

基于双联盟链的工业物联网安全数据共享架构

李晓伟, 张维江, 段文钰, 何远, 杨邓奇, 杨毅宇

(大理大学数学与计算机学院, 云南 大理 671003)

摘要: 频繁的数据交互与共享是工业物联网的典型特点之一。密文策略的属性加密 (ciphertext-policy attribute-based encryption, CP-ABE) 为数据交互与共享提供了安全的保障。然而基于单链的CP-ABE算法未将数据和属性进行隔离, 链式结构的持续延伸导致数据共享与属性撤销效率低。为解决上述问题, 提出一种基于双联盟链的工业物联网数据共享架构。该架构中的双链由属性联盟链和数据联盟链组成, 通过两条联盟链分别将属性权限和数据存储独立管理, 解决单链CP-ABE方案中属性和数据未分离问题。在属性联盟链中提出属性单向哈希链, 解决属性批量撤销困难的问题。同时, 采用链上链下协同存储机制存储共享数据, 缓解单一区块链的存储压力。最后基于FISCO BCOS平台实现了上述的双联盟链架构。

关键词: 工业物联网; 数据共享; 双联盟链; 属性单向哈希链; 属性加密

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025043

Secure data sharing architecture for industrial Internet of things based on dual consortium chains

LI Xiaowei, ZHANG Weijiang, DUAN Wenyu, HE Yuan, YANG Dengqi, YANG Yiyu

School of Mathematics and Computer Science, Dali University, Dali 671003, China

Abstract: Frequent data interaction and sharing were identified as typical characteristics of the Industrial Internet of Things (IIoT). Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was recognized as providing a secure foundation for data interaction and sharing. However, traditional CP-ABE schemes based on a single blockchain were found to lack isolation between data and attributes, and the continuous expansion of the chain structure resulted in low efficiency in both data sharing and attribute revocation. To address these issues, a data sharing architecture for IIoT based on a dual consortium chain was proposed. In this architecture, the dual chain consisted of an attribute consortium chain and a data consortium chain, which independently managed attribute permissions and data storage, respectively, thereby resolving the inseparability of attributes and data inherent in single-chain CP-

收稿日期: 2025-04-29; **修回日期:** 2025-07-13

通信作者: 李晓伟, lixiaowei_xidian@163.com

基金项目: 国家自然科学基金 (62262001); 云南省兴滇人才计划项目 (XDYC-QNRC-2022-0137)

Foundation Items: The National Natural Science Foundation of China (62262001), Yunnan Xingdian Talents Support Program (XDYC-QNRC-2022-0137)

引用格式: 李晓伟, 张维江, 段文钰, 等. 基于双联盟链的工业物联网安全数据共享架构[J]. 网络与信息安全学报, 2025, 11(4): 73-85.

Citation Format: LI X W, ZHANG W J, DUAN W Y, et al. Secure data sharing architecture for industrial Internet of things based on dual consortium chains[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 73-85.

ABE schemes. Within the attribute consortium chain, an attribute one-way hash chain was introduced to overcome the challenges associated with batch attribute revocation. Additionally, a collaborative on-chain and off-chain storage mechanism was adopted to store shared data, alleviating the storage burden on any single blockchain. Finally, the described dual consortium chain architecture was implemented using the FISCO BCOS platform.

Keywords: industrial IoT, data sharing, dual consortium chain, unidirectional hash chain of attributes, attribute-based encryption

0 引言

工业 4.0 背景下, 工业物联网呈快速发展趋势。智能设备、5G 移动通信、云计算的广泛使用进一步推动了工业物联网的发展^[1]。工业物联网中大规模传感器及设备会产生海量数据, 随着数据交互与共享的日益增长, 数据安全问题日益凸显, 已成为制约工业物联网进一步发展的关键挑战^[2]。

为解决上述问题, 研究者将基于密文策略的属性加密 (ciphertext-policy attribute-based encryption, CP-ABE) 引入工业物联网数据共享场景中^[3]。CP-ABE 允许数据所有者根据数据使用者的属性制定访问策略对数据进行加密, 从而控制数据共享权限。这种方法将访问控制直接嵌入加密过程, 确保只有满足特定属性集合的数据使用者才能解密和访问数据, 在提升数据共享便捷性的同时显著增强安全性。然而, 基于 CP-ABE 的工业物联网数据共享架构将数据集中存储在云上, 存在单点故障的风险, 因此, 亟须探索更为有效的安全数据共享机制^[4-5]。

区块链是一种去中心化的点对点系统与分布式不可变账本^[6], 能够提供高效、透明的数据管理与控制机制, 保障数据的完整性、透明度和可信度, 成为保护敏感工业物联网数据的理想选择。将区块链与 CP-ABE 相结合, 既可确保访问控制的有效性, 又能规避数据存储的单点故障风险^[7-10]。但传统的基于单链的 CP-ABE 机制依然存在以下两个问题:

1) 未将数据和属性进行隔离, 存在动态权限管理缺陷;

2) 属性撤销时需遍历全量密文数据, 导致撤销效率降低。

针对以上问题, 本文提出了基于双联盟链的工业物联网数据共享架构, 通过该架构将数据和

属性权限管理分离, 提供安全的数据共享机制。同时在此架构中提出属性单向哈希链实现属性批量撤销。最后实现了该方案的核心双联盟链架构。具体研究内容如下。

1) 设计基于双联盟链的工业物联网数据共享架构。双联盟链由属性联盟链和数据联盟链组成, 分别对数据和属性权限进行管理, 实现数据和属性分离, 从而解决单链中数据与属性冗余问题。

2) 针对单链属性撤销困难问题, 在属性联盟链中设计属性单向哈希链, 实现属性加密数据共享时的高效属性撤销。

3) 基于 FISCO BCOS 平台部署并验证双联盟架构。

1 相关工作

Hohenberger 等^[11]首次提出密钥策略属性基加密方案, 有效解决了密文或私钥中使用的属性数量设限问题, 突破了解密效率随属性数量线性增长的长期瓶颈。进一步地, 提出通用可调框架, 允许用户根据自身需求在 GPSW (goyal - pandey-sahai-waters) 低存储开销到该方案极速解密间自主调节, 且无须更新公共参数或加密算法。Zhang 等^[12]提出基于双权威机构协同密钥生成的新型 ABE 方案, 有效解决云环境密钥托管与滥用问题。随着区块链技术的日益成熟, 研究者开始探索区块链与属性加密融合的方案。

郑丽娟等^[13]提出一种结合区块链与属性加密的数据共享方案, 通过多授权中心协同管理密钥以消除单点信任风险, 并采用代理解密服务降低用户计算负担。该方案通过区块链实现策略更新记录与操作审计, 支持动态属性撤销和访问追溯功能。左娇等^[14]提出一种基于区块链和密文策略属性基加密的跨域认证方案。利用模糊提取技术保护用户身份信息不被泄露, 结合区块链技

对称密钥, 随后从云存储上获取原始数据的密文。

3) 数据所有者 (data owner, DO)。工业物联网数据提供方。数据所有者可以制定访问策略, 与属性授权机构交互, 以限定数据使用者的访问权限。此外, 数据所有者负责对原始工业物联网数据使用对称加密后将密文上传到云存储上, 并获取从云存储返回的数据存储位置, 随后将对称密钥和数据进行属性加密, 并将加密后的密文上传至数据联盟链。

4) 属性授权机构 (attribute authority, AA)。负责系统初始化、数据使用者注册与认证、密钥生成、属性撤销等任务。它通过生成系统的公钥和主密钥来初始化系统, 并为 DU 分配唯一标识符和属性公钥, 确保数据使用者身份的认证。AA 还为每个数据使用者生成对应的密钥, 并通过属性匹配控制数据访问权限。在需要撤销数据使用者访问时, 它更新数据使用者的属性公钥, 并通过智能合约在属性联盟链上执行撤销操作。

5) 云存储 (cloud storage, CS)。云存储负责存储加密后的数据, 以减轻区块链的存储压力, 同时提供存储数据的地址并将其返回给数据联盟链。云存储还需要确保数据的安全性, 支持数据的可靠存储和后续的读取与下载操作。

2.2 双链细节

2.2.1 属性联盟链

如何高效地进行属性撤销是属性加密中的一个关键问题。为此, 本文提出属性单向哈希链以实现属性的高效撤销。链中首节点 X_0 标记整条哈希链的状态信息, 后续节点存储数据使用者的属性信息, 包括身份标识 X_{uid} 和属性公钥 $e_{X[uid]}$ 。首节点 X_0 的哈希值 $H_0 = H(\text{null})$, 节点 X_{i+1} 的哈希值由节点 X_i 的哈希值 H_i 和该节点数据使用者的属性信息 X_{uidi+1} 和 $e_{X[uidi+1]}$ 计算得到。 $H_{i+1} = H(H_i || X_{uidi+1} || e_{X[uidi+1]})$ 。

属性单向哈希链存储结构如图 2 所示。本文将上述提出的属性单向哈希链结合到属性联盟链中。属性单向哈希链的独特性在于可以快速地验证用户属性是否合法, 从而提升属性验证的效率。由于每个工业物联网机构的属性信息是相互独立的, 当图 2 中属性单向哈希链的首节点状态失效时, 整条属性哈希链中所有节点的状态同时

失效, 进而实现高效的属性撤销。属性联盟链结构如图 3 所示。

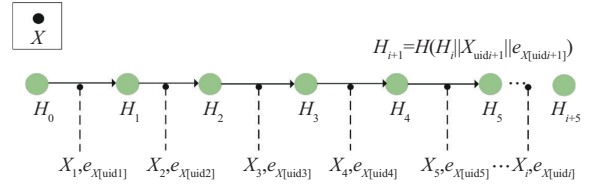


图 2 属性单向哈希链存储结构

Figure 2 Storage structure of unidirectional hash chain for attributes

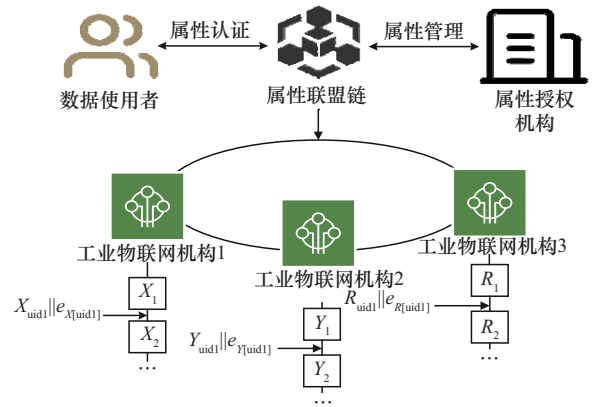


图 3 属性联盟链结构

Figure 3 Structure of attribute consortium chain

属性联盟链作用如下。

1) 属性信息上链。以图 2 中的 X 链为例, 属性授权机构把符合访问策略的第一个数据使用者身份标识 X_{uid1} 和属性公钥 $e_{X[uid1]}$ 上传至属性联盟链, 属性联盟链中的智能合约找到链中的节点 X_1 通过哈希函数计算得到 X_1 节点的哈希值 $H_1 = H(H_0 || X_{uid1} || e_{X[uid1]})$, 并将该节点的状态标记为“已认证”。后续认证时数据使用者仅需提交 X_{uid1} 和 $e_{X[uid1]}$ 到属性联盟链上, 智能合约检索哈希链, 若哈希链中查找到区块被标记为“已认证”, 则属性认证通过。

2) 数据使用者的访问权限撤销。当数据使用者的访问权限被撤销时, 数据所有者上传新的访问策略到属性授权机构, 属性授权机构将数据使用者之前的属性集合与新的访问策略进行匹配。若不符合新的访问策略, 则将 X_1 节点状态标记为“无效”状态。此时数据使用者用更新前的 X_{uid1} 和 $e_{X[uid1]}$ 再次提交到属性联盟链上后, 智能合约计算 H_1 的值并访问其状态为“无效”状态,

即完成权限撤销。

3) 批量撤销。当某个工业物联网机构被取消访问权限时,通过属性联盟链中的智能合约将该机构属性单向哈希链中的首节点的状态位标记为“无效”。由于 $H_{i+1} = H(H_i || X_{uidi+1} || e_{X[uidi+1]})$, 当 H_0 失效时会导致 H_1 失效, H_1 失效后 H_2 也失效, 如此往复, 整条属性单向哈希链的其余节点哈希值均为无效。即当一条属性单向哈希链中的首节点的状态位为无效时, 这条属性单向哈希链就失去了有效性, 从而实现批量撤销操作(单向哈希链虽然大大增加了批量撤销效率, 但是批量撤销后用户权限会消失, 若从灵活性角度出发, 用户部分属性仍需要保留, 可通过增加子链等方法实现, 这里不再详述)。属性批量撤销如图4所示。

针对哈希链鲁棒性问题, 即单向哈希链作为连续验证过程, 若中间节点被篡改导致后续节点验证失败的问题。事实上, 本文的哈希链在每个节点验证通过后需要将属性公钥等信息部署到属性链中, 后续节点均从属性链上读取数据并完成验证。因此, 若有伪造节点导致中间节点验证失败, 那么其数据不会记录到属性链中, 仅真实节点的信息被更新到属性链, 从而保证了整条链验证的完整性。

2.2.2 数据联盟链

数据联盟链存储数据块 D_n , 该数据块由密文 MST_n 和唯一的数据标识符 $dataId$ 组成。 MST_n 由数据在云存储中的存储地址 CS_{addr} 、对称密钥 M_{SE} 和 MAC 密钥 M_{MAC} 组成。此外, 在数据联盟链中部署智能合约, 以实现数据的自动化管理, 如图5所示。

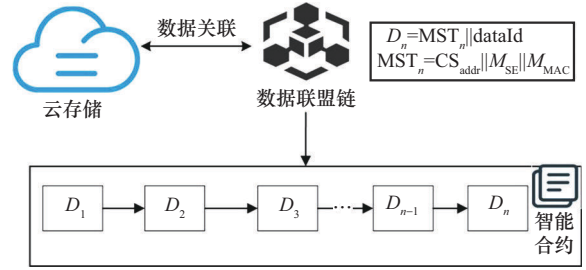


图5 数据联盟链结构

Figure 5 Structure of data consortium chain

数据联盟链的作用如下。

1) 保证数据安全。数据拥有者使用对称密钥 M_{SE} 将数据加密, 将加密后的密文存储到云存储上, 云存储返回存储地址 CS_{addr} 给数据拥有者。之后数据拥有者生成唯一的数据标识符 $dataId$, 并将 CS_{addr} 和用来解密的对称密钥 M_{SE} , 以及用于数据完整性校验的 M_{MAC} 使用属性加密得到轻量级密文 MST , 生成数据块 D_n 进行上链, 用于后续的数据查询。这种设计不仅减轻了链上存储压力, 还确保了数据的安全性。这里需要指出的是本文方案中 CS 假设是可信的, 包括属性联盟链中的 AA 也是可信的。有些场景中这两种角色属于不可信或者半可信, 可以采用零知识证明以及在可信执行环境中来增强安全。

2) 审计跟踪。数据联盟链存储数据后会生成所有操作、访问和密钥管理的详细日志信息。这些日志包括数据使用者访问的时间戳、访问者的身份信息、操作内容以及数据的存储地址等。通过这些信息, 数据联盟链为所有数据的使用提供了完整的审计链条, 其结合智能合约能够确保所有的数据访问和操作都可以追溯到特定的数据使用者和事件。

3) 数据回滚机制设计。属性链和数据链之间

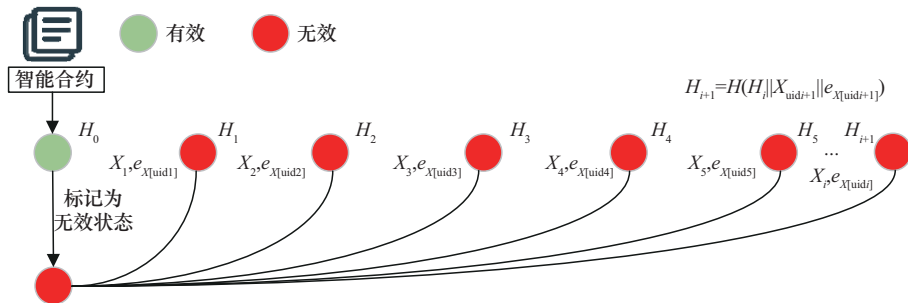


图4 属性批量撤销示意

Figure 4 Illustration of batch revocation of attributes

可发送跨链事件，从而完成双链的信息同步。尤其是当属性链中属性被撤销时，有些场景下其对应数据也需要更新。数据链会检测属性链发出的跨链事件请求。请求内容包括更新新的哈希链内容、数据同步请求等。此机制保证了数据与属性的同步。

此外，本节提出的双联盟链架构设计理念具有显著的跨领域适用性。从系统架构的角度分析，该架构的核心优势在于实现了数据存储与访问控制逻辑的解耦，这一特性使其能够有效支持多种复杂权限管理的分布式应用场景。例如，在医疗健康数据共享场景中，权限链可以精确管理患者、医疗机构和科研单位之间的多级访问权限，同时数据链能够确保电子健康记录的完整性和不可篡改性；在供应链管理溯源领域，通过权限链可以实现供应商、物流服务商和监管机构之间的差异化数据访问策略，而数据链则提供了全流程可验证的商品流转记录。

3 基于双联盟链的工业物联网数据共享通用方案

3.1 方案流程设计

双链架构由属性联盟链与数据联盟链构成。数据拥有者使用对称加密算法加密原始数据明文并上传至云存储，获取对称加密密文在云存储中的存储位置。数据拥有者设定访问策略后，由属性授权机构将符合访问策略的数据使用者属性信息存入属性联盟链便于后续的属性认证，再通过属性加密算法加密对称加密密文在云存储中的位置和对称加密密钥，并将加密后的数据上传至数据联盟链。数据使用者向属性联盟链提交属性信息，经智能合约进行属性认证通过后，从数据联盟链解密得到对称加密密文在云存储中的位置和对称加密密钥，进而从云存储端获取原始密文并解密得到原数据。符号说明见表1，方案流程如图6所示。

1) 初始化阶段：由属性授权机构执行，输入安全参数、生成系统公钥 PK 和系统的主密钥 MSK，如式(1)所示。

$$\text{Setup}(\lambda) \rightarrow (\text{PK}, \text{MSK}) \quad (1)$$

双联盟链初始化，实现合约的部署。

2) 密钥生成阶段：数据拥有者设定访问策略

发送给属性授权机构，数据使用者发送属性集合 A 到属性授权机构。属性授权机构将符合访问策略的数据使用者分发对应的 uid 和 e_{uid} ，并且上传至属性联盟链上，触发智能合约对其进行标记为“已认证”，并生成密钥 USK。

$$\text{KeyGen1}(\tau, A) \rightarrow \text{uid}, e_{\text{uid}} \quad (2)$$

$$\text{KeyGen2}(\text{PK}, \text{MSK}, A) \rightarrow \text{USK} \quad (3)$$

3) 数据上传阶段：数据拥有者输入属性集合设置访问策略，并使用对称密钥 M_{SE} 将原始数据明文 M 加密得到对称加密密文 CT，使用 M_{MAC} 生成 M 的消息鉴别码 MAC，并上传到云存储中。数据拥有者获取云存储返回的 CT 存储地址 addr 。将存储地址 addr 、对称密钥 M_{SE} 以及消息鉴别码密钥 M_{MAC} 进行属性加密后生成属性加密密文 MST，并为此密文生成标识符 dataId 上传到数据联盟链上。

$$\text{SE.Encrypt}(M_{\text{SE}}, M) \rightarrow \text{CT}, \text{addr} \quad (4)$$

$$\text{SE.MAC}(M_{\text{MAC}}, M) \rightarrow \text{MAC} \quad (5)$$

$$\text{ABE.Encrypt}(M_{\text{SE}}, M_{\text{MAC}}, \text{addr}) \rightarrow \text{MST} \quad (6)$$

4) 数据获取阶段：数据使用者提交 uid 和 e_{uid} 到属性联盟链上，智能合约在属性单向哈希链中查找 $H_i = H(H_{i-1} \| X_{\text{uid}} \| e_{X[\text{uid}]})$ 的值获取认证状态。若为“已认证”，则数据使用者通过认证，可以获取数据联盟链上的属性加密密文 MST。数据使用者进行解密后得到对称密钥 M_{SE} 、 M_{MAC} 和原始数据的存储地址 addr 。最后在云存储下载数据，进行解密得到原始的数据 M ，并验证其完整性。

$$\text{ABE.Decrypt}(\text{MST}, \text{USK}, \text{PK}) \rightarrow \text{addr}, M_{\text{SE}}, M_{\text{MAC}} \quad (7)$$

$$\text{SE.Decrypt}(M_{\text{SE}}, \text{CT}) \rightarrow M \quad (8)$$

$$\text{SE.MAC}(M_{\text{MAC}}, M) = \text{MAC} \quad (9)$$

5) 属性撤销阶段：若撤销某个数据使用者的访问权限，首先，由智能合约在属性联盟链上找到对应的属性单向哈希链节点，将节点认证状态标记为“无效”。然后，属性授权机构为该数据使用者生成新的属性公钥 e'_{uid} ，智能合约将 e'_{uid} 进行更新。数据使用者使用之前的 e_{uid} 进行属性认证，则不会通过认证，如式(10)所示。进行机构批量撤销时，智能合约只需要将机构属性单向哈希链中的首节点状态标记为“无效”，即表示该条哈希链上的所有数据使用者无效，实现机构批量属性撤销。

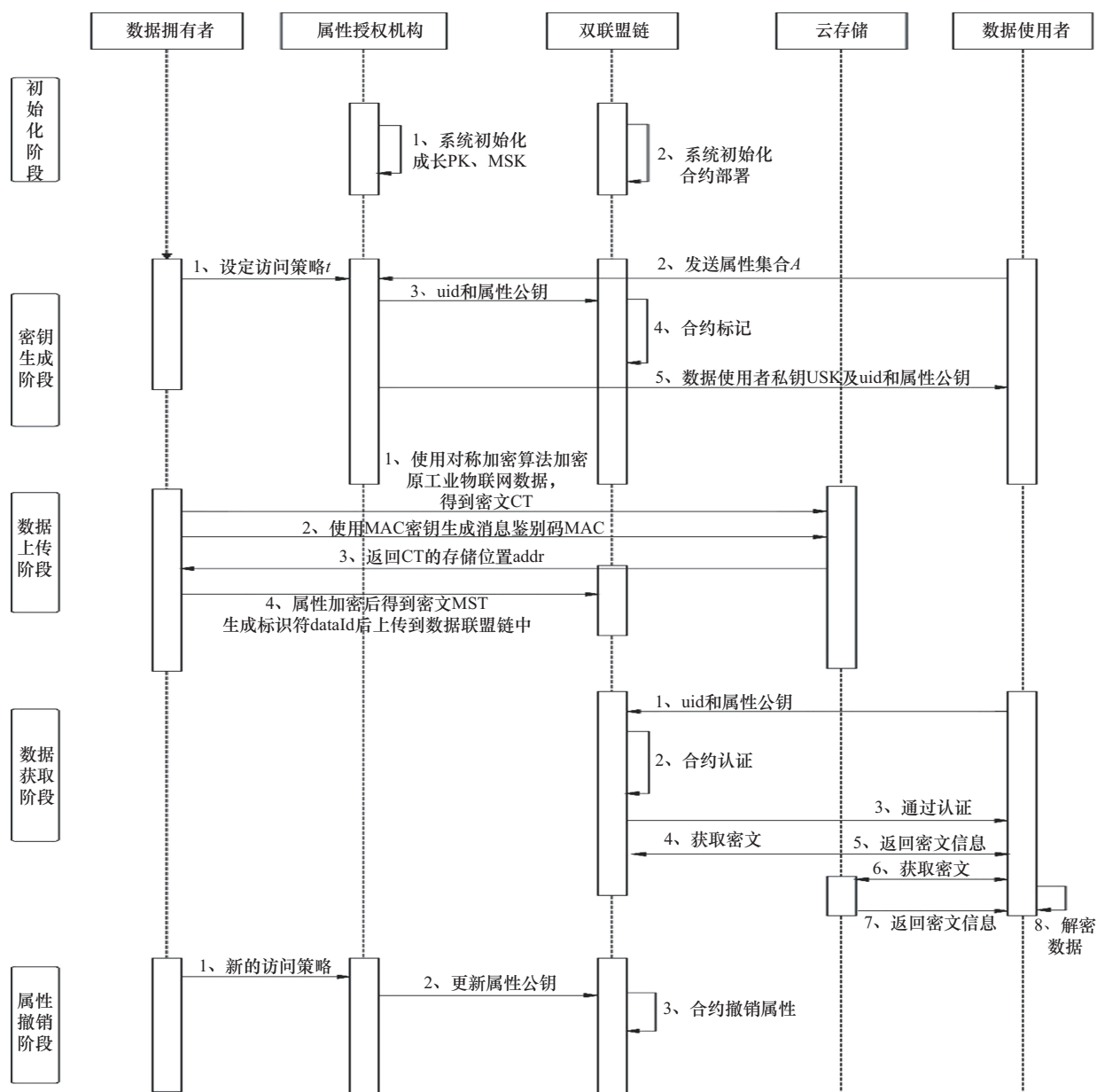


图6 方案流程

Figure 6 Scheme flow chart

表1 符号说明

Table 1 Symbol explanation

符号	含义	符号	含义
e_{uid}	属性公钥	PK	系统公钥
MSK	系统主密钥	addr	对称加密密文存储地址
USK	数据使用者私钥	M_{SE}	对称加密密钥
uid	数据使用者身份标识	M_{MAC}	MAC 密钥
SE	对称加密	M	原始数据明文
ABE	属性加密	CT	对称加密密文
A	属性集合	MST	属性加密密文

$$\text{UPDATE}(uid, e_{uid}) \rightarrow uid, e'_{uid} \quad (10)$$

3.2 安全性分析

下面将对本文提出的基于属性加密的双联盟链数据共享方案在数据共享和存储安全性、前向和后向安全性、防止女巫攻击 (sybil attack) 方面进行分析。

1) 数据共享和存储安全性。本文提出的方案在整个数据共享过程中, 所有信息都采用加密传送方式, 即使中途数据被第三方拦截, 也无法直

接获取数据的明文信息。在存储上, 本文采用链上链下存储机制。链下将原始明文数据对称加密后存储在云存储上, 链上将数据在云上的存储位置和对称加密密钥使用属性加密存储在数据联盟链上。即使云存储服务器上的数据被第三方获取, 也并不能获取对称解密密钥, 无法解密得到数据的具体内容。此外, 数据联盟链上也只存储属性加密后的存储地址和对称密钥, 第三方无法从数据联盟链上获取数据使用者的个人信息。综上所述, 本文方案能确保数据共享和存储过程中的安全性。

2) 前向和后向安全性。当新的用户加入并获得当前属性公钥、通过认证阶段进行属性解密时, 由于历史密文是之前对应访问策略的属性加密密钥进行加密的, 若新用户不满足原访问策略, 便无法解密旧密文获取数据存储地址, 从而确保前向安全性。当某一数据使用者的特定属性被撤销时, 属性授权中心会为该属性重新计算, 分发新的属性公钥 e'_{uid} 并上传到链上, 属性联盟链收到新的属性公钥后会重新计算 $H(H_{i-1} || X_{uid} || e'_{X[uid]})$ 的值, 并将属性哈希链上对应节点标记为“已撤销”。对于已经被撤销特定属性的数据使用者, 在下次属性认证时, 智能合约将使用最新的 $H(H_{i-1} || X_{uid} || e'_{X[uid]})$ 值来验证。如果该数据使用者的认证信息与服务器上存储的最新验证值不符, 则认证失败。且当有数据使用者获得新的属性公钥 e'_{uid} 并进行身份认证时, 属性联盟链中的智能合约用更新后的来认证信息。因此, 数据使用者能够顺利地通过身份认证, 并参与到部分解密过程中成功解密密文, 确保了后向安全性。综上, 本文方案确保了在撤销或添加数据使用者及其属性时能够同时维持前向安全性和后向安全性。

3) 防止女巫攻击。女巫攻击是指攻击者通过创建大量伪身份来破坏网络服务的信誉系统, 从而获得远超常规的影响或操纵网络资源。在本文方案中, 由于引入了属性联盟链结合智能合约的身份认证机制。每当数据需求者发送数据请求时, 必须先经过属性联盟链进行身份验证。这意味着每个请求都需要通过一个严格的认证过程, 确保只有合法数据使用者才能发起交易或请求。因此, 本文方案能抵抗女巫攻击。

3.3 效率分析与对比

文献[13]是属性加密和单区块链进行数据共享的一个典型应用, 通过区块链实现策略更新记录与操作审计, 支持动态属性撤销和访问追溯功能。但其依赖单一联盟链对数据存储和属性进行管理, 随着联盟链长度的增加, 存在存储冗余和检索效率下降的问题。本文提出的双联盟链架构通过属性联盟链和数据联盟链分别对属性和数据进行管理, 有效地对属性和数据进行了隔离, 解决了单链长度增加带来的检索效率下降问题。此外, 在属性联盟链层面, 提出多条属性单向哈希链管理数据使用者的属性信息, 通过动态修改属性哈希链的首节点状态位, 实现权限变更的高效响应, 提升批量撤销操作的执行效率。在数据联盟链层面, 采用轻量级数据存储策略, 即链上仅存加密后的云存储地址与对称加密密钥, 链下将原始数据以对称加密后的密文存储于云服务器中, 缓解了链上的存储压力。同时通过加密传输与存储机制, 确保了数据的隐私安全与可追溯性。在撤销效率方面对比了文献[13]的属性撤销方式和批量撤销的时间复杂度。文献[13]采用区块链加更新代理密钥列表的方式进行属性撤销。在属性撤销时会由数据拥有者向区块链发送撤销指令, 区块链更新代理密钥列表, 将对应用户 uid 的代理密钥标记无效。设标记时间为 T_m 在批量撤销时需要为 N_u 个用户进行撤销的时间为 $N_u \cdot T_m$, 撤销时间随 N_u 个数的增加呈线性增长。而本文使用属性单向哈希链结合智能合约实现批量撤销操作, 通过标记属性单向哈希链的首节点状态实现对 N_u 个用户批量撤销, 因此只需单次标记时间 T_m 即可。

将本文提出的双联盟链架构与文献[13]中提出的基于属性加密的单链数据共享方案进行了功能对比。实验环境为 Ubuntu 22.04.1 操作系统, 硬件配置为 12th Gen Intel(R) Core i9-12900HX 处理器 (主频 2.3 GHz) 和 16.00 GB 系统运行内存。在此设备上, 配置内存为 2 GB, 处理器为 4 核, 在硬盘容量 20 GB 的虚拟机上完成了 FISCO BCOS 联盟链搭建, 采用 PBFT (practical byzantine fault tolerance) 算法, 在此基础上进行了联盟链的相关实验测试。由于链下的加解密时间由具体使用

的加解密算法决定，而文献[13]中单链架构和本文双链架构采用相同的加解密算法，时间相近，因此实验主要对数据共享过程中链上性能进行测试。测试内容包括在单链和双链架构下，对单笔交易在串行合约和并行合约测试下的时间消耗分布区间和不同交易量下平均耗时进行测试对比，以验证方案在实际运行中的性能表现。

1) 串行合约测试：串行合约测试旨在评估区块链系统中串行执行的智能合约在性能负载场景下的表现。在数据共享场景中，针对数据拥有者与使用者高频数据操作和低频属性操作的业务特点，对单链和双链架构下的单笔交易耗时分布进行测试分析。实验设定总交易数量为500笔（数据链300笔交易，属性链200笔交易）。串行合约下单链双链单笔交易耗时分布对比如图7所示。

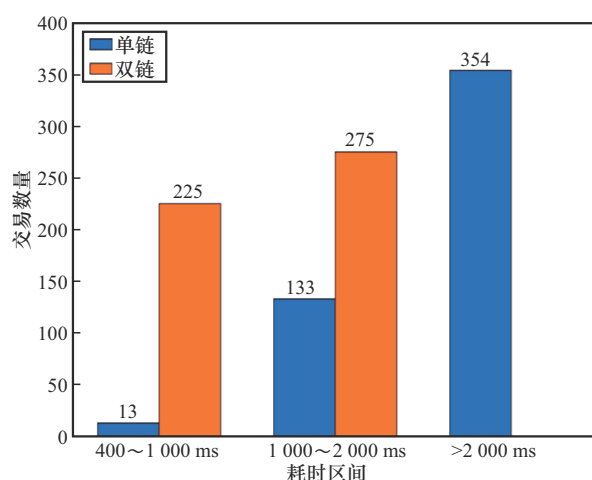


图7 串行合约下单链双链单笔交易耗时分布对比
Figure 7 Comparison of single-chain and dual-chain latency distributions for individual transactions under sequential contract execution

2) 并行合约测试：并行合约测试聚焦于评估区块链系统支持智能合约或交易并行执行的性能表现（即非顺序排队处理模式）。本文方案在并行合约测试场景下，设计了与串行测试一致的实验数量。通过对比单链与双链并行架构下的交易耗时分布，验证双链结构相对于单链的性能提升效果。并行合约下单链双链单笔交易耗时分布对比如图8所示。

3) 不同交易量下的平均耗时：本实验测试对比单链与双链架构分别在1000笔、2000笔

和3000笔交易规模下的平均耗时。在双链中设定数据与属性交易量比例为7:3。结果显示，在不同的交易规模下双链架构平均耗时均低于单链架构，表明双链架构处理交易效率更高。不同交易量下的平均耗时对比如图9所示。

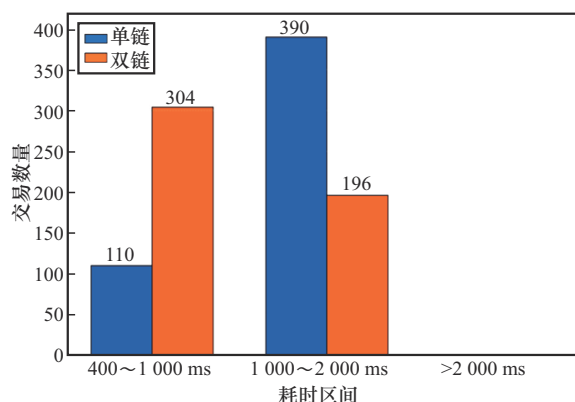


图8 并行合约下单链双链单笔交易耗时分布对比
Figure 8 Comparison of single-chain and dual-chain latency distributions for individual transactions under parallel contract execution

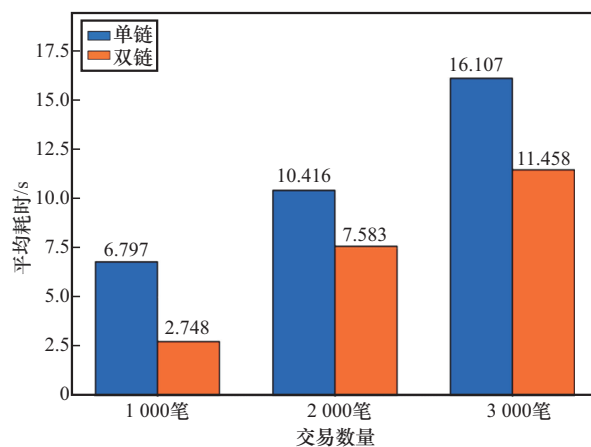


图9 不同交易量下的平均耗时对比
Figure 9 Comparison of average time consumption under different transaction volumes

4 双联盟链方案实现

4.1 方案设计

本文方案基于FISCO BCOS平台搭建并部署了数据联盟链和属性联盟链。共识算法采用PBFT共识算法，并提供了智能合约部署。系统架构自上而下依次为应用层、合约层、业务层、共识层、网络层和数据层。方案架构如图10所示。

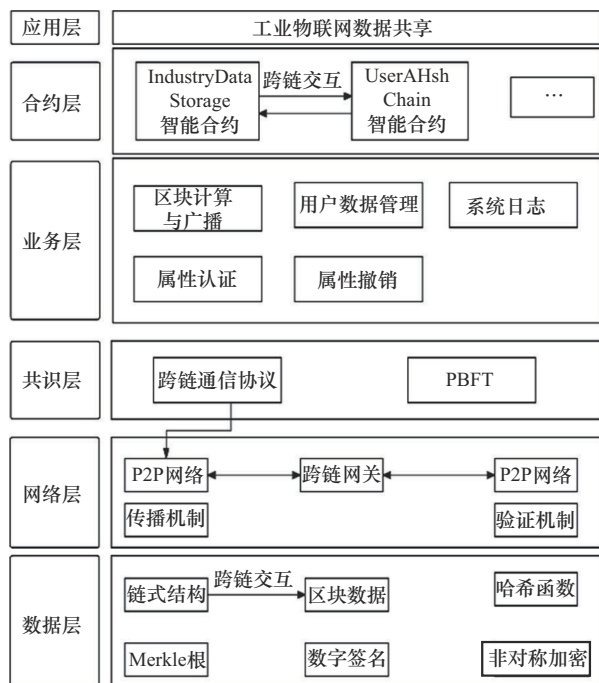


图 10 方案架构

Figure 10 Scheme architecture

4.2 方案实现

(1) 双联盟平台搭建与配置

本文方案基于虚拟机的 Ubuntu 22.04.1 系统，安装 Java JDK 1.8.0_362 版本、openssl 3.0.2 版本和 MySQL 8.0.33 版本。采用 WeCross 跨链平台搭建双联盟链架构。设置 Group1 作为数据联盟链存储属性加密后的 AES 密钥云存储地址密文，Group2 作为属性联盟链存储用户身份标识和属性公钥。双联盟链的共识机制采用 PBFT 共识算法，支持属性动态更新，当用户属性撤销时，属性联盟链将标记原属性无效并生成新认证凭证，确保系统在部分节点故障时仍保持安全一致。

(2) 导入并部署智能合约

WeCross 环境搭建完成并启动成功后，可以输入 Login 登录 WeCross 的控制台查看区块链群组的整体状态，在控制台内将合约部署到 WeCross 文件目录下的 Solidity 中，并生成对应的压缩文件。

在 Group1 数据联盟链中部署名称为 IndustryDataStorage 智能合约用于管理轻量级数据，在 Group2 属性联盟链上部署 UserAHashChain 合约用于管理用户属性。

4.3 智能合约功能与算法

4.3.1 IndustryDataStorage 智能合约

1) storeIndustryData 函数：该函数将数据存储到数据联盟链，并触发 IndustryDataStored 事件记录数据 ID、加密密钥及云存储位置。存储成功后生成链上日志。

2) getIndustryData 函数：该函数接收 dataId，仅授权用户可调用，返回加密数据存储位置和密钥。

3) deleteIndustryData 函数：该函数为附加功能，仅合约管理员可通过 dataId 删除工业物联网数据记录，清空存储地址和加密密钥，释放区块链存储空间，增强隐私保护。

IndustryDataStorage 智能合约存储数据到联盟链算法见算法 1。

算法 1 存储数据到联盟链

输入 数据的唯一标识 dataId，加密数据地址 dataAddr，加密密钥 key

输出 数据存储状态

```

1 FnctionstoreIndustryData(dataId, dataAddr, key):
2   //权限验证，防止未授权操作
3   require(msg.sender == owner)
4   // 检查数据 id 是否已经存在数据记录中
5   if dataId in industryDataRecords then
6     throw error "数据已存在"
7   end if
8   // 生成数据块哈希链
9   prevHash = lastBlockHash // 获取链上最新区块哈希
10  currentHash = hash(dataAddr || key || prevHash) // 计算当前数据哈希
11  // 初始化区块
12  industryDataChain[dataId] = {
13    encryptedDataAddress: dataAddr,
14    encryptedKey: key,
15    prevHash: prevHash,
16    currentHash: currentHash
17  }
18  lastBlockHash = currentHash // 更新链尾
19  emit industryDataStored(dataId, currentHash) // 记录链式存储
20 end

```

4.3.2 UserAHashChain 智能合约

1) **authenticateUser** 函数：函数认证数据使用者唯一标识符与属性公钥，存入属性联盟链的属性哈希链完成身份认证，触发 **UserAuthenticated** 事件并记录相关信息。

2) **addNode** 函数：函数验证数据使用者信息，匹配后将认证节点添加至属性哈希链尾存储，触发 **UserUpdated** 事件记录加入操作。

3) **revokeUser** 函数：合约拥有者调用此函数撤销数据使用者的有效性，需提供其标识符。函数验证使用者是否有效（**isValid** 设为 **true**），若无效则将其标记为无效（**isValid** 设为 **false**），并触发 **UserRevoked** 事件记录撤销状态。

4) **revokeChain** 函数：通过标记机构链首节点状态实现批量撤销，合约查找机构哈希值，将其属性哈希链全局状态标记为无效，使链下用户节点批量失效（无须遍历），撤销后触发 **Chain-Revoked** 事件以确保权限回收实时可审计。

5) **getNodeData** 函数：此 **view** 类型函数作为附加功能，输入数据使用者地址后，通过访问 **nodes** 映射存储数据，返回其标识符、属性公钥及有效性状态 **isValid**，确保信息透明以支持状态验证与管理。

UserAHashChain 合约的撤销机构链见算法2。

算法2 撤销机构链

输入 链首节点 X_1

输出 撤销状态

```
1 FuctionrevokeChain( $X_1$ )
```

```
2 // 权限验证：仅属性管理机构可操作
```

```
3 if msg.sender != AA then
```

```
4     throw error "权限不足"
```

```
5 end if
```

```
6 // 机构链存在性检查
```

```
7 if orgHashChains[ $X_1$ ].head == null then
```

```
8     throw error "机构链不存在"
```

```
9 end if
```

```
10 end
```

4.4 操作流程

具体的操作流程如图 11 所示。

(1) 数据联盟链

1) 调用 **storeMedicalData** 函数，传入唯一标识符 **dataId**、加密数据地址 **encryptedDataAddress** 和加密密钥 **encryptedKey**。合约验证 **dataId** 唯一性后，将数据存入 **industryDataRecords** 映射，并触发 **IndustryDataStored** 事件。

2) 授权用户通过 **getIndustryData** 函数获取加密数据地址和密钥。合约验证调用者权限，确保数据隐私。

3) 管理员通过 **deleteIndustryData** 函数删除指定 **dataId** 的记录，操作不可逆。

(2) 属性联盟链

1) 调用 **authenticateUser** 函数，验证数据使用者唯一标识符 **uid** 和属性认证公钥 **PK**，存入属性哈希链并触发 **UserAuthenticated** 事件。

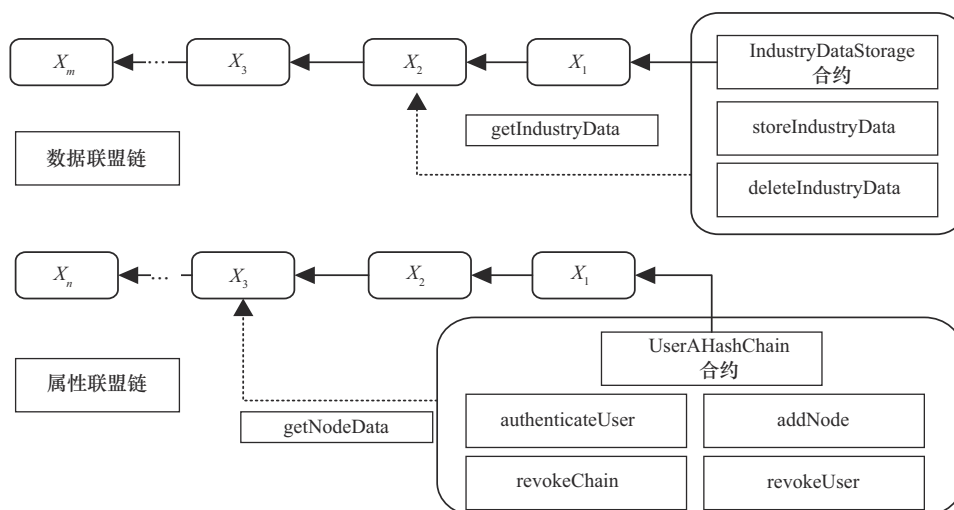


图 11 操作流程

Figure 11 Operation flowchart

2) 管理员调用 `addNode` 函数, 验证 `uid` 和 `PK` 后将新节点添加到属性哈希链末尾, 初始状态为有效 (`isValid=true`), 触发 `UserUpdated` 事件。

3) 调用 `revokeUser` 函数, 根据 `uid` 和 `PK` 将指定节点的 `isValid` 标志设为 `false`, 触发 `UserRevoked` 事件。

4) 调用 `revokeChain` 函数, 将机构链首节点的全局状态标记为无效 (`isActive=false`), 使所有关联节点失效, 触发 `ChainRevoked` 事件。

5) 管理员通过 `getNodeData` 函数查看特定用户节点的 `uid`、`PK` 和有效性标志, 只读操作确保数据安全。

此外, 本文的双联盟链架构已部署在 GitHub 平台上。

5 结束语

本文围绕工业互联网环境下基于属性加密数据共享时及属性撤销时的效率问题, 提出了一种基于双联盟链的工业物联网安全数据共享架构, 有效解决了单链属性撤销需遍历全链的效率问题。在该架构下构造了基于属性加密的数据共享通用方案。实验表明该方案在链上数据交易效率优于单链。同时, 通过 FISCO BCOS 平台实现了双联盟链的核心功能, 为工业物联网数据共享提供了一种新的架构选择。

参考文献:

- [1] SISINNI E, SAIFULLAH A, HAN S, et al. Industrial Internet of things: challenges, opportunities, and directions[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(11): 4724-4734.
- [2] SINGH A, CHATTERJEE K. Cloud security issues and challenges: a survey[J]. *Journal of Network and Computer Applications*, 2017, 79: 88-115.
- [3] 屠袁飞, 苏清健, 杨庚. 一种适用于工业控制系统的加密传输方案[J]. *电子与信息学报*, 2020, 42(2): 348-354.
TU Y F, SU Q J, YANG G. An encryption transmission scheme applicable to industrial control systems[J]. *Journal of Electronics and Information Technology*, 2020, 42(2): 348-354.
- [4] 牛淑芬, 杨平平, 谢亚亚, 等. 区块链上基于云辅助的密文策略属性基数据共享加密方案[J]. *电子与信息学报*, 2021, 43(7): 1864-1871.
NIU S F, YANG P P, XIE Y Y, et al. A cloud-assisted ciphertext-based attribute-based data sharing encryption scheme on blockchain[J]. *Journal of Electronics and Information Technology*, 2021, 43(7): 1864-1871.
- [5] SINGAMANENI K K, YADAV K, ALEDAILY A N, et al. Decoding the future: exploring and comparing ABE standards for cloud, IoT, blockchain security applications[J]. *Multimedia Tools and Applications*, 2025, 84(13): 12299-12327.
- [6] 刘敖迪, 杜学绘, 王娜, 等. 区块链系统安全防护技术研究进展[J]. *计算机学报*, 2024, 47(3): 608-646.
LIU A D, DU X H, WANG N, et al. Research progress on blockchain system security technology[J]. *Chinese Journal of Computers*, 2024, 47(3): 608-646.
- [7] 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.
- [8] 乔康, 游伟, 王领伟, 等. 基于区块链的 5G 物联网数据共享方案[J]. *网络与信息安全学报*, 2020, 6(4): 45-55.
QIAO K, YOU W, WANG L W, et al. Data sharing scheme for 5G IoT based on blockchain[J]. *Chinese Journal of Network and Information Security*, 2020, 6(4): 45-55.
- [9] 金琳, 田有亮. 基于区块链的多 19 权限属性隐藏电子病历共享方案[J]. *网络与信息安全学报*, 2022, 8(4): 66-76.
JIN L, TIAN Y L. Multi-authority attribute hidden for electronic medical record sharing scheme based on blockchain[J]. *Chinese Journal of Network and Information Security*, 2022, 8(4): 66-76.
- [10] 刘尚, 郭银章. 云计算多授权中心 CP-ABE 代理重加密方案[J]. *网络与信息安全学报*, 2022, 8(3): 176-188.
LIU S, GUO Y Z. Multi-authority based CP-ABE proxy re-encryption scheme for cloud computing[J]. *Chinese Journal of Network and Information Security*, 2022, 8(3): 176-188.
- [11] HOHENBERGER S, WATERS B. Attribute-based encryption with fast decryption[M]//*Public-Key Cryptography-PKC 2013*. Heidelberg: Springer, 2013: 162-179.
- [12] ZHANG Z T, ZENG P, PAN B F, et al. Large-universe attribute-based encryption with public traceability for cloud storage[J]. *IEEE Internet of Things Journal*, 2020, 7(10): 10314-10323.
- [13] 郑丽娟, 刘佳琪, 陶亚男, 等. 基于区块链的医疗信息属性加密访问控制方案[J]. *信息安全学报*, 2023, 8(1): 93-107.
ZHENG L J, LIU J Q, TAO Y N, et al. Medical information attribute encryption access control scheme based on blockchain[J]. *Journal of Cyber Security*, 2023, 8(1): 93-107.
- [14] 左娇, 张龙, 张可佳. 基于区块链和 CP-ABE 的跨域认证方案[J]. *计算机工程与设计*, 2025, 46(4): 1056-1063.
ZUO J, ZHANG L, ZHANG K J. Cross-domain authentication scheme based on blockchain and CP-ABE (ciphertext policy attribute based encryption) [J]. *Computer Engineering and Design*, 2025, 46(4): 1056-1063.
- [15] TIAN H L, LI M R. A lightweight IoT data security sharing scheme based on attribute-based encryption and blockchain[J]. *Computers, Materials & Continua*, 2025, 83(3): 5539-5559.
- [16] 刘炜, 李阳, 田钊, 等. IDDS: 一种双链结构传染病数据共享区块链模型[J]. *计算机应用研究*, 2021, 38(3): 675-679.
LIU W, LI Y, TIAN Z, et al. IDDS: double-chain structure infectious disease data sharing blockchain model[J]. *Application Re-*

search of Computers, 2021, 38(3): 675-679.

- [17] LAMANNA M, PERAZZO P, DINI G. SEA-BREW: a scalable attribute-based encryption revocable scheme for low-bitrate IoT wireless networks[J]. Journal of Information Security and Applications, 2021, 58: 102692.

- [18] MOSTEIRO-SANCHEZ A, BARCELO M, ASTORGA J, et al. Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0[J]. Journal of Manufacturing Systems, 2020, 57: 367-378.

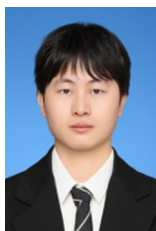
- [19] 郭瑞, 魏鑫, 陈丽. 工业物联网环境下可外包的策略隐藏属性基加密方案[J]. 信息网络安全, 2023, 23(3): 1-12.

GUO R, WEI X, CHEN L. An outsourceable and policy-hidden attribute-based encryption scheme in the IIoT system[J]. Netinfo Security, 2023, 23(3): 1-12.

[作者简介]



李晓伟 (1985-), 男, 吉林通化人, 大理大学副教授, 主要研究方向为密码协议、云计算安全以及区块链技术。



张维江 (2001-), 男, 云南镇雄人, 大理大学硕士生, 主要研究方向为区块链技术、数据共享。



段文钰 (1998-), 男, 河北秦皇岛人, 大理大学硕士生, 主要研究方向为区块链技术、数据共享。



何远 (1977-), 男, 云南大理人, 大理大学讲师, 主要研究方向为信息安全、人工智能等。



杨邓奇 (1979-), 男, 云南大理人, 大理大学教授, 主要研究方向信息安全、人工智能。



杨毅宇 (1987-), 男, 云南大理人, 大理大学讲师, 主要研究方向为物联网安全、移动安全、密码学应用。