计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
63(10): 2527−2542, 2026

物联网中基于区块链与雾计算的轻量级访问控制机制

余 韦[1,2] 许光全[1] 刘如静[2] 张津耀[2] 李春志[1] 白宏鹏[1]
[1](天津大学网络安全学院 天津 300072)
[2](浙江越秀外国语学院国际商学院 浙江绍兴 312000)
(losin@tju.edu.cn)

A Lightweight Access Control Mechanism Based on Blockchain and Fog Computing for the Internet of Things

Yu Wei[1,2], Xu Guangquan[1], Liu Rujing[2], Zhang Jinyao[2], Li Chunzhi[1], and Bai Hongpeng[1]
[1](*School of Cybersecurity*, *Tianjin University*, *Tianjin* 300072)
[2](*International Business School*, *Zhejiang Yuexiu University of Foreign Languages*, *Shaoxing*, *Zhejiang* 312000)

Abstract To address resource constraints of terminal devices, distributed cross-domain trust, and dynamic access policies in large-scale Internet of things (IoT) environments, we propose a lightweight access control mechanism based on blockchain and fog computing. The mechanism adopts a layered architecture of on-chain trusted state maintenance, fog-side real-time authorization, and terminal-side lightweight identity response. High-complexity operations in attribute-based encryption (ABE), including key generation, policy matching, encryption, and decryption, are offloaded to fog nodes, while terminals only perform physical unclonable function (PUF) response generation and SHA-256 hashing. To support fine-grained and trusted cross-domain access, a hybrid authorization framework combining ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE) is designed, where CP-ABE expresses resource-level access policies and KP-ABE supplements user-level resource permissions. Device identity hashes, policy states, and revocation events are recorded on a Hyperledger Fabric consortium blockchain, forming a trusted identity chain that combines PUF-based physical uniqueness with on-chain state consistency. In addition, a short-lived cross-domain access token and a challenge-hash-based verification method are introduced for cross-domain authentication and lightweight outsourced decryption verification. Security analysis shows that the mechanism satisfies identity authentication, session establishment, data confidentiality, collusion resistance, replay resistance, and unforgeability of cross-domain credentials. Prototype experiments show that, with five attributes, CP-ABE encryption and decryption take approximately 13.3 ms and 5.5 ms, respectively, and the data access path latency is approximately 18 ms. The results demonstrate that the proposed mechanism can support fine-grained, auditable, and cross-domain access control for resource-constrained IoT scenarios.

Key words IoT security; access control; attribute-based encryption; blockchain; fog computing; physical unclonable function; provable security

摘 要 针对大规模物联网环境中终端资源受限、跨域信任分散和访问策略动态变化等问题,提出一种区块链与雾计算协同的轻量级访问控制机制。该机制采用“链上可信状态维护、雾侧实时授权计算、端侧轻量身份响应”的分层架构,将属性基加密中的密钥生成、策略匹配与加解密等高复杂度操作迁移至雾节点,终端仅执行物理不可克隆函数响应生成和SHA-256哈希计算。为实现细粒度授权与跨域可信访问,构建

收稿日期: 2026-06-06; **修回日期**: 2026-07-09
基金项目: 国家自然科学基金项目(62672454)
This work was supported by the National Natural Science Foundation of China (62672454).

CP-ABE 与 KP-ABE 协同的混合授权框架,分别表达资源级访问策略和用户级资源权限;同时将设备身份哈希、策略状态和撤销事件写入 Hyperledger Fabric 联盟链,形成 PUF 物理唯一性与链上状态一致性结合的可信身份链。进一步设计短期跨域访问令牌和基于挑战哈希的外包解密验证方法,以支持跨域认证和轻量级结果校验。安全分析表明,该机制满足身份认证、会话建立、数据机密性、抗共谋、抗重放和跨域凭证不可伪造等安全目标。原型实验表明,在 5 个属性条件下,CP-ABE 加密和解密时间分别约为 13.3 ms 和 5.5 ms,数据访问路径延迟约为 18 ms。结果表明,所提机制能够支持资源受限物联网场景下的细粒度、可审计和跨域访问控制。

关键词 物联网安全;访问控制;属性基加密;区块链;雾计算;物理不可克隆函数;可证明安全

中图法分类号 TP393.08

DOI: 10.7544/issn1000-1239.202660455 **CSTR:** 32373.14.issn1000-1239.202660455

物联网终端规模持续扩张,使访问控制同时面临资源受限、跨域信任分散和策略动态变化 3 类约束。大量传感器、车载单元和智能设备缺乏长期保存密钥和执行复杂公钥运算的能力,而业务数据又需要在多组织、多域环境中流转,传统集中式授权模型难以兼顾细粒度控制、审计可信和实时响应。已有研究指出,物联网安全威胁具有终端异构、边界模糊、攻击面广和跨层传播等特点[1],其中访问控制一旦失效,可能导致隐私泄露、权限滥用和跨域风险扩散,因此已成为物联网安全体系中的关键问题[2]。

现有研究主要沿区块链和属性基加密 2 条路线推进:前者提供去中心化存证与策略审计[3-4],后者将访问策略嵌入加密过程,能够实现“不满足策略即无法解密”的密码学约束[5]。单独采用区块链会把高频访问引入共识路径[6],单独采用 ABE 虽能实现细粒度加密访问控制[7],但其加解密和密钥生成过程涉及较多指数运算与双线性配对,在资源受限终端上存在计算开销问题,同时难以单独解决设备物理身份认证和跨域状态一致性问题[2]。

从系统结构看,集中式访问控制与物联网分布式部署之间存在天然错配。百万级终端分布在不同组织和地理区域,单一策略决策点既容易成为性能瓶颈,也难以提供跨域可验证的审计证据[2-3]。

从终端能力看,许多设备仅具备低功耗 MCU、有限 SRAM 和间歇式网络连接,直接执行多次公钥运算会明显增加能耗和时延。属性基加密虽然能够支持细粒度访问控制,但其密钥生成、加密和解密过程通常涉及指数运算与双线性配对,直接部署在资源受限终端上会受到计算能力和能耗约束[8]。因此,方案设计必须把重计算从终端侧移出,同时避免把所有访问请求推入远端云端。

从策略语义看,物联网访问决策往往同时依赖身份、设备状态、资源类别、时间窗口和域间信任关系。单一 RBAC 或 ABAC 模型难以同时表达这些动态条件,也难以在跨组织场景中证明策略执行过程未被篡改[9-10]。

因此,本文没有把问题简化为单一算法替换,而是从计算边界、信任边界和策略边界 3 个层面重新组织访问控制流程:终端侧只保留最低限度的身份证明能力,雾侧承担实时授权与密码计算,链侧负责不可篡改状态和跨域信任。

针对上述问题,本文提出一种双层混合 ABE+PUF+Fabric 联盟链的轻量级访问控制机制。方案将复杂密码运算上移至雾节点,终端仅承担 PUF 响应和哈希计算,并通过 Fabric 维护身份、策略和撤销状态。主要贡献如下:

1)构建基于策略的属性加密(ciphertext-policy ABE, CP-ABE)与基于密钥的属性加密(key-policy ABE, KP-ABE)协同的双层授权框架,分别覆盖资源级细粒度策略和用户级权限管理。

2)将 PUF 物理身份与链上身份哈希绑定,提升低成本终端在跨域环境中的不可克隆认证能力。

3)实现注册、认证、加解密、跨域认证和撤销的端到端原型,并在 Fabric 测试网络上评估实际开销。

4)采用 BAN 逻辑、IND-sCPA 归约和混合论证分析身份认证、会话建立与数据机密性。

5)从计算、通信、链上存储和安全属性维度与典型方案进行对比,验证方案适用于资源受限物联网场景。

1 相关工作

物联网访问控制研究经历了从集中式授权模型到属性驱动授权模型,再到区块链辅助去中心化授

权的演进。传统基于角色的访问控制(role-based access control, RBAC)模型便于权限聚合和集中管理，但在大规模异构终端场景中容易出现角色膨胀，难以适应设备类型、业务场景和组织边界频繁变化的需求[9]。基于属性的访问控制(attribute-based access control, ABAC)通过主体、资源和环境等属性提升了策略表达能力，但通常仍依赖可信策略决策点，难以在跨组织环境中证明属性声明和策略执行过程的可信性[2,10]。为缓解集中式授权中的单点信任问题，已有研究将区块链引入物联网访问控制，通过分布式账本和智能合约记录身份、策略和访问日志，增强跨域环境下的可审计性[3-4,6]。然而，区块链共识过程并不适合承载每次高频数据访问请求，否则容易将毫秒级本地访问扩展为秒级状态变更。因此，如何区分低频可信状态维护与高频本地授权执行，仍是区块链辅助物联网访问控制需要解决的关键问题。

属性基加密(attribute-based encryption, ABE)能够将访问策略与密文或密钥绑定，实现“不满足策略即无法解密”的密码学强制访问控制，是细粒度数据保护的重要技术[5,7-8]。其中，CP-ABE 适合由数据拥有者定义资源级访问策略，KP-ABE 适合由系统或授权中心分配用户侧资源类别权限，二者分别对应资源侧策略表达和用户侧权限管理。然而，ABE 在物联网环境中的直接部署仍面临计算开销和策略维护问题。其密钥生成、加密和解密过程通常涉及指数运算与双线性配对，低功耗终端直接执行会增加时延和能耗。为降低终端负担，已有研究提出外包解密、多权威管理和属性撤销等机制，将部分计算或权限管理过程迁移至云端或边缘节点[11-13]。但外包计算仍需要结果验证机制支撑，多权威和细粒度撤销机制虽然提升了灵活性，也引入了密钥分发、版本同步和跨域协作成本。

除区块链和 ABE 外，物理不可克隆函数(physical unclonable function, PUF)与雾计算也为资源受限物联网访问控制提供了重要支撑。PUF 利用芯片制造差异生成设备唯一挑战——响应关系，可为低成本终端提供无需长期密钥存储的物理身份根，适合传感器、车载单元等难以部署安全存储模块的设备[14-16]。但单独使用 PUF 只能证明设备物理唯一性，难以保证跨组织身份记录和撤销状态的一致性。雾计算将计算、存储和网络能力下沉至靠近终端的边缘侧，适合承载物联网终端无法执行的复杂密码运算[17-18]。Hyperledger Fabric 作为许可链平台，支持成员身份管理、链码执行和多组织状态维护，适合用于联盟场景下的身份、策略和撤销管理[19]。近年来，也有研究尝试将 PUF、区块链、雾计算或属性加密用于车联网认证、云雾协同访问控制和轻量级远程认证等场景[12-13,20-21]。

综上，现有研究已分别从链上审计、细粒度加密、物理身份认证和边缘计算卸载等方面改进物联网访问控制，但仍存在 3 方面不足：一是链上可信状态维护与链下高频授权执行之间缺少清晰分离；二是细粒度数据保护与资源受限终端计算能力之间仍存在矛盾；三是设备物理身份、跨域审计和数据机密性保护尚未形成统一机制。针对上述问题，本文提出融合双层混合 ABE、PUF 与 Fabric 联盟链的轻量级访问控制机制，以兼顾终端轻量化、身份可信、跨域审计和细粒度数据访问控制。

2 预备知识

本文方案涉及属性基加密、物理不可克隆函数、雾计算、Fabric 联盟链以及形式化安全分析等基础技术。本节仅介绍后续系统模型、协议设计和安全性分析所需的基本概念，具体协议流程、链上状态定义和安全推导将在后续章节展开。

ABE 是一类面向细粒度访问控制的公钥加密机制，其核心思想是将访问策略与密文或用户密钥绑定，使满足策略的用户能够解密数据，不满足策略的用户无法获得明文。Feng 等人[5]对属性基密码体制的基本模型和安全性质进行了系统梳理。Goyal 等人[7]提出的 KP-ABE 将访问结构嵌入用户密钥，密文关联属性集合，适合表达用户侧权限；Bethencourt 等人[8]提出的 CP-ABE 将访问策略嵌入密文，用户密钥关联属性集合，适合由数据拥有者定义资源级访问条件。

设属性全集为$\mathcal{U}=\{a_1,a_2,\cdots,a_n\}$，用户属性集合为 $S\subseteq\mathcal{U}$，访问策略为$\mathcal{A}$。以 CP-ABE 为例，其加密和密钥生成过程可抽象为

$$CT=Enc(PK,M,\mathcal{A}),SK_S=KeyGen(MSK,S)。\quad(1)$$

当$S\vDash\mathcal{A}$时，用户可通过 $Dec(SK_S,CT)$恢复明文 M；否则解密失败，输出$\perp$。需要说明的是，式(1)主要用于刻画 CP-ABE 的基本解密条件；在 KP-ABE 中，访问结构嵌入用户密钥，密文关联资源属性集合，二者将在第 3 节的混合授权框架中分别用于资源级策略和用户级权限表达。

ABE 通常建立在双线性映射之上。设G和G_T为

素数阶双线性群，g为G的生成元，双线性映射为$e:G\times G\to G_T$，满足$e(g^a,g^b)=e(g,g)^{ab}$。由于ABE的加密、解密和密钥生成过程通常涉及指数运算与双线性配对，直接部署在低功耗物联网终端上会带来较高计算开销。Green等人[11]提出将ABE解密过程外包给第三方，以降低用户侧计算负担；Yu等人[12]和Xu等人[13]也在云雾辅助或雾计算场景下讨论了属性加密外包、签密和撤销机制。因此，将复杂密码运算迁移至靠近终端的计算节点，是降低资源受限设备负担的重要思路。

PUF利用芯片制造过程中的不可控物理差异生成设备唯一挑战——响应关系，可为低成本终端提供无需长期保存密钥的硬件身份根。Rührmair等人[14]讨论了PUF的基础安全性质，Suh等人[15]将PUF用于设备认证和密钥生成，Dodis等人[16]提出的模糊提取器为从噪声响应中提取稳定密钥材料提供了理论基础，Gassend等人[22]较早提出硅物理随机函数，为后续基于硬件制造差异的设备身份认证提供了基础。给定挑战值c，设备D_i的PUF响应可抽象为$r_i=PUF_{D_i}(c)$。由于不同设备的物理结构存在不可控差异，攻击者即使复制设备标识或程序，也难以生成相同的物理响应。本文后续将PUF响应与链上身份状态结合，用于增强设备在跨域环境中的不可克隆认证能力。

雾计算由Bonomi等人[17]提出，其核心思想是将计算、存储和网络能力下沉至靠近终端的边缘侧，以满足物联网场景中的低时延、大规模接入和近端服务需求。Alrawais等人[18]进一步指出，雾计算在物联网安全与隐私保护中可承担近端认证、数据处理和安全服务部署等任务。对于资源受限终端而言，雾节点能够承担ABE密钥生成、加解密、会话管理和跨域凭证处理等复杂操作，从而降低终端计算负担并减少远端云往返延迟。

Hyperledger Fabric是一种面向许可链场景的联盟链平台。Androulaki等人[19]提出的Fabric架构支持成员身份管理、链码执行、背书策略和共享账本维护，适合多组织协同但互信不足的联盟场景。与公有链相比，Fabric中参与方具有明确组织身份，可通过成员服务、背书策略和链码执行机制约束状态更新过程，因而更适合多组织许可链环境下的身份、策略和撤销状态维护。

本文利用Fabric维护身份、策略和撤销等低频可信状态，而将高频数据访问和密码计算放在雾侧完成，以避免每次访问均进入共识路径。

BAN逻辑由Burrows、Abadi和Needham[23]提出，常用于认证协议中的信任关系和消息新鲜性分析。本文使用的基本符号包括：$P\mid\equiv X$表示主体P相信命题X；$P\mid\sim X$表示P接收到消息X；$P\mid\sim X$表示主体P曾发送消息X；$\#(X)$表示消息X是新鲜的；$P\Rightarrow X$表示P对命题X具有管辖权。为避免符号推导在预备知识中过度展开，本文仅给出BAN逻辑的2条基本思想：其一，若主体P相信自己与Q共享密钥K，且P收到由K保护的消息X，则P可以相信该消息曾由Q发送；其二，若P进一步相信X是新鲜的，则可以将“曾经发送”提升为“当前相信”。后续第4节将基于这些规则分析设备认证、会话令牌和跨域凭证的有效性。

判定双线性Diffie-Hellman(decisional bilinear Diffie-Hellman, DBDH)假设是双线性群上常用的困难性假设。给定$(g,g^a,g^b,g^c,Z)\in G^4\times G_T$，DBDH问题要求判断$Z$是$e(g,g)^{abc}$还是$G_T$中的随机元素。若任意概率多项式时间敌手均不能以非忽略优势区分二者，则认为DBDH假设成立。本文后续在该假设下分析CP-ABE与KP-ABE组件的IND-sCPA安全性，并通过混合论证说明双层ABE框架的数据机密性。

3 系统模型与方案设计

3.1 系统架构

本文采用“云—链—雾—端”四层协同架构，在端层与云层之间引入雾节点和Fabric联盟链层，如图1所示。该架构参照Bonomi等人[17]提出的雾计算范式，将部分计算、存储和安全服务下沉至靠近终端的边缘侧，以降低远端云交互带来的时延。同时，结合Hyperledger Fabric许可链架构的成员身份管理、链码执行和多组织账本维护能力[19]，并参考其在物联网属性访问控制实现中的适配性研究[24]，在雾层与云层之间构建链上可信状态维护层。

系统参与实体包括物联网终端、雾节点、Fabric联盟链和云服务中心。端层由传感器、车载单元、智能终端等异构设备组成，负责数据采集和轻量级身份响应；雾层部署在管理域边缘，承担设备认证、会话管理、ABE密钥生成与加解密、跨域凭证生成和本地缓存等任务；链层基于Hyperledger Fabric构建，用于维护设备身份哈希、访问策略状态、撤销状态和域间信任白名单；云层负责长期数据备份、证书管理和批量分析，不参与实时访问控制决策。

该架构的核心思想是将实时性要求较高的数据

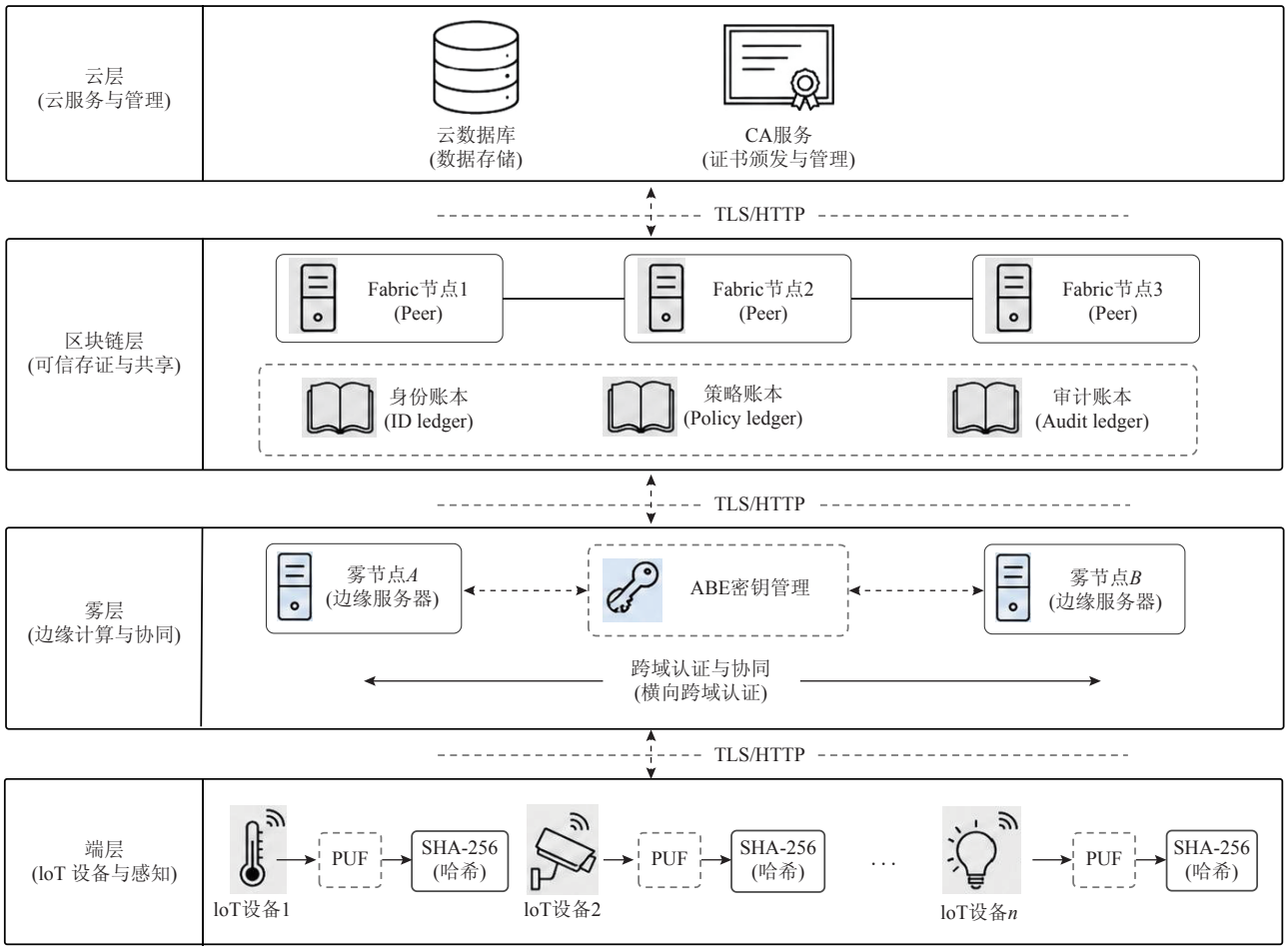


Fig. 1 Four-layer system architecture of cloud fog chain end

图 1 云雾链端 4 层系统架构

访问路径放在雾侧，将一致性和可审计性要求较高的身份、策略、撤销和域间信任状态放在链上。端层设备内置 PUF 模块，在注册和认证阶段根据挑战值生成响应。PUF 可利用芯片制造差异生成设备唯一响应，适合用于设备认证和密钥生成[15,22]。因此，终端设备无需保存长期私钥，也不执行双线性配对等复杂公钥运算。雾节点负责维护 PUF 挑战、验证设备身份、执行 CP/KP-ABE 相关密码运算，并在认证通过后生成短期会话 Token。Fabric 联盟链通过链码维护设备状态和策略状态，为跨组织身份认证、策略审计和撤销管理提供一致可信依据。云层仅提供长期备份和离线分析能力，避免远端云往返延迟进入实时访问控制路径。

因此，PUF 提供设备物理唯一性，Fabric 提供跨域状态一致性，雾节点提供近端密码计算能力。三者共同构成从终端身份认证到数据授权访问的轻量级访问控制闭环。

3.2 威胁模型与安全目标

物联网安全威胁具有终端异构、攻击面广、边界模糊和跨域传播等特点[1]，访问控制一旦失效，可能导致隐私泄露、越权访问和跨域风险扩散[2]。本文依据 GB/T 22239 对身份鉴别、访问控制、安全审计和可信验证等方面的要求，考虑资源受限物联网场景中的典型攻击。敌手可监听端—雾、雾—链以及跨域通信信道，获取认证请求、访问请求和跨域凭证等消息；也可注入、篡改或重放历史消息，尝试绕过身份认证或访问控制策略。敌手还可能复制设备软件标识，伪造设备身份，组合多个用户的 ABE 密钥分量实施共谋解密，或由恶意管理域伪造跨域凭证和设备属性声明。

本文考虑的主要攻击能力包括窃听与篡改攻击、重放攻击、设备克隆攻击、共谋解密攻击、恶意域伪造攻击和好奇雾节点攻击。其中，设备克隆攻击指敌手可复制设备标识符或软件凭据，但难以复制真实设备的 PUF 物理响应；共谋解密攻击指多个用户组合各自持有的 ABE 密钥分量，尝试解密单个用户本不满足策略的密文；好奇雾节点攻击指雾节点按照协议执行计算，但可能尝试从中间计算结果、访问

请求或外包解密结果中获取额外信息。

本文作出如下安全假设：Fabric 联盟链在既定容错条件下能够保证账本状态一致性和交易不可篡改性[19]；PUF 满足不可克隆性和响应不可预测性[14-15,22]；SHA-256、ECDSA、ABE 等密码学原语满足相应标准安全性；雾节点为诚实但好奇实体，可按协议完成认证转发、授权计算和外包解密辅助，但不应获得用户数据明文、ABE 主密钥或可独立恢复数据密钥的完整信息。其行为受链上设备状态、策略版本、Token 有效期和审计日志约束，返回的外包结果由挑战哈希证明进行轻量验证。

围绕身份可信、数据机密、访问可控和跨域可审计等需求，本文设定 5 项安全目标：G1 设备身份不可伪造，未注册设备或无法产生正确 PUF 响应的设备不能通过认证；G2 数据机密性与抗共谋，不满足访问策略的用户不能解密受保护数据，多个用户也不能通过组合 ABE 密钥分量绕过访问策略；G3 抗重放，历史认证消息、会话 Token 和跨域凭证不能被重复使用；G4 跨域凭证不可伪造，恶意域或外部攻击者不能伪造合法跨域访问凭证；G5 外包计算结果可验证，雾节点返回的外包解密结果可通过轻量方式进行校验。上述目标分别由 PUF 与链上身份哈希绑定、CP/KP-ABE 的 IND-sCPA 安全性、短期 Token、ECDSA 签名、链上信任白名单以及挑战哈希证明共同实现。

3.3 系统初始化与链上状态

系统初始化阶段由可信授权机构生成系统公共参数、ABE 主密钥和链上初始状态。ABE 能够将访问策略与密文或密钥绑定，实现细粒度访问控制[5,7-8]。近年来，区块链与属性访问控制、ABE 的结合也被用于提升物联网数据访问过程中的透明性、可追溯性和去中心化管理能力[25]。本文采用 CP-ABE 与 KP-ABE 协同的双层授权结构，其中 CP-ABE 用于表达资源级细粒度策略，KP-ABE 用于表达用户级资源类别权限。

系统首先选择素数阶双线性群G和G_T，生成元为g，双线性映射为$e:G\times G\to G_T$。CP-ABE 与 KP-ABE 分别生成独立的主密钥和公钥：

$$\left(MSK_{\mathrm{cp}},PK_{\mathrm{cp}}\right)\leftarrow Setup_{\mathrm{cp}}(1^{\lambda}),\tag{2}$$

$$(MSK_{\mathrm{kp}},PK_{\mathrm{kp}})\leftarrow Setup_{\mathrm{kp}}(1^{\lambda})。\tag{3}$$

2 层密钥空间相互独立，分别服务于资源级策略控制和用户级权限管理，避免跨层随机性复用。

同时，Fabric 联盟链部署身份管理、策略管理和撤销管理链码，初始化设备状态表、策略版本表和域间信任白名单。本文将链上设备状态抽象为

$$State_i=\left(h_i,policy_{ver_i},status_i\right),\tag{4}$$

其中，h_i表示设备身份哈希，$policy_{ver_i}$表示当前策略版本，$status_i$表示设备生命周期状态，$status_i\in\{\text{active},\text{revoked}\}$。链上只维护身份、策略和撤销相关状态，不保存明文、密文和 PUF 原始响应，以降低账本膨胀和敏感信息扩散风险。

3.4 设备注册、认证与撤销

设备注册阶段用于建立 PUF 物理身份与链上身份记录之间的绑定关系，注册协议时序如图 2 所示。雾节点首先为设备D_i生成随机挑战c_i，设备调用本地 PUF 模块输出响应：$r_i=PUF_{D_i}(c_i)$，雾节点计算设备身份哈希：

$$h_i=H(device_{\mathrm{id}}\|r_i),\tag{5}$$

其中$H(\cdot)$表示 SHA-256 哈希函数。随后雾节点调用 Fabric 链码，将h_i、策略版本号和设备状态写入链上。链上仅保存身份哈希，不保存原始 PUF 响应。设备认证阶段采用“本地 PUF 校验+链上状态查询”的双重验证方式。雾节点向设备发送新的挑战值c_i'，设备返回响应$r_i'=PUFD_i(c_i')$，雾节点根据预登记的挑战——响应信息或本地 PUF 验证函数进行校验：

$$Verify_{\mathrm{PUF}}(ID_i,c_i',r_i')=1。\tag{6}$$

设备认证流程如图 3 所示，若本地校验通过，则进一步查询 Fabric 链上状态，确认$status_i=\text{active}$。验证通过后，雾节点生成短期会话$token=H(ID_i\|t\|nonce)$，其中t为时间戳，$nonce$为随机数。后续数据访问优先使用本地会话缓存，避免每次访问都进入链上共识路径。当设备失效、被盗或存在异常行为时，管理员调用 Fabric 链码执行撤销操作：$status_i\leftarrow\text{revoked}$。

需要说明的是，链上身份哈希用于绑定注册阶段的设备身份记录，认证阶段的新挑战响应由雾节点在链下完成 PUF 校验；Fabric 主要用于确认设备是否已注册且状态为 active，而不直接保存或比对原始 PUF 响应。链上撤销交易确认后，雾节点清除本地会话缓存、PUF 挑战记录和相关 Token 信息。后续认证阶段，一旦查询到链上状态为 revoked，则拒绝该设备访问。由于注册、认证和撤销属于低频管理操作，其链上交易延迟不会进入高频数据访问路径。

为降低 PUF 响应噪声对认证结果的影响，注册阶段可采用受控安全信道完成初始挑战——响应对采集，并结合模糊提取器或汉明距离阈值对响应偏差进行容忍。雾节点对挑战值设置一次性使用和有

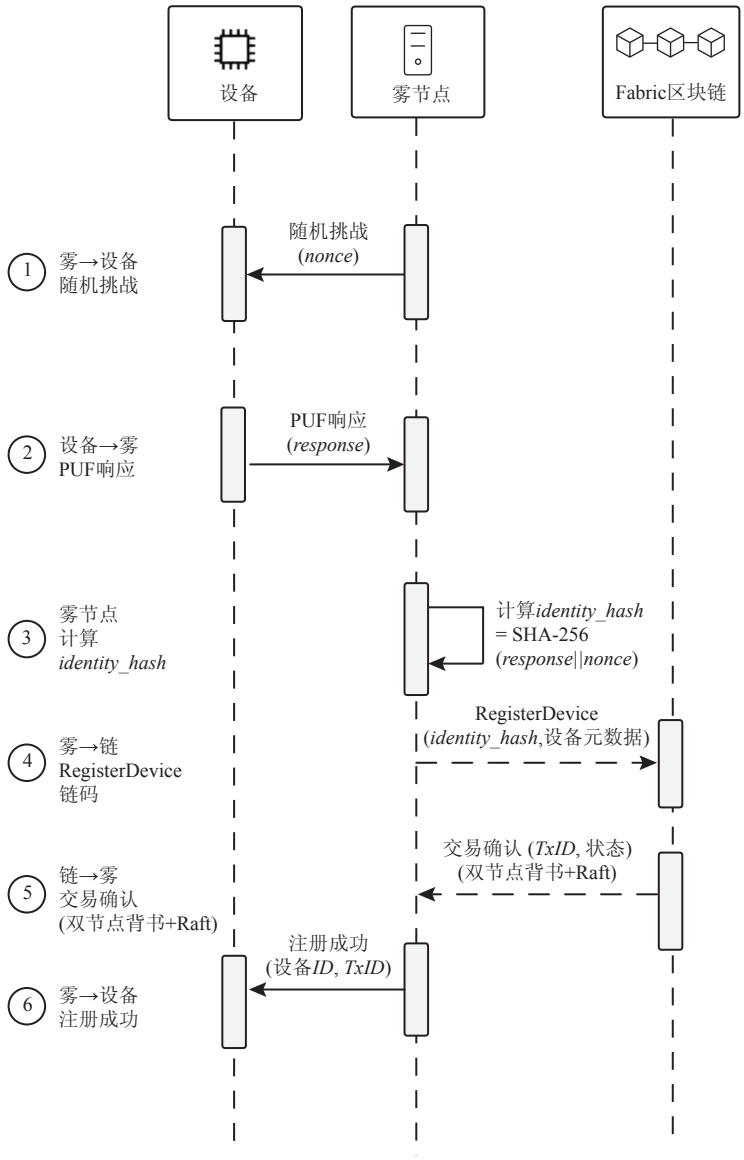


Fig. 2 Sequence diagram of device registration protocol

图 2 设备注册协议时序图

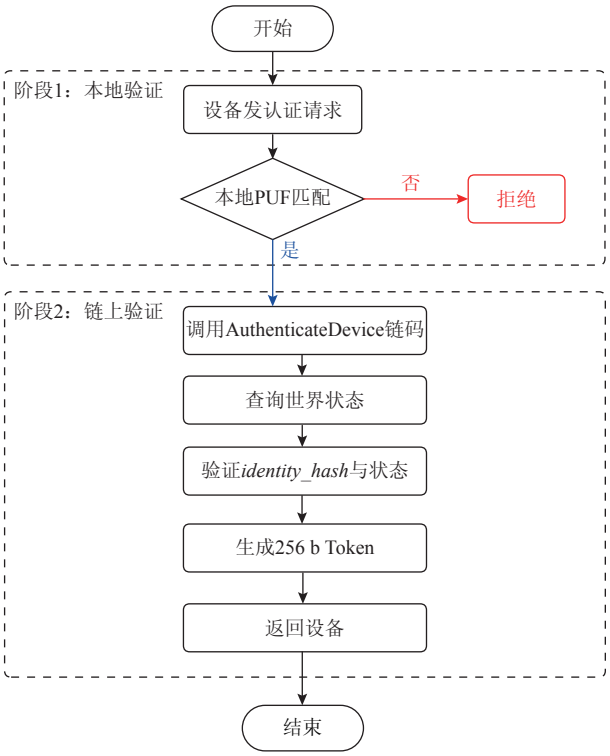
效期约束，避免同一挑战被重复利用。设备撤销交易确认后，链上状态、雾节点本地会话缓存、挑战记录和 Token 状态同步更新，后续认证请求均以链上最新状态为准。

3.5 混合 ABE 数据访问控制

已有研究表明，区块链与 ABE 结合能够增强物联网数据访问控制中的可审计性和细粒度授权能力[25]。基于第 2 节所述 CP-ABE 与 KP-ABE 的策略绑定差异，本文设计二者协同的混合访问控制框架：CP-ABE 用于表达由数据拥有者定义的资源级细粒度策略，KP-ABE 用于表达系统或授权中心分配的用户级资源类别权限。

图 4 展示了混合 ABE 机制的分支选择式授权流程。系统在接收访问请求后，首先进行设备身份、链上状态和策略有效性校验；若资源存在有效 CP 策略，则优先执行 CP-ABE 判定，属性满足时授权访问并恢复数据密钥，不满足时直接拒绝访问，且不回退至 KP-ABE。仅当资源不存在有效 CP 策略或 CP 策略缺省时，系统才启用 KP-ABE 补充分支，根据用户密钥策略与资源属性的匹配结果决定是否授权。对于策略校验失败、设备状态异常或分支条件不满足的情况，系统均采用默认拒绝原则，并将授权结果写入区块链审计日志。

本文采用“CP-ABE 优先、KP-ABE 补充”的授权逻辑：对于配置了强制资源级策略的密文，必须满足 CP-ABE 策略后才能访问；对于未配置细粒度资源策略或系统策略允许按资源类别授权的场景，再由 KP-ABE 判断用户是否具有相应资源类别权限。因此，



注：Token 有效期为 1 h，后续数据路径不经过区块链。

Fig. 3 Flow chart of equipment certification

图 3 设备认证流程图

KP-ABE 不用于绕过资源拥有者显式定义的 CP-ABE 策略，而是用于补充资源级策略缺省或用户级权限管理场景。若 2 层策略均不满足，则系统拒绝访问。

由表 1 可见，CP-ABE 策略具有优先约束作用。当资源存在有效 CP 策略时，系统以 CP-ABE 判定结果为准，KP-ABE 不作为绕过 CP 策略的回退路径；仅当资源不存在有效 CP 策略或 CP 策略缺省时，KP-ABE 才作为用户级资源类别权限的补充判定机制。

混合 ABE 数据访问控制流程如图 5 所示。发送方根据资源级策略和资源属性生成双层密文，2 层密钥空间相互独立；接收方按照上述授权逻辑进行解密判断。

设明文数据为 M，资源访问策略为 $\mathcal{A}_{\mathrm{cp}}$，用户属集合为 S。CP-ABE 加密过程可抽象为

$$CT_{\mathrm{cp}} = Enc_{\mathrm{cp}}\left(PK_{\mathrm{cp}}, M, \mathcal{A}_{\mathrm{cp}}\right) 。 \tag{7}$$

用户密钥为 $SK_S = KeyGen_{\mathrm{cp}}(MSK_{\mathrm{cp}}, S)$。当 $S \vDash \mathcal{A}_{\mathrm{cp}}$ 时，用户可恢复明文：$M = Dec_{\mathrm{cp}}(SK_S, CT_{\mathrm{cp}})$；否则解密失败，输出 $\perp$。KP-ABE 层将策略绑定在用户密钥中。设资源属性集合为 $\mathcal{A}_{\mathrm{r}}$，用户访问结构为 $\mathcal{A}_{\mathrm{kp}}$，则 KP-ABE 加密和解密可表示为：

$$CT_{\mathrm{kp}} = Enc_{\mathrm{kp}}\left(PK_{\mathrm{kp}}, M, \mathcal{A}_{\mathrm{r}}\right) , \tag{8}$$

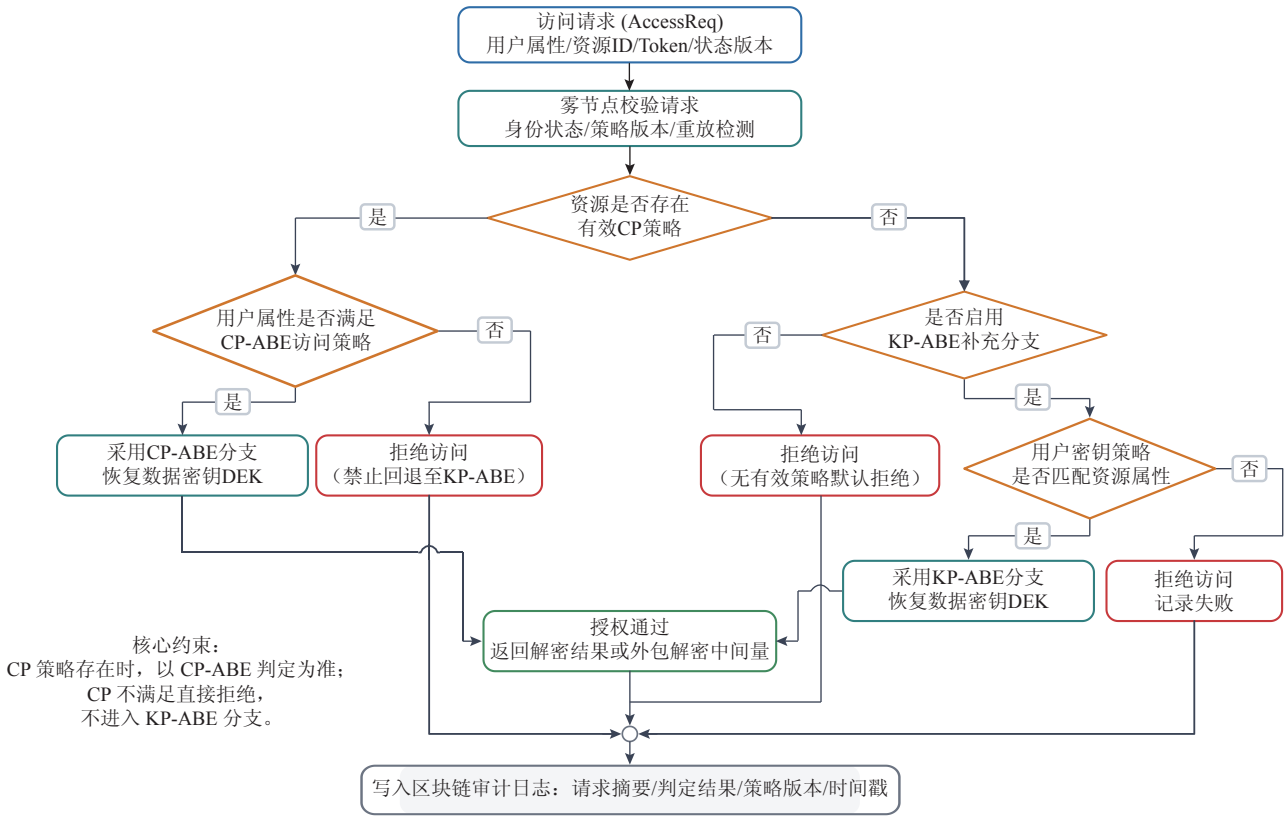


Fig. 4 Mixed ABE branch selection-based authorization process

图 4 混合 ABE 分支选择式授权流程

Table 1 Mixed ABE Authorization Decision Rules

表 1 混合 ABE 授权判定规则

资源 CP 策略状态	CP-ABE 判定结果	KP-ABE 补充分支	KP-ABE 判定结果	系统处理结果
存在有效 CP 策略	满足	不启用	不判定	授权访问，采用 CP-ABE 分支恢复数据密钥
存在有效 CP 策略	不满足	不启用	不判定	拒绝访问，禁止回退至 KP-ABE
CP 策略无效或缺省	不判定	启用	满足	授权访问，采用 KP-ABE 分支恢复数据密钥
CP 策略无效或缺省	不判定	启用	不满足	拒绝访问
CP 策略无效或缺省	不判定	未启用	不判定	默认拒绝访问
策略校验失败或设备异常	不执行	不执行	不执行	拒绝访问，并触发状态同步或审计记录

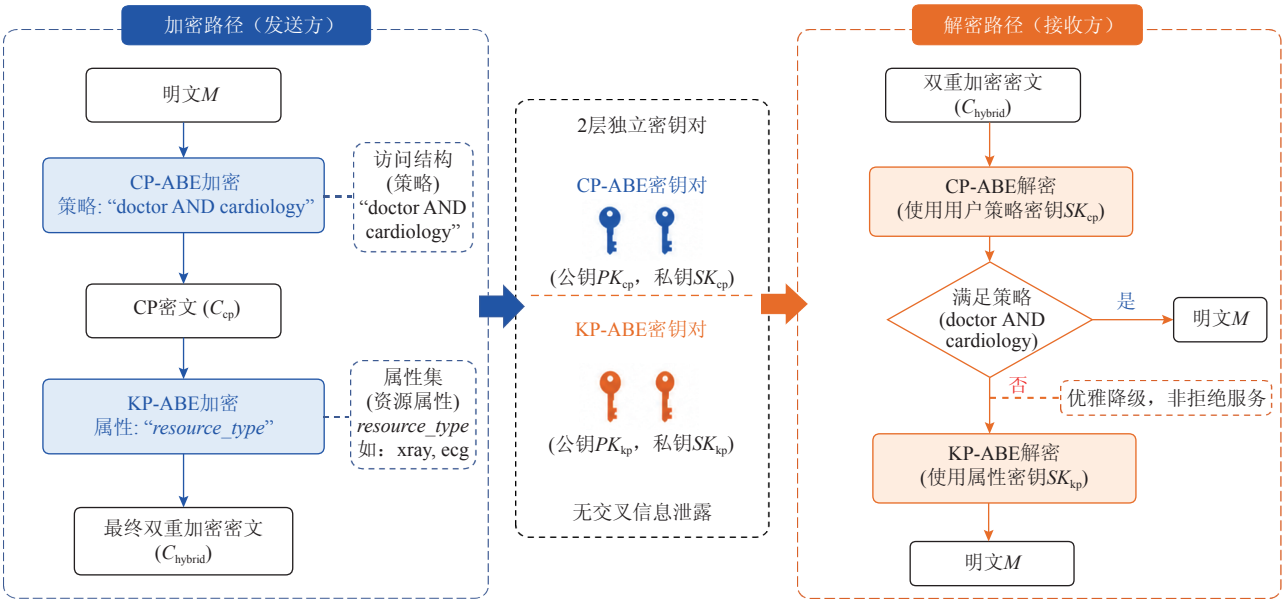


Fig. 5 Hybrid ABE encryption and decryption framework

图 5 混合 ABE 加解密框架

$$SK_{\mathcal{A}_{kp}} = KeyGenkp\left(MSK_{kp}, \mathcal{A}_{kp}\right) 。 \tag{9}$$

当$\mathcal{A}_r \vDash \mathcal{A}_{kp}$时，KP-ABE 解密成功；否则拒绝访问。

2 层 ABE 使用独立主密钥和独立随机数空间，避免密钥分量跨层复用。由于 ABE 加解密过程通常涉及较高计算开销，已有研究提出将 ABE 解密外包给第三方以降低用户侧负担[11]。本文进一步将 CP/KP-ABE 的密钥生成、策略匹配和加解密等重运算迁移至雾节点，终端侧仅进行 PUF 响应和哈希计算，从而降低资源受限设备的计算负担。

3.6 跨域认证与可验证外包解密

跨域认证用于支持设备从源域访问目标域资源。近年来，PUF 与区块链结合已被用于车联网等场景中的设备认证和隐私保护[20]，区块链与轻量密码机制也被用于雾辅助物联网远程认证[21]。同时，零信任访问控制等近期研究表明，区块链与细粒度加密机制结合仍是物联网跨域可信访问的重要方向[26]。设备在源域完成认证后，源域雾节点查询 Fabric 链上身份状态，并构造短期跨域访问令牌：

$$T_{cross} = (ID_i, h_i, Attr, dom_{sou}, dom_{tar}, t, exp) , \tag{10}$$

其中，$Attr$表示设备或用户属性集合，t表示签发时间，exp表示过期时间。源域雾节点对令牌核心字段进行 ECDSA 签名：

$$\sigma = Signsk_{sou}(H(T_{cross})) 。 \tag{11}$$

目标域收到跨域访问请求后，依次验证凭证字段完整性、源域签名、时间戳和过期时间、目标域字段、链上信任白名单以及链上身份哈希。只有上述条件均满足时，目标域才接受该跨域凭证。跨域凭证验证流程如图 6 所示。目标域依次完成字段完整性检查、哈希与签名校验、时效性检查、目标域匹配、链上信任白名单查询和链上身份哈希仲裁。

为降低终端计算负担，本文将 ABE 解密过程外包至雾节点执行。云雾辅助访问控制和外包属性加密已有相关研究基础[11-13]。相关综述表明，ABE 在云计算和物联网访问控制中已被广泛用于细粒度授权，

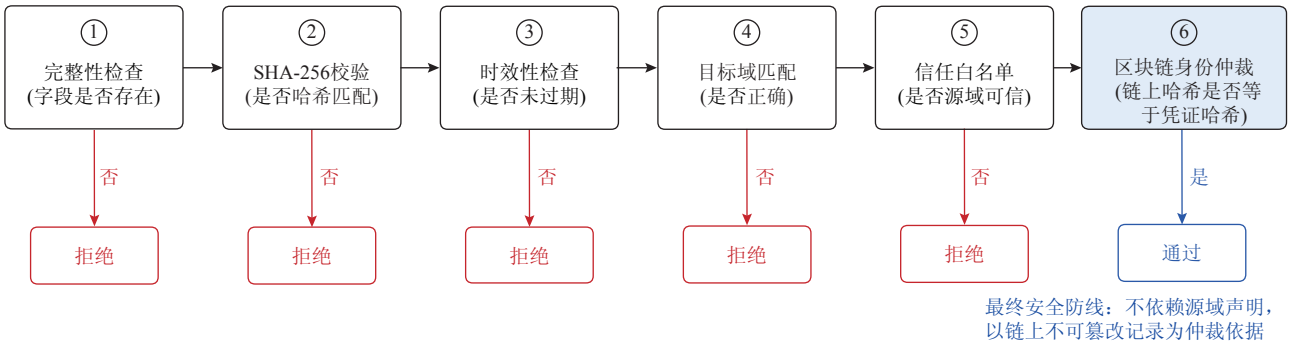


Fig. 6 Six-step verification of cross domain authentication

图 6 跨域认证 6 步验证

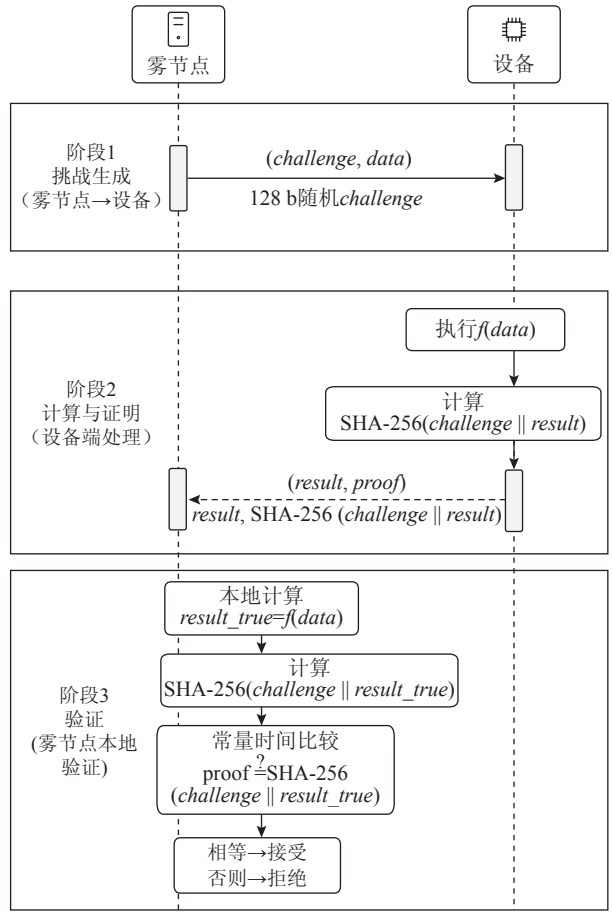
但其计算开销、属性撤销和动态策略管理仍是实际部署中的主要限制[27-28]。近年来，也有研究将多权威 ABE、属性基签密和区块链结合，用于边缘辅助物联网访问控制和安全数据共享[29-30]。然而，外包计算结果仍需要轻量验证机制来避免错误或恶意返回。本文引入基于挑战哈希的验证方法。雾节点生成随机挑战 *challenge*，并将其与密文标识发送给设备。设备基于原始数据 M_{raw} 计算证明：

$$\pi = H(challenge \| M_{\text{raw}}) \text{ 。} \tag{12}$$

雾节点执行 ABE 解密得到结果（M'），并验证

$$\pi \stackrel{?}{=} H(challenge \| M') \text{ 。} \tag{13}$$

若等式成立，则说明解密结果与设备原始数据一致；否则，拒绝该结果。比较过程采用常量时间比较，以降低时序侧信道风险。可验证外包解密流程如图 7 所示。该流程包括挑战生成、设备侧证明计算和雾节点本地验证 3 个阶段。终端侧仅需执行 1 次哈希计算，避免重复执行 ABE 解密或双线性配对运算。该方法适用于终端仍可持有或重构原始采集数据的场景；对于终端无法保留原始明文的场景，可进一步结合消息认证码、承诺机制或可信执行环境扩展验证能力。



注：设备端仅 $f(data)$ + 1次 SHA-256，Cortex-M0 约 50~100 μs。

Fig. 7 Flow chart of three-stage protocol interaction

图 7 三阶段协议交互流程图

4 安全性评估

4.1 认证与会话安全分析

BAN 逻辑用于刻画协议认证层面的主体相信关系、消息新鲜性和管辖权推理；ABE 组件的数据机密性则在第 4.2 节中基于 DBDH 假设进行说明。

在设备认证阶段，雾节点 F 首先生成新鲜挑战 *challenge*，设备 D 返回 PUF 响应 $response = PUF_D(challenge)$。PUF 可基于芯片制造差异生成难以复制的挑战——响应关系，适合用于设备认证和密钥生成[14-15,22]。认证过程可抽象为：雾节点接收设备发送的 $(ID_i, challenge, response)$，并从 Fabric 账本读取对应设备的身份状态 $(h, status)$。

初始假设包括：雾节点相信挑战 *challenge* 是新鲜的；Fabric 对链上身份状态具有管辖权；合法设备的 PUF 对给定挑战具有不可克隆响应能力。由于响应 *response* 与新鲜挑战 *challenge* 绑定，历史响应无法通过校验。结合第 3.4 节的双重认证流程，雾节点首先基于预登记挑战——响应信息或本地 PUF 验证函

数校验(*challenge*,*response*)是否匹配；若本地 PUF 校验通过，再查询链上设备状态。若链上状态为 active，则雾节点可相信该设备为已注册且未撤销的合法终端。

会话建立阶段，Token 由雾节点在设备认证通过后生成，并绑定随机数、时间戳和有效期。由于 Token 具有新鲜性和有效期约束，历史 Token 在过期后无法通过验证，攻击者即使截获旧 Token，也难以在后续会话中继续使用。因此，协议能够支持设备身份认证、短期会话建立和抗重放。设备身份认证的 BAN 逻辑推导过程如图 8 所示。

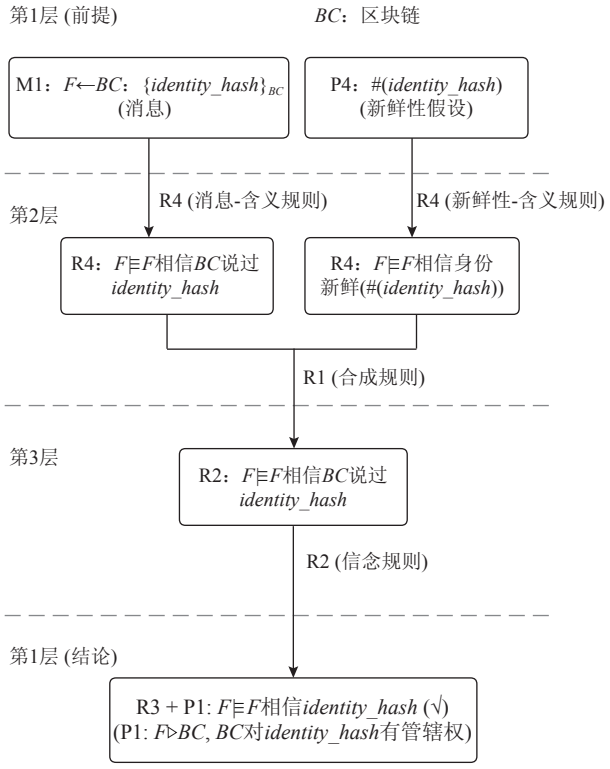


Fig. 8 BAN logical identity authentication derivation tree

图 8 BAN 逻辑身份认证推导树

4.2 数据机密性与抗共谋分析

根据第 3.5 节给出的混合 ABE 数据访问控制机制，本节从策略满足性、IND-sCPA 安全性和抗共谋性 3 个方面分析数据机密性。CP-ABE 层用于约束资源级访问策略，只有用户属性集合 S 满足资源访问策略 A_{cp} 时，用户才能恢复对应密文；KP-ABE 层用于补充用户级资源类别权限，只有资源属性集合 A_{r} 满足用户密钥中的访问结构 A_{kp} 时，用户才能获得相应授权。若 2 层授权条件均不满足，系统拒绝访问。

在选择明文攻击模型下，ABE 组件的 IND-sCPA 安全性可归约至 DBDH 假设。给定 DBDH 实例 (g,g^a,g^b,g^c,Z)，敌手需要判断 $Z=e(g,g)^{abc}$ 是否还是目标群中的随机元素。若存在概率多项式时间敌手能够以非忽略优势区分挑战密文对应的明文，则可构造算法利用该敌手区分真实 DBDH 元素和随机元素，从而违背 DBDH 假设。因此，在 DBDH 假设成立时，CP-ABE 和 KP-ABE 组件在相应标准安全模型下满足 IND-sCPA 安全性[7-8]。

4.3 跨域认证与外包验证安全分析

跨域认证过程主要面向凭证篡改、跨域重放和恶意域伪造等攻击。根据第 3.6 节，源域雾节点在设备认证通过后生成短期跨域访问令牌并对令牌核心字段进行签名。

目标域收到跨域访问请求后，依次验证字段完整性、源域签名、凭证时效性、目标域匹配、源域信任白名单和链上身份哈希。若攻击者篡改令牌字段，则哈希或签名验证失败；若攻击者重放旧凭证，则时间戳和过期时间检查失败；若恶意域伪造凭证，则无法通过源域签名和链上白名单验证。因此，跨域凭证能够满足来源真实性、字段完整性和抗重放性。

对于外包解密，采用挑战哈希机制验证雾节点返回结果。雾节点发送随机挑战 *challenge*，设备基于原始数据 M_{raw} 生成证明：雾节点解密得到结果 M' 后，比较 π 与 $H(challenge\|M')$ 是否相等。由于挑战 *challenge* 具有新鲜性，历史证明不能被重复使用；若雾节点返回错误明文，即 $M'\neq M_{\mathrm{raw}}$，则在 SHA-256 抗碰撞性假设下，等式成立的概率可忽略。因此，该机制能够以一次哈希计算实现轻量级外包结果校验。需要说明的是，该方法适用于终端能够保留或重构原始采集数据的场景；若终端无法保存原始明文，可进一步结合消息认证码、承诺机制或可信执行环境扩展验证能力。

4.4 安全属性对比

本文从混合授权、策略链上存证、跨域认证、可验证外包、PUF 身份绑定、终端轻量化和形式化分析等维度与典型方案进行比较，如表 2 所示。

Xiong 等人[20]的方案侧重 PUF 与区块链结合的车联网认证，能够抵抗设备克隆，但主要面向身份认证场景，对细粒度数据访问控制支持不足。LH-ABSC 方案采用云雾辅助的属性基签密机制，能够降低终端计算负担，但缺少 PUF 物理身份绑定和链上跨域状态管理[12]。Xu 等人[13]的方案支持多权威属性管理和外包撤销，但系统复杂度较高，且未结合设备物理身份。Harbi 等人[21]的方案强调雾辅助物联网中的轻量级远程认证，但对数据机密性和细粒度授权覆盖有限。

由表 2 可见，本方案同时结合 PUF 物理身份、

Table 2 Security Attribute Comparison

表 2 安全属性对比

对比维度	本方案	文献[20]	LH-ABSC	文献[13]	文献[21]
混合 ABE(CP+KP)	✓	×	△	×	×
策略链上存证	✓	△	×	×	△
跨域认证	✓	△	×	×	×
可验证外包	✓	×	△	✓	×
PUF 身份绑定	✓	✓	×	×	△
终端零配对运算	✓	✓	✓	✓	✓
形式化验证	BAN+DBDH	安全分析			安全分析

注：“✓”表示明确支持，“△”表示部分支持、场景限定或实现侧重点不同，“×”表示未涉及或支持不足。

Fabric 链上可信状态、CP/KP-ABE 双层授权和挑战哈希式外包验证机制，在终端轻量化、跨域可审计、细粒度数据保护和认证安全性方面具有综合优势。需要说明的是，本方案并非追求所有单项指标最优，而是在资源受限物联网场景下对安全属性覆盖和工程可部署性进行折中。图 9 进一步展示了不同方案在核心安全属性上的覆盖差异。可以看出，本方案在不可否认性、策略防篡改、数据机密性、抗物理攻击、抗重放和抗共谋等维度上覆盖较均衡。相比之下，Xiong 等人[20]的方案更侧重身份认证与抗物理攻击，LH-ABSC 更侧重数据机密性和抗共谋，Harbi 等人[21]的方案更偏向轻量级认证。本方案并非在所有单项指标上最优，而是在资源受限物联网场景下兼顾身份可信、策略审计、数据保护和跨域访问控制。

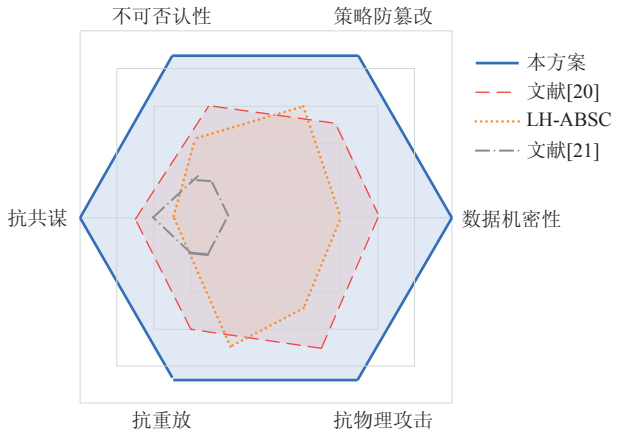


Fig. 9 Comparison of comprehensive security attributes of different schemes

图 9 不同方案综合安全属性对比

5 性能分析

5.1 实验环境

本文基于 Hyperledger Fabric 2.2.15、PBC 0.5.14 和 Flask 2.3.3 实现原型系统。实验环境为 WSL Ubuntu 20.04，硬件配置为 Intel Core i7-12700H 处理器、16 GB DDR5 内存和 1 TB NVMe SSD。Fabric 测试网络包括 1 个 Orderer 和 2 个组织 Peer，并启用 TLS 双向认证。ABE 核心运算采用 PBC 库和 SS512 曲线实现，服务端通过 REST API 提供注册、认证、加解密、跨域认证和撤销接口。除特别说明外，所有实验均重复运行多次并取平均值。

5.2 ABE 核心计算开销

首先测试 CP-ABE 与 KP-ABE 在单属性条件下的核心运算开销。由于 ABE 运算通常涉及指数运算和双线性配对，其计算开销是衡量方案是否适合资源受限物联网场景的重要指标[5,7-8]。结果如表 3 所示。

Table 3 Core Computing Performance of ABE

表 3 ABE 核心运算性能

操作	耗时/ms	平均耗时/ms
系统初始化（CP+KP 双 Setup）	4.2~5.6	4.8
用户密钥生成（CP+KP 双 KeyGen）	4.8~5.6	5.1
CP-ABE 加密（BSW07，单属性）	3.1~3.5	3.3
CP-ABE 解密（BSW07，单属性）	1.4~1.7	1.5
KP-ABE 加密（GPW06，单属性）	1.7~2.1	1.9
KP-ABE 解密（GPW06，单属性）	0.4~0.6	0.5

实验结果表明，在单属性场景下，CP-ABE 与 KP-ABE 核心运算均可在毫秒级完成，其中 KP-ABE 整体开销低于 CP-ABE。CP-ABE 加密开销主要来自访问策略相关的群元素生成和指数运算，KP-ABE 在密钥生成阶段吸收更多策略复杂度，因此单次加密和解密开销相对较低。该结果说明，将 ABE 重运算放在雾节点执行是可行的。雾计算能够将计算、存储和安全服务下沉至靠近终端的边缘侧[17-18]，因此终端侧仅保留 PUF 响应和哈希计算能够显著降低资源受限设备负担。

属性规模对 ABE 核心计算性能的影响如图 10 所示。进一步在 1、3、5、10、15 和 20 个属性条件下测试属性规模对计算开销的影响。结果显示，CP-ABE 与 KP-ABE 主要运算随属性数量近似线性增长；当属性数量增加到 20 时，KeyGen 仍低于 100 ms。说明在常见边缘服务器能力下，几十个属性范围内的 ABE 操作可以作为实时访问控制的一部分。由于终端不参与配对运算，策略复杂度增长主要影响雾节点 CPU 时间和密文大小，而不会显著增加终端计算负担。

5.3 端到端延迟与链上开销

端到端测试结果表明，设备注册和设备认证的

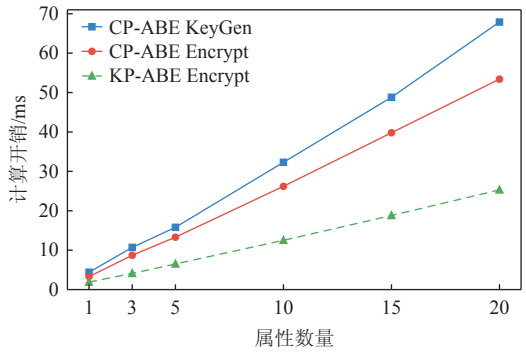


Fig. 10 Effect of attribute size on ABE core computation performance

图 10 属性规模对 ABE 核心计算性能的影响

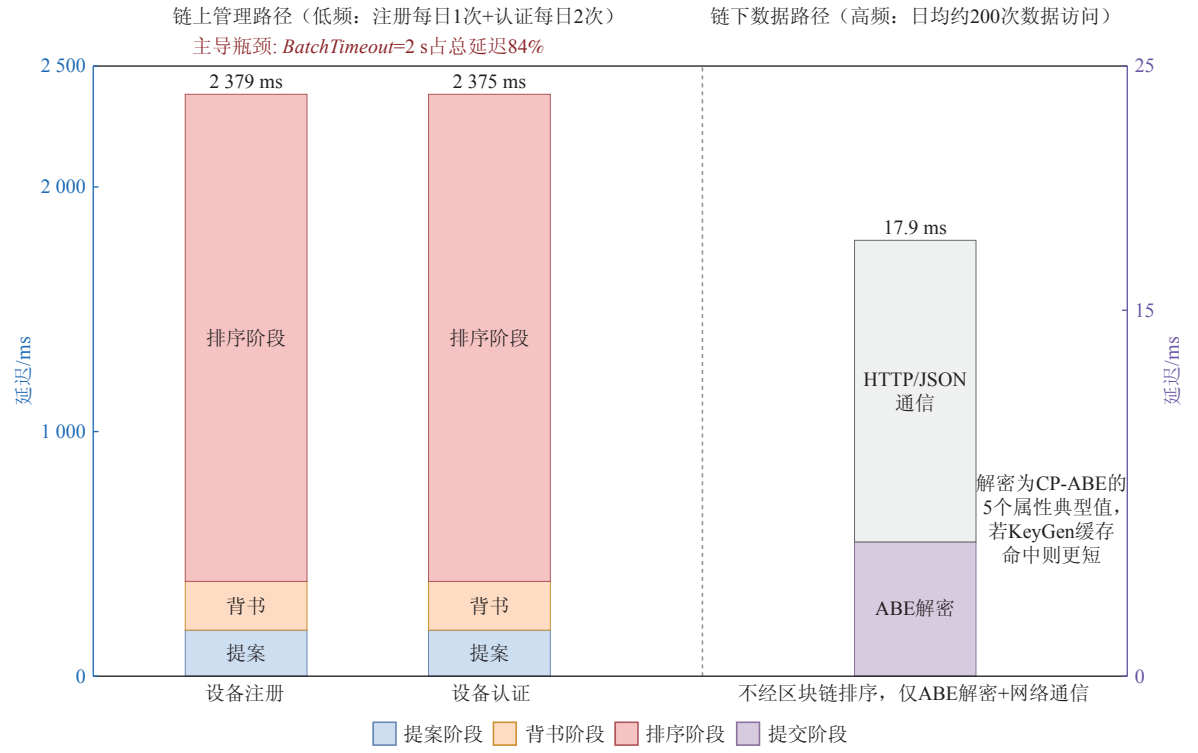
平均延迟分别为 2 379.3 ms 和 2 375.2 ms。2 项实验均独立运行 10 次，标准差分别为 19.5 ms 和 18.6 ms，说明链上管理操作的延迟波动较小。进一步分解可见，Fabric 排序阶段约占 2 000 ms，主要由实验配置中的 Fabric 排序服务的区块打包超时参数 *BatchTimeout* 为 2 s 时决定，是端到端延迟的主导瓶颈；非排序阶段包括交易提案、背书和提交，合计为 375~380 ms。若将 *BatchTimeout* 从 2 s 调整为 500 ms，在其他开销近似不变的情况下，注册和认证延迟理论上可降至 875~880 ms。

与链上管理操作不同，纯 ABE 数据访问路径不经过区块链共识，由雾节点本地完成。实验结果显示，纯 ABE 数据路径延迟约为 17.9 ms，其中 ABE 解密耗时约为 5.5 ms，HTTP/JSON 处理与网络传输开销约为 12.4 ms。在 5 个属性条件下，该路径能够保持毫秒级响应，表明高频数据访问的性能主要由 ABE 运算和雾侧通信开销决定，而非区块链共识延迟决定。

进一步以每日注册 1 次、认证 2 次、数据访问 200 次估算，链上管理操作累计约 7.1 s，数据访问路径累计约 3.6 s。可以看出，虽然单次链上状态操作延迟为秒级，但其发生频率较低；高频数据访问路径保持毫秒级，不受 Fabric 共识过程直接影响。这一延迟结构验证了本文“链上低频管理、链下高频数据访问”的架构设计：链上负责注册、认证、撤销和策略状态等可信管理操作，链下雾节点负责实时授权和 ABE 数据访问。端到端延迟分解如图 11 所示。

5.4 通信与链上存储开销

根据原型接口消息字段统计，设备注册、认证、数据请求和撤销请求均为百字节级；跨域凭证由于包含 ECDSA 签名、源域字段、目标域字段和属性字段，大小约为 490B。混合 ABE 密文大小随属性数量线性增长，主要增加来自属性相关密文分量。对于 ZigBee、BLE 或 LoRa 等低速链路，可通过属性编码、凭证压缩和策略摘要等方式进一步降低通信负载。



注：10 次独立运行实测均值，标准差分别为±19.5 ms 和±18.6 ms

Fig. 11 End-to-end latency decomposition

图 11 端到端延迟分解

链上存储方面,本文遵循“只存状态,不存数据”的原则。近年来,区块链与属性访问控制、ABE 的结合被用于提升物联网数据访问过程中的透明性、可追溯性和去中心化管理能力[25]。但若直接将密文或访问数据写入链上,容易造成账本膨胀和隐私扩散。因此,本文仅在 Fabric 链上保存设备身份哈希、策略版本、撤销状态和域间信任关系,不保存明文、密文和 PUF 原始响应。该设计既避免了直接上链密文带来的存储增长,也降低了敏感数据在多个共识节点间扩散的风险。

综合来看,本文方案将终端侧开销限制为 PUF 响应生成和 SHA-256 哈希,将 ABE 密钥生成、加解密和跨域凭证处理迁移至雾节点,并将 Fabric 链上操作限制在注册、撤销、策略更新和域间信任维护等低频状态变更中。对于属性频繁变化或策略需要隐藏的场景,已有研究进一步讨论了动态属性更新和策略隐藏机制[31]。本文当前主要维护策略版本和撤销状态,尚未展开复杂动态属性更新,后续可在现有链上状态模型基础上进一步扩展。该设计使高频数据访问路径保持在毫秒级,同时保留链上状态审计和跨域一致性能力。

6 结论与展望

本文提出一种面向资源受限物联网终端的轻量级访问控制机制。该机制通过雾节点承载 ABE 重运算、Fabric 维护身份与策略可信状态、PUF 提供设备物理身份根,在不增加终端复杂公钥运算负担的前提下,实现了细粒度授权、跨域认证和可审计撤销。安全分析表明,认证与会话过程可由 BAN 逻辑推导,CP/KP-ABE 组件在 DBDH 假设下满足 IND-sCPA 安全,混合 ABE 框架可由独立密钥空间和混合论证推广为整体安全。实验结果表明,Fabric 交易延迟主要出现在注册、认证和撤销等低频管理操作中,高频数据访问由雾节点完成,核心 ABE 计算保持在毫秒级,适合需要细粒度授权和跨域审计的资源受限物联网场景。

当前方案仍存在 3 方面局限。首先,Fabric 共识延迟对极低功耗、短唤醒窗口终端仍可能偏高,尤其在 LoRa 类设备中,链上认证或状态更新可能与短唤醒窗口发生冲突。其次,属性撤销尚未形成完整机制,若采用时间版本属性会引入周期性密钥刷新和重加密开销,若采用直接撤销则可能增加密文或密钥规模。最后,本文 PUF 部分仍以协议流程和软件模拟为主,尚未覆盖真实硅 PUF 在噪声、温漂、电压扰动和老化条件下的响应不稳定问题;同时,实验拓扑也尚未扩展到多雾节点负载均衡、故障迁移和大规模终端接入场景。

后续工作将从 3 个方向推进:一是补充属性撤销、动态属性更新、策略隐藏和动态跨域信任评估机制,提升访问控制的动态适应能力[28,31];二是引入真实 PUF 测试、可信执行环境、远程证明和轻量级 PUF 认证机制,增强雾节点密钥保护和设备身份验证的工程可信性[32];三是结合 Fabric 新版本共识优化、区块链协议裁剪、批量状态更新和雾节点集群调度,降低链上状态变更延迟[33]。对于终端无法保留原始明文的外包计算场景,后续还可结合可审计外包属性加密机制扩展结果验证能力[34]。此外,可进一步使用 Tamarin-Prover 或 ProVerif 对跨域认证和撤销流程进行自动化形式化验证,以减少手工 BAN 逻辑推导可能遗漏的边界条件。

作者贡献声明:余韦提出了总体研究思路,设计了访问控制机制,进行了实验并撰写论文;许光全指导了方案设计与技术论证,修改了论文;刘如静构建了安全模型,进行了协议安全性分析;张津耀设计了性能评估方案,完成了实验数据分析;李春志参与了系统测试、实验结果核验和论文修改;白宏鹏参与了系统实现,整理了文献与图表并校订了论文。

参 考 文 献

[1] Zhang Yuqing, Zhou Wei, Peng Anni. A survey of Internet of things security[J]. Journal of Computer Research and Development, 2017, 54(10): 2130−2143 (in Chinese)
(张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017, 54(10): 2130−2143)

[2] Liu Qixu, Jin Ze, Chen Canhua, et al. A survey on access control security for Internet of things[J]. Journal of Computer Research and Development, 2022, 59(10): 2190−2211 (in Chinese)
(刘奇旭, 靳泽, 陈灿华, 等. 物联网访问控制安全性综述[J]. 计算机研究与发展, 2022, 59(10): 2190−2211)

[3] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: A new blockchain-based access control framework for the Internet of things[J]. Security and Communication Networks, 2016, 9(18): 5943−5964

[4] Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT[J]. IEEE Internet of Things Journal, 2018, 5(2): 1184−1195

[5] Feng D G, Chen C. Research on attribute-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 1−12

[6] Zhang Y, Kasahara S, Shen Y, et al. Smart contract-based access control for the Internet of things[J]. IEEE Internet of Things Journal, 2018, 6(2): 1594−1605

[7] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89−98

[8] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//Proc of the 28th IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2007: 321−334

[9] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38−47

[10] Hu V C, Ferraiolo D, Kuhn R, et al. Guide to attribute based access control (ABAC) definition and considerations (draft)[J]. NIST Special Publication, 2013, 800(162): 1−54

[11] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts[C]//Proc of the 20th USENIX Security Symp. Berkeley, CA: USENIX Association, 2011: 34

[12] Yu J, Liu S, Wang S, et al. LH-ABSC: A lightweight hybrid attribute-based signcryption scheme for cloud-fog-assisted IoT[J]. IEEE Internet of Things Journal, 2020, 7(9): 7949−7966

[13] Xu Q, Tan C, Fan Z, et al. Secure data access control for fog computing based on multi-authority attribute-based signcryption with computation outsourcing and attribute revocation[J]. Sensors, 2018, 18(5): 1609

[14] Rührmair U, Sölter J, Sehnke F. On the foundations of physical unclonable functions[J]. Cryptology ePrint Archive, 2009: 2009/277

[15] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation[C]//Proc of the 44th Annual Design Automation Conf. New York: ACM, 2007: 9−14

[16] Dodis Y, Ostrovsky R, Reyzin L, et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[J]. SIAM Journal on Computing, 2008, 38(1): 97−139

[17] Bonomi F, Milito R, Zhu J, et al. Fog computing and its role in the Internet of things[C]//Proc of the 1st Edition of the MCC Workshop on Mobile Cloud Computing. New York: ACM, 2012: 13−16

[18] Alrawais A, Alhothaily A, Hu C, et al. Fog computing for the Internet of things: Security and privacy issues[J]. IEEE Internet Computing, 2017, 21(2): 34−42

[19] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger Fabric: A distributed operating system for permissioned blockchains[C]//Proc of the 13th EuroSys Conf. New York: ACM, 2018: 30:1−30:15

[20] Xiong L, Li Q, Tang L L, et al. Blockchain-based conditional privacy-preserving authentication scheme using PUF for vehicular ad hoc networks[J]. Future Generation Computer Systems, 2025, 163: 107530

[21] Harbi Y, Aliouat Z, Harous S, et al. Lightweight blockchain-based remote user authentication for fog-enabled IoT deployment[J]. Computer Communications, 2024, 221: 90−105

[22] Gassend B, Clarke D, van Dijk M, et al. Silicon physical random functions[C]//Proc of the 9th ACM Conf on Computer and Communications Security. New York: ACM, 2002: 148−160

[23] Burrows M, Abadi M, Needham R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18−36

[24] Pancari S, Rashid A, Zheng J, et al. A systematic comparison between the ethereum and hyperledger fabric blockchain platforms for attribute-based access control in smart home IoT environments[J]. Sensors, 2023, 23(16): 7046

[25] Yang Z, Chen X, He Y, et al. An attribute-based access control scheme using blockchain technology for IoT data protection[J]. High-Confidence Computing, 2024, 4(3): 100199

[26] Nie S, Ren J, Wu R, et al. Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of things in a 6G environment[J]. Sensors, 2025, 25(2): 550

[27] Zhang Y, Deng R H, Xu S, et al. Attribute-based encryption for cloud computing access control: A survey[J]. ACM Computing Surveys, 2020, 53(4): 1−41

[28] Penuelas-Angulo A, Feregrino-Uribe C, Morales-Sandoval M. Revocation in attribute-based encryption for fog-enabled internet of things: A systematic survey[J]. Internet of Things, 2023, 23: 100827

[29] Cheng H, Lo S L, Lu J. A blockchain-enabled decentralized access control scheme using multi-authority attribute-based encryption for edge-assisted internet of things[J]. Internet of Things, 2024, 26: 101220

[30] Song C, Chen L, Wu X, et al. A secure data sharing model utilizing attribute-based signcryption in blockchain technology[J]. Sensors, 2024, 25(1): 160

[31] Xu Z, Zhou W, Han H, et al. A secure and scalable IoT access control framework with dynamic attribute updates and policy hiding[J]. Scientific Reports, 2025, 15(1): 11913

[32] Roy S, Das D, Sen B. Secure and lightweight authentication protocolusing puf for the IoT-based wireless sensor network[J]. ACM Journal on Emerging Technologies in Computing Systems, 2023, 20(1): 1−17

[33] Huang Y, Yen I L, Bastani F. Pruning blockchain protocols for efficient access control in IoT systems[C]//Proc of the 30th IEEE Int Conf on Parallel and Distributed Systems. Piscataway, NJ: IEEE, 2024: 617−624

[34] Cai D, Chen B, Zhang L, et al. BA-ORABE: Blockchain-based auditable registered attribute-based encryption with reliable outsourced decryption[EB/OL]. 2024[2026-06-03]. https://doi.org/10.48550/arXiv.2412.08957



Yu Wei, born in 1989. PhD, associate professor. His main research interests include dynamic complex network analysis, anomaly detection, large-scale data mining, and machine learning.

余　韦, 1989 年生。博士，副教授。主要研究方向为动态复杂网络分析、异常检测、大规模数据挖掘、机器学习。



Xu Guangquan, born in 1979. PhD, professor. His main research interests include network and information security, mobile security, IoT security, AI security, and trust management.

许光全, 1979 年生。博士，教授。主要研究方向为网络信息安全、移动安全、物联网安全、人工智能安全、信任管理。



Liu Rujing, born in 2006. Undergraduate. Her main research interest includes big data security modeling.

刘如静, 2006 年生。本科生。主要研究方向为大数据安全建模。



Zhang Jinyao, born in 2002. Undergraduate. His main research interest includes complex network analysis.

张津耀, 2002 年生。本科生。主要研究方向为复杂网络分析。



Li Chunzhi, born in 2001. Bachelor. His main research interests include IoT security, blockchain technology, fog computing, and access control.

李春志, 2001 年生。学士。主要研究方向为物联网安全、区块链技术、雾计算、访问控制。



Bai Hongpeng, born in 1993. PhD candidate. His main research interests include malware detection and Internet of things security.

白宏鹏, 1993 年生。博士研究生。主要研究方向为恶意软件检测和物联网安全。