文章编号:2096-1472(2026)10-0073-06
DOI:10.19644/j.cnki.issn2096-1472.2026.010.012

基于区块链的医疗物联网群组化属性基加密控制方案

张艳清，孙连山

(陕西科技大学电子信息与人工智能学院，陕西 西安 710021)
✉ 231611012@sust.edu.cn; sunlianshan@sust.edu.cn

摘 要:针对医疗物联网(IoMT)中健康数据授权复杂、权限调整困难等问题,提出一种融合属性基加密与群组化管理的访问控制机制。基于属性基加密构建细粒度访问策略,并群组化处理具有相近访问需求的用户,实现权限集中配置。同时引入区块链记录授权更新与访问行为,实现审计追踪不可篡改。安全性分析与实验结果表明,在群组化授权和周期性权限调整场景下,群组化属性基加密机制在保证细粒度控制与可审计性的同时显著降低管理开销,在本地单线程 Java 实现前提下,重加密令牌生成在 30 人规模下仅约为 0.025 ms,标准差为 0.004 ms,密文更新稳定在 7.5 ms 内,标准差为 1.4 ms,且几乎不受属性和成员数影响,具备良好的可扩展性与实用性。

关键词:区块链;医疗物联网;加密控制;群组管理;属性基加密
中图分类号:TP311 **文献标志码**:A

A Blockchain-Based Control Scheme with Group-based Attribute-Based Encryption for Internet of Medical Things

ZHANG Yanqing, SUN Lianshan

(*School of Electronic Information and Artificial Intelligence, Shaanxi University of Science and Technology, Xi'an* 710021, *China*)
✉ 231611012@sust.edu.cn; sunlianshan@sust.edu.cn

Abstract: In response to the challenges of complex health data authorization and difficult permission adjustment in the Internet of Medical Things (IoMT), this paper proposes an access control mechanism integrating attribute-based encryption with group-based management. The mechanism constructs fine-grained access policies based on attribute-based encryption and groups users with similar access requirements to realize centralized permission configuration. Meanwhile, blockchain is introduced to record authorization updates and access behaviors, enabling immutable audit tracking. Security analysis and experimental results show that, under scenarios of group-based authorization and periodic permission adjustment, the proposed group-based attribute-based encryption mechanism not only guarantees fine-grained control and auditability but also significantly reduces management overhead. Under a local single-threaded Java implementation, the re-encryption token generation takes approximately 0.025 ms for a 30-member group with a standard deviation of 0.004 ms. Ciphertext update remains stable within 7.5 ms with a standard deviation of 1.4 ms. Moreover, the mechanism is nearly unaffected by the number of attributes and group members, demonstrating favorable scalability and practicality.

Key words: blockchain; Internet of Medical Things (IoMT); encrypted access control; group management; attribute-based encryption

0 引言(Introduction)

随着医疗物联网(Internet of Medical Things,IoMT)设备的普及,患者健康数据大量上云,为远程诊疗与智能分析提供便利,但因其高度敏感性,在跨机构共享中既面临泄露、滥用与篡改风险[1],还存在患者自主授权管理复杂及数据中心失信的挑战。传统密文策略属性基加密(Ciphertext-Policy Attribute-Based Encryption,CP-ABE)虽可实现按属性访问控制[2],但加解密过程开销较高,在多机构协同中权限撤销困难[3],易造成计算瓶颈。区块链技术凭借去中心化、不可篡改和可追溯的特性,被用于记录访问行为并辅助审计[4]。为此,本研究提出一

收稿日期:2025-12-09
基金项目:国家自然科学基金项目资助(62471280)

www.rjgcz.com

种以患者为中心的群组化属性基加密控制方案，采用 CP-ABE 进行细粒度访问控制，其访问策略支持“与(AND)”“或(OR)”逻辑运算，可满足医疗场景下多角色、多科室的协同访问需求。结合群组化策略整合具有相近访问需求的用户，并引入区块链记录权限变更与访问行为，实现批量管理、权限及时更新与细粒度控制的统一。安全性分析与实验结果表明，本文方案在访问效率、安全审计与权限更新方面具有良好表现，可为医疗数据管理提供可行思路。

1 相关工作(Related works)

在医疗物联网场景中，区块链技术的分布式存储与不可篡改特性为跨机构数据共享提供了重要支撑[5]。现有研究多为结合区块链与加密技术构建可信数据交换与访问管理机制。Lee 等[6]提出多委托模型，强化个人健康信息共享的安全保障；邓昀等[7]设计轻量化区块链密钥认证方案，通过链上密钥登记校验与智能合约自动化管理，实现安全与效率的平衡；段嘉俊等[8]融合区块链与零知识证明、同态加密等技术，构建可信数据共享体系并保障密文计算安全。

CP-ABE 被广泛用于细粒度访问控制[9]。Li 等[10]在 CP-ABE 基础上引入加权协同访问与用户撤销机制，提升跨主体数据共享的灵活性；Zou 等[11]将属性变更信息上链，实现访问策略更新可追溯，增强控制过程可信度。此外，动态群组管理逐渐成为多成员协作场景的优化方向，张邓凡[12]针对云端多用户共享医疗数据的安全需求，提出动态群组完整性验证框架，为多方协作安全提供支撑。

近年来，区块链与属性基加密在医疗领域的研究持续深入，在抗胁迫安全、策略级访问控制以及数据完整性保障等方面取得了积极进展[13-14]。但多数方案侧重单次访问控制安全性或个体权限管理效率，对多成员协作环境中频繁授权变更的管理复杂度与系统开销关注相对有限，且缺乏针对相似访问需求用户的批量管理机制[15-16]。本文则以患者为中心，聚焦医疗团队协作中的动态群组授权与权限撤销问题，通过引入群组化管理与双层加密结构，在保留细粒度访问控制优势的同时，有效降低权限动态更新带来的计算与管理开销。

2 系统模型(System model)

本研究面向医疗物联网中授权频繁变动与多参与方协作带来的管理压力，构建了一种融合区块链审计机制与群组化 CP-ABE 的数据共享体系。系统采用双层加密结构：首先依据数据使用者属性生成对应的属性私钥，并由此完成密文的策略级加密；随后针对同一群组的用户，再利用群组密钥执行二次加密，以实现批量、高效的共享控制。该设计在权限更新时，仅需对群组密钥加密层进行重加密即可，无需执行传统 CP-ABE 的复杂撤销流程，从而兼具细粒度授权与高效可管理性。在多机构协作环境下，区块链承担记录群组调整、授权变更及访问相关事件的职责，形成可追溯、不可抵赖的审计链。星际文件系统(InterPlanetary File System，IPFS)存储密文实体，为链上元数据提供去中心化监管，整体构建出面向患者的可信共享框架。

2.1 系统参与模型

系统模型主要由数据拥有者(Data Owner，DO)、数据使用者(Data User，DU)、区块链(Blockchain)、星际文件系统(IPFS)、云服务器(Cloud Server，CS)等组成，系统框架如图 1 所示。

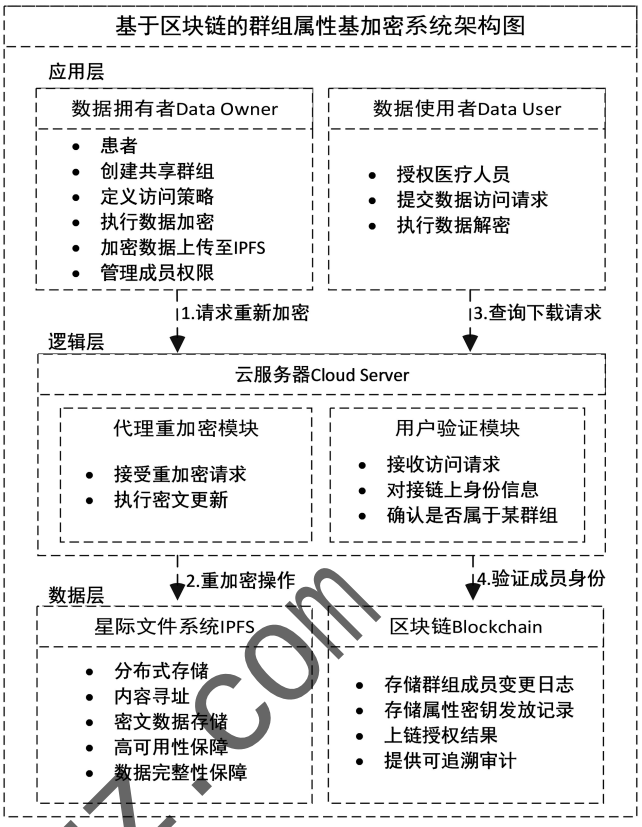


图 1 基于区块链的 IoMT 群组化属性基加密系统架构

Fig. 1 Architecture of blockchain-based group-based ABE system in IoMT

数据所有者(DO)，即患者本身，是系统数据主权的核心控制者，负责制定访问策略与完成医疗数据的加密封装。主要功能包括创建管理群组、定义属性访问策略、对原始医疗数据执行双层加密，并将密文上传至 IPFS，建立元数据索引表并将它上传至区块链，实现不可篡改存证。患者可根据自身需求，灵活指定可信的医疗实体(如患者家属、主治医生等)组成数据访问群组，而群主由患者及指定的可信群组成员(如患者家属等)担任，负责群组密钥与后续令牌操作与管理。

数据使用者(DU)，即授权医疗人员，是经过授权的数据访问方，其主要作用是安全获取所需医疗数据，使用群组密钥和个人属性私钥完成数据解密。

区块链(Blockchain)作为系统的信任基础设施，其核心作用是提供不可篡改的分布式账本服务。包括维护参与实体的链上身份状态，记录数据哈希索引、策略摘要及关键授权操作，确保系统流程具备可审计性、可追溯性与不可抵赖性。

星际文件系统(IPFS)作为分布式存储层，它的主要功能是安全存储医疗数据密文。该系统通过内容寻址确保数据完整性，并与链上元数据记录相互验证。

云服务器(CS)作为密码学服务提供方，是半可信服务器，核心功能是实现密文更新。群组成员权限变更时，CS 可在不接触明文数据的前提下利用代理重加密技术对涉及密文进行安全更新，确保被撤销权限用户无法访问历史数据。

2.2 方案具体流程

本系统构建了一个以患者为中心的、支持动态细粒度访问控制的医疗数据安全共享框架。具体流程如图 2 所示。

www.rjgczz.com

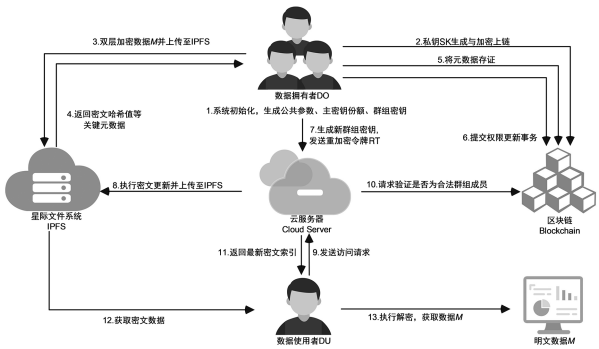


图 2　基于区块链的 IoMT 群组化属性基加密系统流程

Fig. 2 Workflow of blockchain-based group-based ABE system in IoMT

(1)系统初始化。系统初始化由群组初始成员协同完成。初始成员通过安全多方计算协议共同生成公共参数 PP、主密钥的分布式份额 MSK_i、群组密钥 GK。公共参数将公开存储于智能合约中,而主密钥份额则由各成员分别秘密保存,确保密钥生成过程的去中心化与安全性。

(2)属性私钥生成与分发。由群主联合持份者使用分布式份额 MSK_i 为成员生成与属性集合 AttrSet 对应的 CP-ABE 私钥,并将其以密文形式上链保存。

(3)数据加密。数据拥有者 DO 根据对数据的细粒度访问控制需求,定义具体的属性访问策略 Policy。随后,使用系统公共参数及该策略,对原始医疗数据 M 执行属性基加密,生成第一层密文 C_1。此密文保证了数据只能被持有满足策略属性私钥的用户访问。为便于群组级别的管理与未来的动态更新,群主使用群组密钥 GK,对第一层密文 C_1 执行第二次加密,生成最终的第二层密文 C_2。该密文被上传至 IPFS 进行存储。同时,数据拥有者将密文的哈希值、访问策略摘要、时间戳等关键元数据提交至区块链智能合约存证,建立不可篡改的访问记录与数据索引。

(4)数据解密。数据使用者使用当前有效的群组密钥 GK 进行解密,得到第一层密文 C_1。此步骤完成了密文由群组共享层向个人属性访问层的转换。获得密文 C_1 后,数据使用者使用其私钥尝试解密。解密算法将自动验证其属性是否满足加密时嵌入的访问策略。当且仅当属性匹配时,才能成功解密并恢复出原始医疗数据明文 M,实现细粒度的访问控制。

(5)权限撤销。当有成员被撤销访问权限时,为使该成员无法解密历史数据,系统需重新加密相关数据。群主生成新的群组密钥 GK_{new} 和重新加密令牌 RT,由云服务器执行重新加密算法,将涉及的密文 C_2 更新对应于新群组密钥的密文 C_{2new},而被撤销成员持有的旧密钥将随之失效。

2.3　算法设计

相关的符号定义详见表 1,之后即对本方案进行算法介绍。

表1　符号说明

Tab. 1 Symbol descriptions

符号	说明
PP	CP-ABE 公共参数
MSK_i	MSK 门限份额集合
GK	群组密钥
RT	重新加密令牌
AttrSet	成员属性集
Policy	访问策略
$SK_{\{DID,Ver\}}$	属性私钥
M	原始医疗数据
C_1	第一层密文(CP-ABE 加密)
C_2	第二层密文(群组密钥加密)

本文方案包含以下核心算法:

(1)系统初始化算法 $Setup(\lambda, G)\rightarrow(PP, MSK_i, GK)$:群组初始成员通过 MPC 协议协作生成系统公共参数 PP、MSK_i、群组密钥 GK,并部署智能合约 SC。成员生成并保存自己的去中心化标识符(Decentralized IDentifier,DID)和版本相关信息。

(2)属性私钥生成算法 $AttrKeyGen(PP, MSK_i, DID, AttrSet, Ver)\rightarrow SK_{\{DID,Ver\}}$:由群主联合持份者使用公共参数和 MSK_i 为成员生成与属性集合 AttrSet 对应的 CP-ABE 私钥 $SK_{\{DID,Ver\}}$,并将其密文形式上链保存。

(3)数据加密算法。数据拥有者 DO 根据访问策略 Policy,采用算法 $CP\text{-}ABE_{Encrypt}(M, Policy, PP)\rightarrow C_1$ 将数据 M 进行 CP-ABE 加密生成 C_1。并使用群组密钥 GK,通过算法 $GK_{Encrypt}(C_1, GK)\rightarrow C_2$ 将第一层密文 C_1 加密为 C_2。将密文 C_2 上传至 IPFS,同时将关联元数据等记录到智能合约中。

(4)数据解密算法。首先数据使用者 DU 采用预解密算法 $GK_{Decrypt}(C_2, GK)\rightarrow C_1$,利用群组密钥 GK 解密密文 C_2,获得 C_1。之后需采用 CP-ABE 解密算法 $CP\text{-}ABE_{Decrypt}(SK_{\{DID,Ver\}}, C_1)\rightarrow\{M/\perp\}$,使用其属性私钥 $SK_{\{DID,Ver\}}$ 解密 C_1,判断其属性与访问策略是否匹配。

(5)权限撤销算法。当某成员权限被撤销后,群组立即更新群组密钥为 GK_{new},并计算重新加密令牌 $GenToken(GK_{old}, GK_{new})\rightarrow RT$,且云服务器无法从中恢复任意密钥值。云服务器采用算法 $PRE(C_{2old}, RT)\rightarrow C_{2new}$ 对划分的新群组对应的、仍处于有效访问周期且后续可能被访问的密文数据执行密文更新操作,使被撤销者即便持有 GK_{old} 与 $SK_{\{DID,Ver\}}$ 也无法解密更新后的密文。

3　安全性分析与证明(Security analysis and proof)

本章进行群组化属性基加密方案的安全性分析与证明。3.1节给出判定性双线性 Diffe-Hellman(Decisional Bilinear Diffie- Hellman,DBDH)假设定义。3.2 节提出安全模型并定义攻击者能力。3.3 节给出安全性证明并规约到 DBDH 假设。

3.1　DBDH 假设难题

设存在双线性映射 $e: G\times G\rightarrow G_T$,其中 G 和 G_T 为 2 个具有相同素数阶 p 的双线性群,g 是 G 的生成元。随机从整数群 z_p 中选取 a、b、c,并从 G_T 中随机选取元素 R。若对于任何概率多项式时间算法而言,区分以下两组元组在计算上不可行:$(g, g^a, g^b, g^c, e(g,g)^{abc})$和$(g, g^a, g^b, g^c, R)$,即不存在能以显著概率优势区分以上两组元组的算法,则称 DBDH 假设成立。

3.2　安全模型

敌手 A 可自适应查询任意属性集的私钥(不可查询满足挑战策略的私钥)、历史群组密钥、重加密令牌及链上元数据,可重放,不可腐蚀群管理员。

www.rjgcz.com

初始化：敌手 A 选择要挑战的访问策略 Policy*，并发送给挑战者 C。

初始化设置：挑战者 C 运行 Setup 算法，并将 PP 发送给敌手 A。

第一阶段：A 自适应发出私钥查询，但 A 在查询阶段请求的任何私钥对应的属性集都无法满足该策略。

挑战：A 提交等长消息 M_0 和 M_1，C 随机选择 $\beta\in\{0,1\}$，采用策略 Policy* 对 M_β 进行加密并向 A 返回密文 C_1^*。

第二阶段：A 继续阶段一的查询，但仍受相同的限制。

猜测：A 输出 guess $\beta\in\{0,1\}$。$\beta'=\beta$ 则 A 获胜。A 的优势为 $|\Pr[\beta'=\beta]-1/2|$。

定义 1：如果任何多项式时间的敌手赢得上述游戏的优势都是可忽略的，那么本文方案在上述安全模型定义下满足选择明文攻击下的不可区分（INDistinguishability under Chosen-Plaintext Attack，IND-CPA）安全。

3.3 安全性证明

定理 1：如果敌手可以在 IND-CPA 模型下攻破本方案，那么可以构造一个模拟器以不可忽略的优势解决 DBDH 问题。

证明：假设存在敌手 A 在 IND-CPA 模型下可以以优势 ε 攻击本方案，构造了以 $\varepsilon/2$ 优势解决 DBDH 问题的模拟器 B。

给定一个 DBDH 实例 (g,g^x,g^y,g^z,Z)，Z 是 $e(g,g)^{xyz}$ 或 G_T 中的一个随机元素。

初始化：敌手 A 将要挑战的访问策略 Policy* 发送给模拟器 B。

初始设置：B 将 DBDH 实例中的 g、g^x、g^y 嵌入公共参数 PP 并发送给 A。但 B 并不知道 x 和 y 的值。

第一阶段：A 自适应地发出私钥查询，但在查询阶段请求的任何私钥所对应属性集都无法满足该策略。A 发起查询，B 选择随机数并根据算法 AttrKeyGen(PP，MSK_i，DID，AttrSet，Ver)→$SK_{(DID,Ver)}$ 构造模拟私钥。该模拟私钥与真实密钥 $SK_{(DID,Ver)}$ 在分布上不可区分，B 可以正确应答所有私钥查询。

挑战：A 提交等长消息 M_0、M_1，B 选择 $\beta\in\{0,1\}$，根据访问策略 Policy* 构造挑战密文 C_1^* 并将 DBDH 实例中的 g^z 和 Z 嵌入，将密文 C_1^* 发送给 A。

第二阶段：A 继续阶段一的查询，但仍受相同限制。

猜测：A 输出猜测 β'。如果 $\beta'=\beta$，则 A 获胜。若 $Z=e(g,g)^{xyz}$，A 获胜概率为 $1/2+\varepsilon$。若 Z 随机，A 获胜概率为 $1/2$。因此，B 可以根据 A 的输出类判断 Z 的类型，若 A 获胜，则判定 $Z=e(g,g)^{xyz}$，且 B 输出 1，否则输出 0。最终 Z 获胜概率为 $1/2+\varepsilon/2$。

分析：B 解决 DBDH 问题的优势为 $\varepsilon/2$，与 A 的优势线性相关。由于 DBDH 中 ε 必须是可忽略的，因此，敌手无法区分任意明文，方案在数据机密性方面整体满足 IND-CPA 安全。

在权限撤销阶段，系统更新群组密钥为 GK_{new}，并生成重加密令牌 GenToken(GK_{old}，GK_{new})→RT，云服务器通过 PRE(C_{2old}，RT)→C_{2new} 将原密文更新为 C_{2new}。由于重加密令牌仅用于密文转换，且重加密过程不涉及明文恢复，云服务器无法直接获取 GK_{old} 或 GK_{new}，仍无法执行解密操作，不会泄露任何敏感信息。被撤销用户即使持有 GK_{old} 和 $SK_{(DID,Ver)}$，也无法通过 GK_{old} 解密 C_{2new}，满足前向安全性；新加入用户仅被授予 GK_{new}，且由于新旧密钥通过 RT 实现单向转换，无法从 RT 恢复 GK_{old}，因此无法利用 GK_{new} 解密历史密文，满足后向安全。

除此之外，区块链仅存储经过哈希处理的元数据，不包含任何明文字段。基于哈希函数的单向性与抗碰撞性，攻击者无法从链上数据反推出原始访问策略或属性信息。综上所述，结合 CP-ABE 的细粒度访问控制、群组密钥的动态管理机制以及区块链的链上不可篡改[17]与可信审计能力，本方案能够在医疗物联网环境下有效保障数据机密性、不可抵赖性与访问控制安全性，整体具备良好的安全性与隐私保护能力。

4 实验与性能分析（Experiment and performance analysis）

4.1 理论分析

本方案与 Ren 等[16]、Zhai 等[13]和 Wang 等[14]的链上开销对比见表 2。

表 2 计算与链上开销对比

Tab.2 Comparison of computational and on-chain overheads

开销指标	Ren 等[16]	Zhai 等[13]	Wang 等[14]	本文方案
加密开销	$(2k+8)E+P$	$(3l+3)E$	$E+L$	$E_{GT}+(l+2)E_G$
解密开销	$(2k+6)E+4P$	$(2\|I\|+1)P+kE$	$(\|I\|+1)E+2\|I\|P+L$	$E_G+E_{GT}+(l+1)P$
撤销开销	—	$(3\bar{m}+2)E$	—	$L+E_G$
用户平均撤销开销(gas/人)	约 445		—	约 330
链上存储开销/Byte	约 224	约 189	约 233	约 232

其中：k 表示用户属性数；$|I|$ 表示满足策略的属性数；l 表示访问矩阵行数，$|I|\leqslant l$；E 表示群中指数运算；P 表示双线性配对运算；G、G_T 表示 2 个素数阶乘法循环群；L 表示轻量级运算（如乘法、哈希、异或等）；$\bar{m}$ 表示撤销访问策略中的属性数。

本文采用群组化批量加密与轻量级链上验证，加密开销低于 Ren 等[16]和 Zhai 等[13]，解密开销显著低于 Wang 等[14]和 Zhai 等[13]，且相对于 Wang 等[14]无需多权威机构进行协同交互与属性成员证明验证，并规避 Ren 等[16]的阈值密钥碎片管理开销。撤销时采用更新令牌间接撤销，生成重加密令牌并触发云服务器密文更新，开销低于 Zhai 等[13]单策略处理。

对于估算链上成本，Ren 等[16]400 笔交易聚合后单用户分摊 gas 约 445，本方案用户独立撤销开销约为 33 000 gas，30 人群组批量撤销后单用户仅 330 gas，群组化降低约 99%的开销，且相比 Ren 等[16]降低了约 25.8%。同时，单用户链上存储字节数约为 232 Byte，30 人群组化后总存储约为 1160 Byte，群组化降低约 83.3%的链上记录存储开销，相比方案 Zhai 等[13]、Ren 等[16]、Wang 等[14]分别降低约 82.1%、78.8%、82.8%，降低了链上存储负担。

4.2 实验分析

4.2.1 实验环境

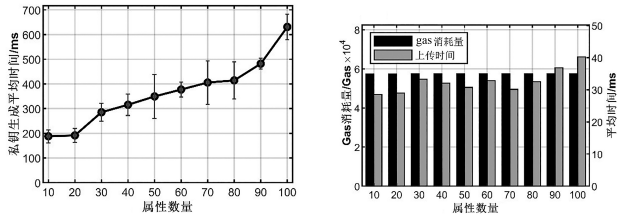
为验证方案可行性，本文在本地搭建了原型系统并开展相关实验。测试平台为 Windows 10 操作系统，硬件配置包含主频 4.00 GHz 的 Intel Core i7-4790K 处理器及 16 GB 内存。密码学运算部分基于 JPBC 库完成实现；区块链模块依托本地部署的 Ganache 环境与 Ethereum 开发框架构建，并通过 MetaMask 模拟账户管理与交易签名过程。

4.2.2 性能实验

性能实验包括模拟属性私钥生成、数据上传、数据下载、权限撤销等阶段。为评估方案在真实医疗协作环境中的适用性，设定群组成员数为 30，以符合一般医疗团队规模。每项操作重复执行 100 次取均值，并将满足访问策略的属性数由 10 增加至 100，步长为 10，以观察属性规模变化对整体计算开销、加

www.rjgcz.com

解密效率及动态更新成本的影响。该属性规模设置与现有基于 CP-ABE 的医疗数据加密控制研究保持一致[13-14],可覆盖典型多科室协同场景下的访问控制需求。实验结果如图 3～图 6 所示,能够有效反映方案在多属性、多成员协同场景下的表现,验证系统在属性数提升时仍能保持稳定性能。



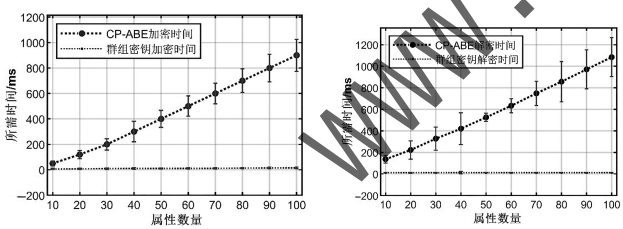
(a)私钥生成　　(b)私钥上链

图 3　私钥生成与上链开销(属性数每 10 取一次样)

Fig. 3 Overheads for key generation and on-chain (attribute count sampled every 10)

图 3(a)表明,30 名成员的平均私钥生成时间随属性数呈线性缓慢上升,整体时间控制在 700 ms 之内,波动幅度较小。上述结果表明,本方案中属性规模提升不会显著增加计算负担,为系统在实际医疗场景下应对多维属性描述提供了良好的性能基础。图 3(b)是基于区块链的密钥发布流程中成员私钥上链操作的 gas 消耗与时间开销,gas 消耗在不同属性数下基本保持稳定。本实验依托本地 Ganache 环境完成,目的是评估智能合约逻辑本身的资源消耗特征,在实际公链或联盟链中,其基础消耗数值与变化趋势具有一致性和可迁移性,但实际费用可能会因 gas price 波动而不同。私钥上传的时间成本也维持在 40 ms 左右,整体变化平稳。在真实区块链环境中,时间开销可能因网络延迟、共识机制和交易确认过程不同而波动,但整体仍呈现随属性数变化幅度较小的趋势。综上,本方案在初始化阶段具备良好的链上部署效率,在保证安全记录的同时有效控制 gas 和时间开销。

为评估数据加、解密效率,对加、解密进行性能模拟,考查 CP-ABE 层与群组密钥层分别的时间开销,实验结果如图 4 所示。



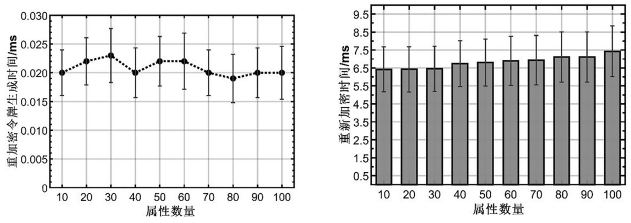
(a)加密　　(b)解密

图 4　加解密时间开销(属性数每 10 取一次样)

Fig. 4 Time overheads for encryption and decryption (attribute count sampled every 10)

如图 4 所示,随着属性数增长至 100,两层加密和解密操作的总体耗时均呈上升趋势。其中,CP-ABE 加密层耗时随属性数近似线性增长,而群组密钥加密层耗时极小且几乎恒定,这是因为群组密钥只需对每个用户组加密一次,无需对每个属性重复操作。CP-ABE 解密层随属性数近似于线性增长,群组密钥解密开销尤其小且几乎是常数,总解密时间稳定控制在 1200 ms 范围内。整体来看,两层操作均保持在可接受范围内,能够在较大属性集与多成员场景下维持高效的访问控制和数据共享性能。

为评估本方案在权限变更场景下的重新加密令牌及密文更新效率,对成员权限撤销流程进行了模拟,实验结果如图 5 所示。



(a)重加密令牌生成　　(b)密文重加密

图 5　权限撤销时间开销(属性数每 10 取一次样)

Fig. 5 Time overheads for permission revocation (attribute count sampled every 10)

如图 5(a)所示,属性规模扩大时,重加密令牌生成百次运行的平均时间保持在 0.025 ms,标准差为 0.004 ms,并在属性数变化时基本保持稳定。原因在于该过程主要涉及向仍具访问权限的成员分发新群组密钥,而与属性规模关系较弱,有效避免了传统 CP-ABE 在属性维度上的额外计算开销。如图 5(b)所示,密文重加密操作百次运行平均时间维持在 7.5 ms 之内,标准差为 1.4 ms,未随属性数出现显著波动,进一步展示出本方案密文转换的高效性。由于采用群组级批量更新机制,无需针对每位用户单独执行属性基加密与密文更新,有效降低了权限撤销带来的计算压力。

如图 6 所示,固定属性数为 100,将群组成员规模从 30 线性扩展至 200,步长设置为 10,验证群组成员增长对重加密令牌生成和密文更新生成无影响。

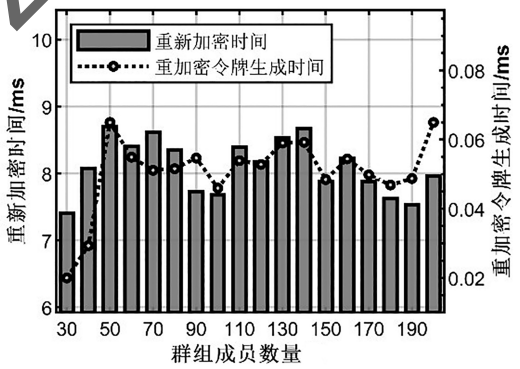


图 6　成员规模扩展的重加密性能(成员数每 10 取一次样)

Fig. 6 Re-encryption performance on group scaling (member count sampled every 10)

综合图 5、图 6 来看,本方案中重加密令牌生成以及重加密时间,与属性数、群组成员数无显著关联,表现出本方案在处理权限变更时具备突出的性能优势,尤其适用于中等规模且协作频繁的医疗应用场景,且在大规模场景下也具备良好的可扩展性。该特性使得系统在确保安全与可控性的同时保持敏捷的密文更新效率,为实际医疗物联网环境中的多方协同提供了有力支持。但本文方案的不足在于可能导致群组增加而提高存储成本,且群组成员增加时分发新群组密钥的成本可能上升。

4.3　链上经济成本

上述实验基于本地 Ganache 环境评估了链上操作的 gas 消耗与执行时间,真实部署成本主要由 gas 消耗和网络实时 gas price 共同决定。根据本文实验结果,单次成员私钥发布的 gas 消耗约为60 000。以 Ethereum 主网实时数据(参考 Etherscan Gas Tracker: https: // etherscan. io/chart/gasprice? utm _

www.rjgcz.com

source=chatgpt.com)为例,取近一个月平均 gas price 0.75 Gwei 计算,单次交易手续费约 0.000 045 ETH(0.13 USD/次)。在 10 000 群组规模下(30 人/组、每季度更新密钥),单群组授权元数据负载约为 1160 Byte ,年度新增链上存储约 46.4 MB。按 5 年生命周期估算,全节点总存储约 0.23 GB。长期场景可通过节点裁剪(Pruning)机制进一步缓解存储压力,平衡可扩展性与审计完整性。

本方案可较为平滑地迁移至低成本区块链环境。在 Layer2 网络中,以 Rollup 为例,单群组迁移数据约为200 Byte,10 000 群组年度总迁移量约为 8 MB,通过交易聚合将单次成本降至主网的 5%~20%,兼顾安全与经济性;在侧链环境中,以 Polygon 为例,在 10 000 群组规模下,单群组迁移数据约为 300 Byte,10 000 群组年度总迁移量约为 12 MB。但是本文不限于公有链进行部署。在基于 Hyperledger Fabric 联盟链的部署模式下,无 gas 计费机制,链上经济成本主要体现为节点运维开销,适配于医疗场景的权限可控需求。

5 结论(Conclusion)

本文提出了一种基于区块链的医疗物联网群组化属性基加密访问控制机制,系统将群组密钥管理与细粒度属性控制结合,通过链上密钥可信发布与访问记录审计,实现了批量授权、可信分发与可追溯共享。方案采用双层加密结构,使群组共享与个体属性控制兼容,从而在保持安全性的同时有效降低传统属性基加密在权限撤销场景中的更新负担。实验结果表明,本方案在典型的权限撤销场景下具有显著效率优势,重新加密令牌生成在成员规模为 30 时保持在 0.025 ms,标准差为 0.004 ms,而密文更新稳定在 7.5 ms 之内,标准差为 1.4 ms,且几乎不随属性和成员数量变化。这表明该机制在中等规模群组、权限更新频繁的实际协作环境中表现尤为突出,且具有良好的可扩展性,特别适用于远程医疗、跨科室数据协作以及病历共享等医疗场景。

总体而言,本文方案在功能完整性、访问审计可信度及权限更新效率方面均表现优良,证明群组化属性基策略是应对动态访问控制需求的有效路径。后续研究可进一步面向更大规模群组与强对抗模型,引入门限或分布式密钥管理机制以弱化单点信任,并结合链上多方触发及智能合约机制实现重加密令牌去中心化生成,提升管理员异常场景下的系统的可用性与安全性。此外,将引入层次化群组管理机制与云上大规模数据批量更新与管理[18-19]技术,持续提升方案的规模化适配能力与大规模场景下的运行效率。

参考文献(References)

[1] 陈嘉莉,马自强,兰亚杰,等. 基于区块链技术的医疗信息共享研究综述[J]. 计算机应用研究,2024,41(9):2573-2584.

[2] Yadav R K. Scalable and secure data access control in cloud environments using ciphertext-policy attribute-based encryption[J]. IAENG International Journal of Computer Science, 2025, 52(9): 3067.

[3] 范悦. 面向智慧医疗的分层属性基加密方案研究[D]. 西安:西安电子科技大学,2024:25-26.

[4] Zhang Q Y, Qian S, Cui J, et al. Blockchain-based privacy-preserving deduplication and integrity auditing in cloud storage[J]. IEEE Transactions on Computers, 2025, 74(5): 1717-1729.

[5] 蔡楚君,柳毅. 基于区块链的医疗数据安全共享方案[J]. 计算机应用与软件,2024,41(12):360-366.

[6] Lee J Y, Oh J, Kwon D K, et al. Blockchain-enabled key aggregate searchable encryption scheme for personal health record sharing with multidelegation[J]. IEEE Internet of Things Journal, 2024, 11(10): 17482-17494.

[7] 邓昀,刘瑾,陈守学. 基于区块链的 MEC 环境身份认证与密钥协商[J]. 计算机工程与设计,2025,46(7):1959-1966.

[8] 段嘉俊,柳毅,陈家辉. 基于区块链的电子医疗数据安全共享方案[J]. 计算机应用与软件,2024,41(10):116-121,226.

[9] 尹晓帆,李晓会,张思琪. 基于区块链和属性基加密的用户分类分级访问控制模型[J]. 计算机工程与科学,2025,47(9):1609-1618.

[10] Li X M, Wang H, Ma S, et al. Revocable and verifiable weighted attribute-based encryption with collaborative access for electronic health record in cloud[J]. Cybersecurity, 2024, 7(1): 18.

[11] Zou Y P, Peng T, Wang G J, et al. Blockchain-assisted multi-keyword fuzzy search encryption for secure data sharing[J]. Journal of Systems Architecture, 2023, 144: 102984.

[12] 张邓凡. 群组共享云数据完整性验证方案研究[D]. 北京:北京印刷学院,2025:36-41.

[13] Zhai Y, Yang H C, Yao J Y, et al. CR^2-ABE: a blockchain-assisted coercion-resistant and revocable attribute-based encryption for IoMT[J]. IEEE Internet of Things Journal, 2025, 12(9): 13075-13096.

[14] Wang H, Xie Y, Luo M, et al. EAPDS: efficient auditable and privacy-preservation data sharing scheme based on attribute-based encryption for IoMT[J]. IEEE Internet of Things Journal, 2025, 12(14): 26844-26854.

[15] Chen L, Xu S, Zhang H, et al. Fair-and-exculpable-attribute-based searchable encryption with revocation and verifiable outsourced decryption using smart contract[J]. IEEE Internet of Things Journal, 2024, 12(4): 4302-4317.

[16] Ren Z X, Yan E H, Chen T W, et al. Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof[J]. Journal of King Saud University-computer and Information Sciences, 2024, 36(3): 101969.

[17] 郭文俊,杨泽民. 基于区块链的物联网可信访问控制研究[J]. 软件工程,2024,27(6):30-33.

[18] Radhika D, Duraipandian M. Optimized dynamic task scheduling in cloud computing for big data processing[J]. Wireless Networks, 2025,31(5):3661-3672.

[19] Jain A K. Architecting scalable and distributed cloud database systems[J]. International Journal of Technology, Management and Humanities, 2025, 11(2): 1-9.

作者简介:

张艳清(2001-),女(汉族),朔州,硕士生。研究领域:区块链,医疗数据隐私,访问控制。

孙连山(1977-),男(汉族),佳木斯,教授,博士。研究领域:区块链,安全数据治理,大模型安全。本文通信作者。

www.rjgczz.com