25]，则在 *t* s 内总计未生成区块 $(t-x-y)$ 次，恶意节点若想成功篡改区块，则必须满足 $x\geqslant y+h$。恶意节点篡改成功的概率 *P* 可由公式（2）计算得出。

$$P=\sum_{x=0}^{(t-1-h)/2}\sum_{n=1}^{t-2x-h}\frac{t!/x!\left(n+h+x\right)!\left(t-2x-n-h\right)!}{v\left(1-s\right)^x s\left(1-v\right)^{n+h+x}\left(1-v\left(1-s\right)-s\left(1-v\right)\right)^{t-h-n-2x}}\tag{2}$$

（2）当恶意节点算力为诚实节点算力的 30%，且区块高度为 2 时[26]，恶意节点篡改成功的概率约为 0.001，而实际中需要篡改的区块高度较高，且恶意节点的算力十分有限，因此，本文基于区块链的数据共享方案安全可信。

隐私保护。政务数据包含大量用户以及企业的敏感数据，在共享过程中，做好数据的隐私保护工作尤为重要。在本文框架中，DO 将可共享数据先进行 AES 加密，再上传到 IPFS 分布式网络，消除了不诚实的云服务器窃听用户私人数据的风险。此外，在 BC 中，DO 只将智能合约生成的数据信息描述摘要上传至 BC，避免了 BC 中的恶意节点篡改数据。本文提出的 BT-GDS 系统架构包含多个政府部门节点，如司法局、公安局、水务局等，该架构在一定程度上避免了私有链中将认证和审计权完全交给特定的权威节点，降低了单点故障、权威节点信任危机等风险。

（3）机密性。为确保没有恶意节点能够解密

已发布的数据，本方案使用 AES 和 CP-ABE 加密算法，以确保数据的机密性。在本文模型中，DO 首先利用对称密钥对共享的政务数据进行数据加密，然后将加密的密文上传至 IPFS，并将对称密钥存储在 BC 上。即使 IPFS 是恶意的，也无法获取数据的明文，因为其属性无法匹配访问策略，所以无法获取和解密出对称密钥。此外，DO 使用 CP-ABE 算法将对称密钥进行加密，然后将密文上传至区块链。只有具有属性私钥的数据用户才能对密文进行解密，使得整个系统的机密性更加完整。

(4)数据完整性。DR 调用解密算法并且解密成功后会获得 IPFS 分布式网络中唯一检索密文的 hash 值，DR 将利用 Keccak 算法对 hash 值进行重加密得到的值和索引加密得到的 hash 值进行比较。一旦数据在边缘存储层被篡改，数据用户将通过重新计算完整数据的 hash 摘要来检测问题。此外，在数据存储或传输过程中，没有区块链网络层的授权，任何人都不能修改或窃听数据。

(5)可溯源。在本文提出的 BT-GDS 方案中，系统初始化、密钥生成、数据加密、索引加密、CP-ABE 解密均在链下进行计算，在 BC 上借助事务进行相关参数数据的传递，任何请求和授权记录均作为不可篡改的交易存储在区块链上，因此，BC 上任意一个节点的数据共享过程都可进行追溯。当政府部门发生业务共享需求时，每个部门对数据的操作都将记录在区块链的账本上，管理人员可通过查阅区块链账本实现数据追踪，从而解决数据滥用和责任认定问题。

4.2 算法安全性

本文提出的政务大数据共享方案 BT-GDS 的算法安全性论证基于 q-parallel BDHE 问题假设，即在随机预言机下，若不存在一种算法，使得敌手 B 攻破算法的优势 τ 可忽略不计，则说明该方案的算法是安全的。下面定义本方案的安全模型。

假设 1：定义一个群生成算法 γ，分布如下:

$$(N=abc,G_T,e,G)\leftarrow\gamma(\lambda),g_a\leftarrow G_a,$$
$$g_c\leftarrow G_c,X_3\leftarrow G_c,F=(N,G,G_T,e,g_a,X_3)$$
$$P_1\leftarrow G_a\times G_b,P_2\leftarrow G_a$$

定义任意一个敌手 ϑ，其攻破假设 1 的优势由公式(3)所示。

$$Adv1_{\vartheta}=\left|\Pr\left[\vartheta(F,P_1)=1\right]-\Pr\left[\vartheta(F,P_2)=1\right]\right| \quad (3)$$

对于任意一个群生成算法 γ 和一个多项式时间内的算法，若敌手 ϑ 攻破假设 1 的优势 $Adv1_{\vartheta}<\theta$，且 θ 是可忽略的，那么由 q-parallel BDHE 问题假设可知，算法 γ 满足假设 1。

假设 2：定义一个群生成算法 δ，分布如下：

$$(N=abc,G_T,e,G)\leftarrow\delta(\lambda),g_a\leftarrow G_a,$$
$$(g_a,X_1)\leftarrow G_a,(X_2,Y_2,Z_2)\leftarrow G_b,X_3\leftarrow G_c,$$
$$F=(X_1X_2,X_3,Y_2Y_3,N,G,G_T,e,g_a),P_1\leftarrow G,P_2\leftarrow G_a\times G_b$$

定义任意一个敌手 μ，其攻破假设 2 的优势如公式(4)所示。

$$Adv2_{\mu}=\left|\Pr\left[\mu(F,P_1)=1\right]-\Pr\left[\mu(F,P_2)=1\right]\right| \quad (4)$$

同理，对于任意一个群生成算法 δ 和一个多项式时间内的算法，若敌手 μ 攻破假设 2 的优势 $Adv2_{\mu}<\theta$，且 θ 是可忽略的，那么由 q-parallel BDHE 问题假设可知，算法 δ 满足假设 2。

假设 3：定义一个群生成算法 ρ，分布如下：

$$(N=abc,G_T,e,G)\leftarrow\rho(\lambda),g_a\leftarrow G_a,$$
$$\alpha,s\leftarrow Z_N,g_a\leftarrow G_a,(X_2,Y_2,Z_2)\leftarrow G_a,X_3\leftarrow G_c$$
$$F=\left(g_a^{\alpha}X_2,X_3,g^sY_2,Z_2,N,G,G_T,e,g_a\right),$$
$$P_1\leftarrow e(g,g)^{\alpha s},P_2\leftarrow G_T$$

定义任意一个敌手 σ，其攻破假设 3 的优势由公式(5)所示。

$$Adv3_{\sigma}=\left|\Pr\left[\sigma(F,P_1)=1\right]-\Pr\left[\sigma(F,P_2)=1\right]\right| \quad (5)$$

同理，对于任意一个群生成算法 ρ 和一个多项式时间内的算法，若敌手 σ 攻破假设 3 的优势 $Adv3_{\sigma}<\theta$，且 θ 是可忽略的，那么由 q-parallel BDHE 问题假设可知，算法 ρ 满足假设 3。

定理 1：如若上述假设 1～3 成立，那么本文

提出的 BT-GDS 算法是安全的。

证明 为证明本文所提 BT-GDS 算法的安全性，需要引入功能性密文和半功能性密文[6]，具体证明见 Shi 等[14]的研究。

5　实验分析

本实验实现了一个原型以分析政务大数据共享方案 BF-GDS 的可行性和性能。实验平台和环境的具体配置如下：操作系统为 Ubuntu 20.04.2 LTS；处理器为 Intel Core i5-9400F CPU @ 2.90 GHz，16 GB 内存；编程语言为 Go 和 C＋＋。本实验搭建了 IPFS 及 CP-ABE 环境，BC 采用 Hyperledger Fabric 1.4。在不同数据大小以及不同属性个数的情况下，对本文方案加解密的时间开销进行测试，并与其他方案进行对比。其中，数据集大小分别设置为 1 MB、10 MB、50 MB、100 MB、500 MB；属性个数分别设置为 1、3、5、7、9。此外，针对不同数据集大小，本实验还测试了方案中 IPFS 数据上传和下载的时间开销，并与传统云服务器的上传和下载时间开销进行了对比。所有实验均重复进行 100 次，最终结果取平均值。

5.1　结果分析

5.1.1　加解密时间分析

由于政务数据共享的时间开销集中在数据加密和数据解密阶段，本实验将从数据加密时间、数据解密时间等方面，将本模型与 Shi 等[14]和芦效峰等[21]的研究进行比较。Shi 等[14]将 CP-ABE 与 BC 相结合，实现了交易的动态溯源和隐私保护；芦效峰等[21]将 KP-ABE 与线性秘密共享结合，实现了系统的细粒度访问控制。当文件数据集大小不同时，各方案的加解密时间对比结果如图 4～5 所示。由图 4～5 可知，当文件数据集较小时，各方案的加解密时间没有较大差异，当文件数据集为 500 MB 时，本方案的加解密时间明显减少。

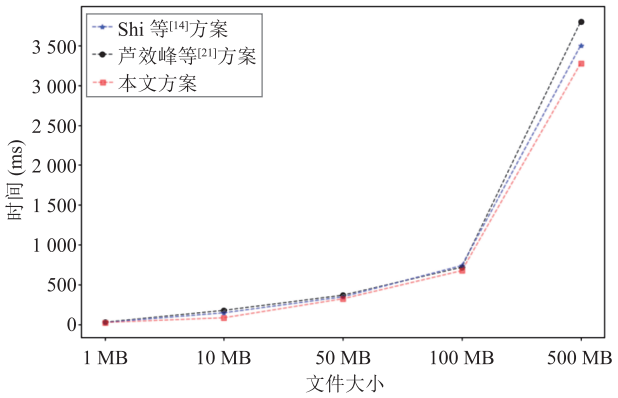

图 4　不同文件大小加密时间对比

Fig. 4　Comparison of encryption time of different file sizes

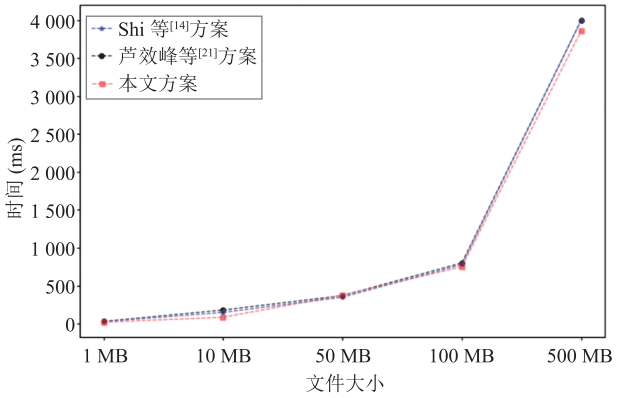

图 5　不同文件大小解密时间对比

Fig. 5　Comparison of decryption time of different file sizes

当属性个数不同时，各方案的加解密时间对比结果如图 6～7 所示。由图 6 可知，系统的加密时间开销随着访问属性增加而增加，当属性个数较少时，各方案的加密时间没有较大差异，在属性个数为 5 时，与其他两方案相比，本文方案约有 15% 的提升；由图 7 可知，本文方案在解密方面的时间开销较其他两方案明显较少，且随着访问属性数量的进一步增长，解密时间趋于平稳，这对在实际数据共享系统中的用户较为友好。综上所述，本文方案较其他两方案有着更低的加解密时间开销，且在用户访问属性较多、访问结构较复杂时，解密时间较为稳定，对实际数据共享系统的用户节点更友好。

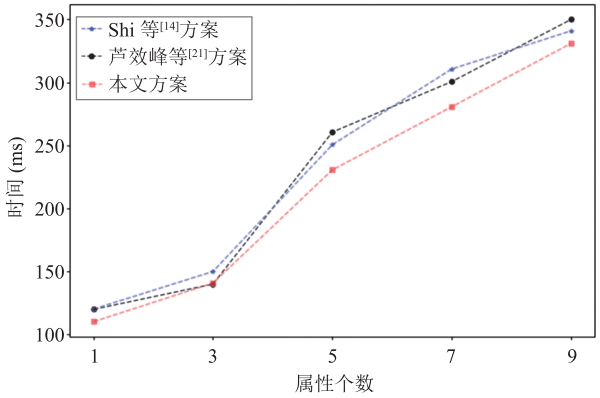

图 6 不同属性个数加密时间对比

Fig. 6 Comparison of encryption time of different attribute numbers

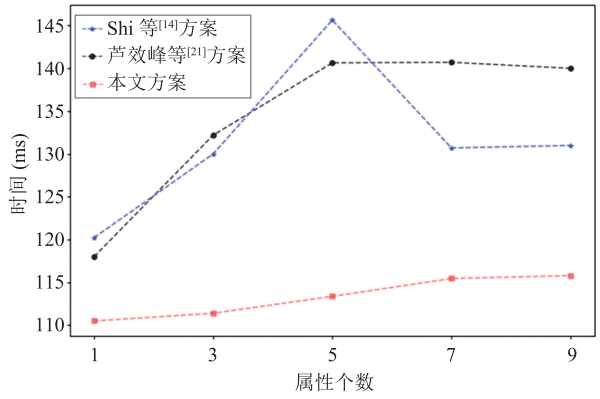

图 7 不同属性个数解密时间对比

Fig. 7 Comparison of decryption time of different attribute numbers

5.1.2 数据存储分析

本模块实验为不同大小数据集条件下，传统云服务器存储与 IPFS 分布式网络存储的性能比较。本文数据集大小分别为 500 kB、1 MB、2 MB、3 MB、4 MB，对于每个不同大小的数据，在 IPFS 和云服务器上分别测试 100 次上传和下载的时间开销，并计算其平均值。实验结果如表 2 和表 3 所示。

图 8～9 更直观地比较了上述两种方案的上传和下载时间开销。由图 8 可知，当数据大小约为 500 KB 和 1 MB 时，与云服务器相比，本文方案的数据上传速度较慢；但随着数据规模的增

表 2 IPFS 和云服务器上传时间对比表

Table 2 Comparison table of upload time between IPFS and cloud server

	500 kB	1 MB	2 MB	3 MB	4 MB
本文方案上传时间 (ms)	73.47	178.10	182.07	195.67	207.57
云服务器上传时间 (ms)	69.85	139.70	279.40	419.11	558.81

表 3 IPFS 和云服务器下载时间对比表

Table 3 Comparison table of download time between IPFS and cloud server

	500 kB	1 MB	2 MB	3 MB	4 MB
本文方案下载时间 (ms)	2.15	4.30	8.61	12.92	17.23
云服务器下载时间 (ms)	74.53	173.90	188.73	197.53	206.35

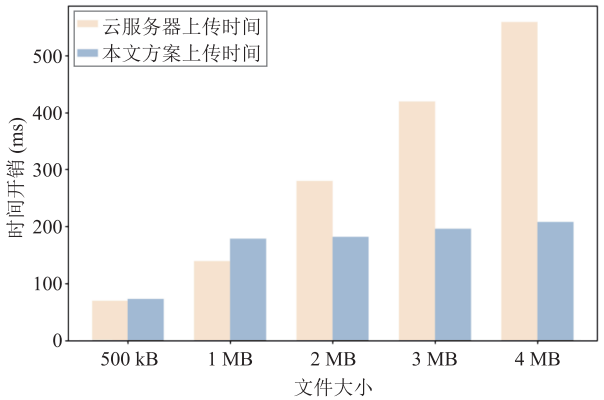

图 8 数据上传时间对比

Fig. 8 Comparison of data upload time

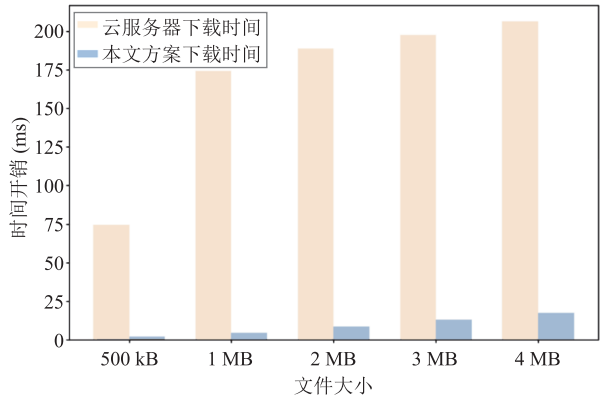

图 9 数据下载时间对比

Fig. 9 Comparison of data download time

加，本文方案的上传时间开销约为云服务器的50%。因此，当数据较小时，云服务器可能比本文方案的上传速度快，但当数据较大时，本文方案的上传速度有较大优势。由图 9 可知，本文方案的下载时间开销约为云服务器的 8%。综上所述，本文方案采用 IPFS 分布式存储可极大地减少时间开销，提升系统的运行效率。

5.2　方案对比

郭丽峰等[20]的研究与本文工作类似，但没有考虑文件较大时的加密效率问题；Shi 等[14]在访问控制方面进行了研究，但没有采用分布式存储，导致数据较大时 BC 的存储压力急剧上升，可扩展性较差；Piao 等[13]采用分布式存储，减小了 BC 的存储压力，但数据共享及存储都依赖于可信的第三方机构，可能出现单点故障，导致数据在共享过程中被恶意篡改。本文方案将密文 ABE 与 BC 相结合，实现对数据的细粒度访问控制；采用 IPFS 分布式存储，降低区块链的存储压力，保证数据在共享过程中的效率；使用 BC 和 SC 实现数据加密和共享过程中的信息跟踪，通过对所有参与者的行为记录上链，实现共享过程中的数据溯源，解决数据滥用和责任认定问题。本文方案与其他方案的对比分析如表 4 所示。

6　总结与展望

传统政务数据共享系统一般采用集中式共享模式，但集中式共享易引发各种问题，如数据隐私泄露、部门权限问题、单点故障等，因此，本文提出了一种 ABE 与 BC 相结合的政务数据共享方案。在该方案中，由 DO 制定访问控制策略，对 DR 的属性进行限制，利用子集覆盖技术，实现数据安全共享中的细粒度访问控制及密钥更新，密钥生成中心充当区块链中的节点，通过区块链的去中心化特性解决了传统密钥生成节点不可信或半可信的问题，使组织之间的通信和协作变得高度安全。安全性分析和实验分析的结果表明，本文方案不仅实现了细粒度的访问控制和数据的精确管理，而且可对数据共享的过程进行追溯，解决了数据滥用和责任认定问题。实验表明，当文件数据集较大时，与同类方案相比，本文方案的加密和解密开销较低，通过链上链下共同存储，大大减少了区块链的存储压力。目前，本研究还存在一定的局限性，未来将进一步深入研究，在算法上考虑结合代理重加密，并对其安全性与效率进行测试，在模拟政府部门数据上传和下载的实验中增大数据规模，最终搭建基于区块链的政务大数据共享平台，针对整体系统进行并发访问与性能测试。

参 考 文 献

[1] 闫冠辰, 姜顺荣, 李胜利, 等. 基于联盟链的安全和支持高效模糊查询的电子病历共享系统 [J]. 密码学报, 2022, 9(5): 805-819.
Yan GC, Jiang SR, Li SL, et al. Secure and efficient fuzzy search for EHR sharing based on consortium blockchain [J]. Journal of Cryptologic Research, 2022, 9(5): 805-819.

[2] 马英. 政务数据共享授权决策模型研究 [J]. 信息

表 4　本文方案与其他方案的对比分析

Table 4　Comparison between the scheme in this paper and other schemes

方案	访问控制	分布式存储	隐私保护	完整性验证	可扩展性
Shi 等[14]的方案	强	弱	强	强	弱
Piao 等[13]的方案	强	强	弱	强	弱
郭丽峰等[20]的方案	弱	强	强	强	强
本文方案	强	强	强	强	强

安全与通信保密, 2021, (10): 67-74.
Ma Y. Authorization decision model for government data sharing [J]. Information Security and Communications Privacy, 2021, (10): 67-74.

[3] 张晓东, 陈韬伟, 余益民, 等. 基于区块链和密文属性加密的访问控制方案 [J]. 计算机应用研究, 2022, 39(4): 986-991.
Zhang XD, Chen TW, Yu YM, et al. Access control scheme based on blockchain and CPABE [J]. Application Research of Computers, 2022, 39(4): 986-991.

[4] Ge CP, Liu Z, Fang L. A blockchain based decentralized data security mechanism for the internet of things [J]. Journal of Parallel and Distributed Computing, 2020, 141: 1-9.

[5] 郭海洲, 褚全红, 龚思扬, 等. 基于区块链技术的柴油机电控系统数据共享平台研究 [J]. 现代电子技术, 2022, 45(19): 173-177.
Guo HZ, Chu QH, Gong SY, et al. Research on data sharing platform for diesel engine electronic control system based on blockchain technology [J]. Modern Electronics Technique, 2022, 45(19): 173-177.

[6] 汪金苗, 王国威, 王梅, 等. 面向雾计算的隐私保护与访问控制方法 [J]. 信息网络安全, 2019, (9): 41-45.
Wang JM, Wang GW, Wang M, et al. Achieving privacy preserving and flexible access control in fog computing [J]. Netinfo Security, 2019, (9): 41-45.

[7] Dinh TTA, Liu R, Zhang MH, et al. Untangling blockchain: a data processing view of blockchain systems [J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 30(7): 1366-1385.

[8] Porwal S, Mittal S. A fully flexible key delegation mechanism with efficient fine-grained access control in CP-ABE [J]. Journal of Ambient Intelligence and Humanized Computing, 2022. https://doi.org/10.1007/s12652-022-04196-y.

[9] 杜瑞忠, 张添赫, 石朋亮. 基于区块链且支持数据共享的密文策略隐藏访问控制方案 [J]. 通信学报, 2022, 43(6): 168-178.
Du RZ, Zhang TH, Shi PL. Ciphertext policy hidden access control scheme based on blockchain and supporting data sharing [J]. Journal on Communications, 2022, 43(6): 168-178.

[10] Li T, Wang HQ, He DB, et al. Blockchain-based privacy-preserving and rewarding private data sharing for IoT [J]. IEEE Internet of Things Journal, 2022, 9(6): 15138-15149.

[11] Li D, Han DZ, Zheng ZB, et al. MOOCsChain: a blockchain-based secure storage and sharing scheme for MOOCs learning [J]. Computer Standards & Interfaces, 2022, 81: 103597.

[12] Ma CJ, Li Y. Government information sharing scheme for cross-departmental collaboration [C] // Proceedings of the 2020 International Signal Processing, Communications and Engineering Management Conference, 2020: 169-172.

[13] Piao C, Hao YR, Yan JQ, et al. Privacy preserving in blockchain-based government data sharing: a service-on-chain (SOC) approach [J]. Information Processing & Management, 2021, 58(5): 102651.

[14] Shi DL, Cao CJ, Ye J. Secure government data sharing based on blockchain and attribute-based encryption [C] // Proceedings of the International Symposium on Security and Privacy in Social Networks and Big Data, 2022: 324-338.

[15] 陈思琦, 黄汝维. 支持连接关键词搜索的属性加密方案研究 [J]. 计算机工程与科学, 2021, 43(7): 1219-1225.
Chen SQ, Huang RW. Attribute-based encryption supporting conjunctive keyword [J]. Computer Engineering & Science, 2021, 43(7): 1219-1225.

[16] 张嘉懿. 无线体域网中公钥可搜索加密方案 [J]. 现代计算机, 2017, (5): 14-17.
Zhang JY. Public key encryption with keyword search in wireless body area network [J]. Modern Computer, 2017, (5): 14-17.

[17] 沈剑, 周天祺, 曹珍富. 云数据安全保护方法综述 [J]. 计算机研究与发展, 2021, 58(10): 2079-2098.
Shen J, Zhou TQ, Cao ZF. Protection methods for cloud data security [J]. Journal of Computer Research and Development, 2021, 58(10): 2079-2098.

[18] 闫玺玺, 何广辉, 于金霞. 可验证的密文策略属性基加密安全外包方案 [J]. 密码学报, 2020, 7(5): 628-642.

Yan XX, He GH, Yu JX. Secure and verifiable outsourced ciphertext policy attribute-based encryption [J]. Journal of Cryptologic Research, 2020, 7(5): 628-642.

[19] 严新成, 陈越, 巴阳, 等. 支持用户权限动态变更的可更新属性加密方案 [J]. 计算机研究与发展, 2020, 57(5): 1057-1069.
Yan XC, Chen Y, Ba Y, et al. Updatable attribute-based encryption scheme supporting dynamic change of user rights [J]. Computer Engineering & Science, 2020, 57(5): 1057-1069.

[20] 郭丽峰, 王倩丽. 自适应安全的带关键字搜索的外包属性基加密方案 [J]. 计算机应用, 2021, 41(11): 3266-3273.
Guo LF, Wang QL. Adaptive secure outsourced attribute-based encryption scheme with keyword search [J]. Journal of Computer Applications, 2021, 41(11): 3266-3273.

[21] 芦效峰, 付淞兵. 属性基加密和区块链结合的可信数据访问控制方案 [J]. 信息网络安全, 2021, 21(3): 7-14.
Lu XF, Fu SB. A trusted data access control scheme combining attribute-based encryption and blockchain [J]. Netinfo Security, 2021, 21(3): 7-14.

[22] Sun K, Gao HY. Adaptively secure KP-ABE for circuits with fan-in *n* and fan-out 1 [J]. The Computer Journal, 2022. https://academic.oup.com/comjnl/advance-article-abstract/doi/10.1093/comjnl/bxac105/6649279?login=false.

[23] Das S, Namasudra S. Multi-Authority CP-ABE-based access control model for IoT-enabled healthcare infrastructure [J]. IEEE Transactions on Industrial Informatics, 2022, 19(1): 821-829.

[24] Kumar S, Bharti AK, Amin R. Decentralized secure storage of medical records using blockchain and IPFS: a comparative analysis with future directions [J]. Security and Privacy, 2021, 4(5): e162.

[25] Jaiman V, Pernice L, Urovi V. User incentives for blockchain-based data sharing platforms [J]. PLoS One, 2022, 17(4): e0266624.

[26] Wee H. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions [C]// Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2022: 217-241.