物联网环境下基于区块链技术的私有数据访问控制模型

蒋伟进[1,2,3]，罗田甜[2,4]，杨莹[1,3]，李恩[1,3]，周文颖[1,3]

（1. 数据智能与智慧社会国家重点实验室（培育）基地，湖南 长沙 410205；2. 新零售虚拟现实技术湖南省重点实验室，湖南 长沙 410205；
3. 湖南工商大学计算机学院，湖南 长沙 410205；4.湖南工商大学前沿交叉学院，湖南 长沙 410205）

摘 要：基于传统“中心化”的访问控制技术已经无法保证当前物联网环境中私有数据访问控制的安全性问题。以基于属性的访问控制（ABAC, attribute-based access control）模型为基础，提出了一种基于区块链的物联网访问控制框架和私有数据访问控制模型。首先，对访问控制的基本框架与流程进行了详细的阐述与分析，并提出了可审计的访问控制模型，通过存储在区块链网络中的请求、响应和访问记录，对私有数据的访问控制策略进行系统管理；接着，提出了一种基于区块链技术的可审计访问控制系统，可以在物联网中提供分布式、细粒度和动态性的访问控制管理，实现了对数据的有效管理和可审计访问，并采用基于智能合约的访问控制方法实现对物联网资源全程透明、可追溯、自动化的访问控制。最后，通过仿真实验和性能测试验证了该访问控制模型和系统的有效性和安全性。

关键词：区块链；物联网；访问控制；智能合约；数据安全

中图分类号：TP309

文献标志码：A

doi: 10.11959/j.issn.2096−3750.2022.00304

Private data access control model based on block chain technology in the internet of things environment

JIANG Weijin[1,2,3], LUO Tiantian[2,4], YANG Ying[1,3], LI En[1,3], ZHOU Wenying[1,3]

1. State Key Laboratory of Data Intelligence and Smart Society Laboratory(Cultivating) Base, Changsha 410205, China
2. Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Changsha 410205, China
3. School of Computer Science, Hunan University of Technology and Business, Changsha 410205, China
4. School of Advanced Interdisciplinary Studies, Hunan University of Technology and Business, Changsha 410205, China

Abstract: The traditional “centralized” access control technology can no longer guarantee the security of private data access control in the current internet of things environment. Based on the ABAC (attribute-based access control) model, a block-chain based access control framework for the internet of things and a private data access control model were proposed. Firstly, the basic framework and process of access control were described and analyzed in detail, and an auditable access control model was proposed to systematically manage the access control policies of private data through the requests, responses and access records stored in the blockchain network. Then, an auditable access control system based on blockchain technology was proposed, which can provide distributed, fine-grained and dynamic access control management in the internet of things, realize the effective management and auditable access to data, and adopt the access control method based on smart contract to realize the transparent, traceable and automatic access control over the internet of things resources. Finally, simulation experiments and performance tests verify the effectiveness and security of the access control model and system.

Key words: blockchain, IoT, access control, smart contract, data security

---

收稿日期：2022−04−24；**修回日期：**2022−10−17

通信作者：罗田甜，luotiantian1998@126.com

基金项目：国家自然科学基金资助项目（No.61772196）；湖南省自然科学基金资助项目（No.2020JJ4249）；湖南省研究生科研创新项目（No.CX20221139）；湖南省教育厅科学研究重点项目（No.21A0374）

Foundation Items: The National Natural Science Foundation of China (No.61772196), The National Natural Science Foundation of Hunan Province (No.2020JJ4249), The Hunan Provincial Innovation Foundation for Postgraduate (No.CX20221139), The Key Scientific Research Project of Hunan Provincial Department of Education (No.21A0374)

0 引言

随着物联网（IoT, internet of things）技术的飞速发展，越来越多的物联网设备被广泛应用于工/农业、社会治理、智能医疗、智能交通等领域[1]，极大地提高了城市居民生活质量、服务效率和城市竞争力。物联网设备可以通过无线或有线网络连接，形成一个分布式网络[2]，不断地与外部环境进行交互，并产生许多不同类型的数据源，如视频、音频和文本等。此外，物联网数据资源和信息还可以通过分布式网络进行高效共享。在这种情况下，保证物联网设备生成的数据安全和隐私是一个巨大的挑战。例如，智能港口使用物联网设备进行数据采集和交换，降低了记录数据的错误率，提高港口物流效率[3]；然而，它也面临着与物联网设备相同的问题，数据隐私容易被泄露。目前，许多正在建设中的智能港口仍处于信息处理阶段，因此，数据的安全性需要进一步加强。

大多数的传统物联网设备基于云服务器提供的第三方服务存储私有敏感数据，而云服务器的单点故障问题会给数据安全造成巨大的风险。因此，私有数据的隐私安全得不到保障。访问控制技术[4]作为保证物联网私有数据安全的重要技术之一，能够确保数据只能被具有相应权限的特定用户访问，也能使数据请求者在合理的访问控制范围内访问私有数据。但传统的访问控制模型主要应用于封闭环境中的粗粒度控制，并不适用于开放的物联网环境，目前，物联网平台需要细粒度的访问方法来存储和处理数据。Hu 等[5]提出一种基于属性的访问控制（ABAC, attribute-based access control）模型，作为一种细粒度的动态访问管理方法，可以针对主题的任意属性、对象的选定属性以及当前实现策略的环境条件，使用 ABAC 模型控制用户对物联网中私有数据的操作权限。然而，如果 ABAC 被非法创建，私人数据就会受到攻击。且 ABAC 需要存储在一个持久的数据库中，以确保数据的安全性和有效性。区块链技术可以完全满足这一需求，区块链可以解决具有匿名性、分散化等特征的物联网安全问题，以及应对集中化、不可信的第三方信任问题和单点故障的挑战；区块链[6]分布式的存储结构确保了区块链上的数据不易丢失，并通过由每个块的散列组成的单链，保证了数据的完整性和难以篡改性。但常见的公共区块链平台[7]不适合集成到物联网系统中。以太坊主网上存在着大量的账户，在事务同步过程中，大量琐碎的信息会占用带宽，增加物联网设备的功耗，给存储带来巨大的压力。

为了克服这些缺点，本文基于智能合约技术和 ABAC 模型，提出了一种物联网环境下的私有数据访问控制模型和可审计的访问控制系统。该模型可以通过分布式网络和共识认证机制跟踪私有数据的请求记录、响应记录和访问记录；同时，该系统实现了私有数据访问控制策略的动态管理，解决了物联网中私有数据的访问控制问题。本文的主要贡献如下。

1) 提出了一种基于区块链技术的物联网访问控制框架，实现了物联网访问控制策略的分布式管理，有效地提高了访问控制系统的鲁棒性和可信性。

2) 根据物联网的实际应用场景设计了一种私有数据资源存储模型。该模型将物联网数据划分为私有数据和公共数据，并使用不同的方式存储它们，以确保由物联网设备生成的私有数据的安全性。同时，提出了一种可审计的访问控制策略模型，实现了对私有数据、访问控制策略和访问记录的联合管理，确保了物联网中私有数据访问的可控性。基于审计结果，该模型可以实时控制未经授权的访问。

3) 在可审计访问控制模型的基础上，提出了一种部署 4 个智能合约的访问控制系统。第 1 个智能合约实现了访问控制策略的管理，第 2 个合约实现了数据所有者与数据请求者之间的合法请求和响应，第 3 个合约实现了物联网中私有数据的管理，第 4 个合约实现了访问记录的管理。这些智能合约都是可复制的和可转移的。该系统实现了访问权限的动态管理，支持用户高效访问。

1 相关技术及研究

1.1 基于属性的访问控制（ABAC）模型

访问控制[8]作为保护数据资源的一种重要手段，在各种系统和环境中得到广泛应用。传统的访问控制技术，包括自主访问控制（DAC, discretionary access control）技术、强制访问控制（MAC, mandatory access control）技术和基于角色的访问控制（RBAC, role-based access control）技术，它们均在不同的应用场景中发挥着相应的作用，传统访问控制技术见表 1。

表 1　　**传统访问控制技术**

对比项	作用	优点	缺点
DAC[9]	主体对客体的访问权限能够进行自主管理，主体决定是否将客体的全部或部分访问权限授予给其他主体	灵活性较高，也具有一定的可扩展性	安全性较差，开销大，静态分配权限
MAC[10]	主体和客体都被系统分配一个固定的安全属性，安全属性决定一个主体是否可以访问某个客体	信息的机密性较高，安全性较高	灵活性比较差，静态分配权限
RBAC[11]	权限和角色相关联，通过为主体分配适当的角色，其能够获得相应角色的权限	明确责任和授权，安全性和灵活性较高	粗粒度控制，静态分配权限

传统的访问控制技术存在单点故障、难以扩展、可靠性低、吞吐量低等缺点。实际上，物联网设备可能属于不同的组织或用户，并且具有移动性和有限的性能，这使得集中式访问控制难以满足物联网环境中的访问控制要求。且新型计算模式的快速变化，也给访问控制技术带来了巨大的挑战。

1) 海量性

在新型计算模式中，设备终端和用户数量呈现出海量性的特点。在物联网中，终端节点的数量会随着物联网的发展变得十分庞大，而传统的访问控制技术一般采用静态的方式管理用户和访问权限，但随着数据的快速增长，往往需要构建和维护庞大的访问控制列表，这极大地增加了系统的成本开销，也在一定程度上降低了访问控制的效率。

2) 动态性

在新型计算模式中，节点、用户和数据均呈现出动态性的特点。在物联网中，终端节点以及用户会不断地移动，数据对象也在实时变化。传统的静态访问控制技术无法在动态环境下提前设置用户与权限的对应关系。

3）分布式

在新型计算模式中，不同区域间的资源共享和信息互访需求增多，但不同的区域是相互独立的，并拥有自己的访问控制策略。而传统访问控制技术更多应用在封闭环境下，面对新型计算环境下分布式特点，无法支持各域统一访问控制策略标准。

由于以上特点，传统的访问控制技术难以满足新型计算环境对访问控制的需求。因此，研究人员提出了基于属性的访问控制模型。

基于属性的访问控制[12]模型是一种考虑主体、对象、权限和环境属性，通过使用用户、系统和环境条件的属性评估一组规则、策略和关系来管理访问权限的访问控制技术。属性可以是用户的工作开始日期、用户的位置、用户的角色或所有属性。主体和对象的属性是单独定义的，因此 ABAC 模型可以有效地分离策略管理和访问控制。ABAC 模型还具备可伸缩性，能够根据实际情况更改策略，例如添加或减少策略的属性。此外，ABAC 模型可以在访问控制策略中引入上下文信息以及主题和对象的属性，并在策略中添加更多的主题属性、对象属性和上下文信息，能够大大提高 ABAC 模型的动态性和粒度。基于以上原因，本文认为 ABAC 模型相比其他访问控制模型能更好地应用在物联网访问控制实际场景中，且能够为物联网系统实现细粒度的访问控制，灵活性和可扩展性较高。

1.2　相关工作

目前，随着区块链技术的不断发展，已经从区块链 1.0 比特币时代发展到了如今的区块链 3.0 时代[13]。区块链作为一种高度透明的访问控制技术，能够提供端到端分散的安全，减少了人为错误的风险；它还可以抵御黑客攻击，并允许以分布式的方式记录、存储和更新数据，这对于访问控制系统非常重要。随着区块链技术热度的提升，越来越多的研究将区块链技术应用于数据共享和访问控制，为解决物联网中单点故障和不可信的第三方问题提供了技术支持。例如，Zyskind 等[14]通过区块链网络中的访问控制策略存储私有数据，以解决用户无法授权访问私有数据的问题；Košt 等[15]提出了一种改进的区块链结构。在企业网络中，使用私有链分布式管理物联网的设备配置文件，它将设备配置文件存储在区块链上，并通过智能合约监控操作。Ding 等[16]针对传统的访问控制技术不适用于物联网复杂和大规模的网络结构问题，提出一种基于属性的物联网系统访问控制方案，使用区块链技术记录属性的分布，以避免单点故障和数据篡改，其中的区块链系统同样由第三方权威机构维护。

由以上可知，区块链的不可控、开放、透明的特性，使其与物联网的访问控制完美结合。但正因为如此，人们无法将私人信息写入区块链，这极大地限制了它的可扩展性。因此，许多人还提出了使用区块链进行匿名访问或其他方式来保护私有信息。如 Zhou 等[17]设计的分散外包计算方案，服务器可以根据数据所有者的请求计算来自数据所有者的加密数据，检测不诚实的服务器，同时保护数据隐私，降低敏感信息泄露的风险；Henry 等[18]通过研究表明匿名通信系统无法解决通信隐私问题，使得区块链的隐私安全引起了新的关注。Cai 等[19]提出了一种新的智能网络物理系统中的数据上传机制，该机制同时考虑了节能和隐私保护，通过隐藏参与者的异常行为保护隐私，同时引入可接受数量的额外内容来实现一种高效的数据上传方案。

目前，也有一部分研究提出使用智能合约技术来解决物联网的访问控制问题。智能合约和区块链是两种独立的技术。智能合约是指一系列计算机代码和协议，在满足指定条件时可以自动执行协议，合约是通过使用不同编程语言中的特定条件语句进行编码的。当智能合约与区块链技术相结合时，它不仅避免了对规则的进行恶意篡改，而且具有开销成本低和运行效率高等方面的显著优势；同时，智能合约的执行和结果记录被生成并存储在区块链上，保证了整个过程中所有数据和结果的真实性。因此，可以根据不同领域的不同需求，开发相应的智能合约来实现特定的功能。

许多学者对于智能合约在物联网访问控制上的应用开展了很多研究。Kuzmin 等[20]提出了一种利用区块链提供的智能合约设计访问控制服务的新方法，并将访问控制策略编码为区块链上的可执行智能合约。Zhang 等[21]提出了一种基于智能合约的分布式可信访问控制框架，其中访问控制合约提供了一种基于行为判断的访问控制方法，注册合约负责注册访问控制方法、不当行为判断方法和创新合约信息的管理。Pal 等[22]基于区块链技术提出了一种无身份、异步、分散的委托模型，并通过使用私有区块链的概念验证测试平台演示了所提模型的可行性。Song 等[23]提出基于属性的访问控制模型来保护物联网设备上的资源和信息。而 Saini 等[24]建立基于智能合约的访问控制框架，以确保不同实体之间的数据共享。Yang 等[25]提出了一种边缘区块链授权的安全数据访问控制方案，该方案采用阈值秘密共享方案建立分布式权限，并在超账本结构平台上证明了该方案的安全性和有效性。Fotiou 等[26]提出了使用智能合约的令牌进行访问控制，以建立一个广泛的基于事件的物联网控制结构。智能合约中包含了设备操作和功能之间的映射。客户端调用任何函数时，智能合约都会生成一个相对的区块链事件，波动的货币成本和交易时延是这种方法所面临的问题，它可以通过客户端和物联网网关之间的直接交互进行改进。

综上所述，区块链技术与智能合约技术结合可以解决传统访问控制方案的局限性问题，实现可信的分布式访问控制。然而，频繁的用户访问和海量的数据处理给物联网的访问控制带来了新的挑战，即低吞吐量和高交易费用。当在具有大量用户和高度频繁的访问请求的大规模环境中强制执行访问控制时，这两个问题可能会给管理员和用户带来巨大的负担。

2 访问控制模型设计

物联网环境下基于区块链技术的私有数据访问控制模型是一种可靠、安全的私有数据保护方案。系统设计和模型架构的细节在后面的小节中具体介绍，方案中符号及含义见表 2。

表 2 方案中符号及含义

符号	含义
$PK_{owner/user}$	数据所有者或数据请求者的公钥
$SK_{owner/user}$	数据所有者或数据请求者的私钥
$Data_{Pri}$	隐私数据数据包
$Data_{Pub}$	公共数据数据包
$Data_{Ipfs}$	公共数据的 IPFS 地址
$Key_{resource}$	与数据资源对应的键值
Key_{policy}	与策略对应的键值
$Key_{request}$	与请求记录对应的键值
$Key_{response}$	与响应记录对应的键值
Sign( )	ECDSA 的签名算法
Verify( )	ECDSA 的验证算法
Hash( )	计算哈希值

2.1 基于区块链技术的 ABAC 框架及工作流程

本文提出的基于区块链技术的 ABAC 框架如图 1 所示，框架在 ABAC 模型的基础上进行了改进和完善，将区块链技术与访问控制模型进行结

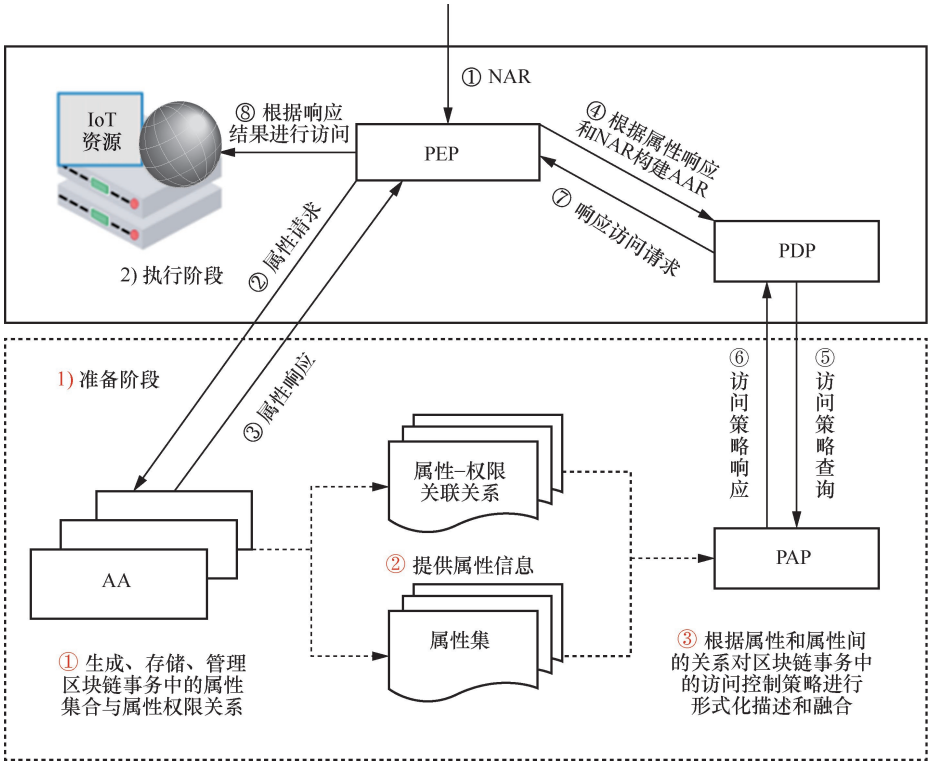


图 1　基于区块链技术的 ABAC 框架

合，并应用在物联网环境中。框架主要包括策略执行点（PEP, policy enforcement point）、策略管理点（PAP, policy administration point）、属性权威（AA, attribute authority）、策略决策点（PDP, policy decision point）这 4 个核心部分。其中，AA、PAP、PDP 是以智能合约的方式来实现的，能够确保区块链中访问控制策略的准确执行，用户需要使用 PEP 作为访问控制客户端来与区块链进行访问控制的交互。

在本框架中，基于区块链技术的访问控制工作流程是对标准 ABAC 模型工作流程的扩展和补充。其整个访问控制工作流程可分为准备阶段和执行阶段（如图 1 所示）。准备阶段主要是根据属性和属性权限关系对区块链事务中的访问控制策略进行形式化的描述和综合管理，而执行阶段是先对访问请求进行判断，然后响应与执行请求，并对区块链中的访问控制策略进行更新。

1) 准备阶段

属性权威（AA）负责生成、储存区块链事务中的属性集合和属性权限关系，并对区块链事务中的属性信息进行整合，包括主体属性、客体属性、权限属性和环境属性集合；然后策略发布方会在区块链中发布访问控制策略，PAP 会结合属性信息描述、收集、整合区块链事务中访问控制策略，PDP 则对该访问请求进行判断。

2) 执行阶段

当 PEP 收到用户向其发送的对某一资源执行某项操作的请求时，PEP 先对这项要求进行分析，并得到原始访问请求中主体、客体和操作语义的信息，然后根据从 AA 得到的属性信息生成基于属性的访问请求（AAR, attribute access request），并将 AAR 发送到 PDP；PDP 向 PAP 查询并请求与物联网资源相关的访问控制策略集，进行访问控制判断，最后将判断结果响应发送回 PEP。

PEP 根据响应结果对物联网资源进行授权的访问操作，由于访问控制策略存储在区块链中，策略信息对任何人都是可验证、可追溯且难以篡改的，物联网资源的访问控制摆脱了传统集中式访问控制管理可能存在的单点故障和访问控制判决透明度的问题，实现了访问控制策略的分布式管理，有效地提高了系统的鲁棒性和可信性。同时，利用智能合约实现访问控制策略的判决过程，无须第三方机构参与，增加了可信度，十分符合物联网资源的访问控制需求。

2.2　私有数据资源存储模型

本文提出的私有数据资源存储模型主要将

物联网数据分为公共数据和私有数据。公共数据是指毫无价值的模板数据，不涉及私密信息和敏感信息，可以将公有数据存储在星际文件系统（IPFS, inter planetary file system）中，IPFS 技术能够使用哈希加密为大量数据生成不可变的永久 IPFS 地址。而私人数据包含有关用户的隐私和机密，还有一些个人敏感信息，为了确保数据的安全性和完整性，可以在区块链网络中存储私有数据，能够保证数据不被轻易篡改，提高了数据的可靠性。

数据所有者通过建立访问控制策略来保护私有数据并且控制访问权限，同时也通过审计私有数据的访问记录、请求记录和响应记录来管理此类访问控制策略。用户不能直接访问私有数据，除非访问控制策略对它们进行身份验证，并且通过了验证。因此，进一步提高了私有数据的可控性和安全性。用户与私有数据之间的关系如图 2 所示。

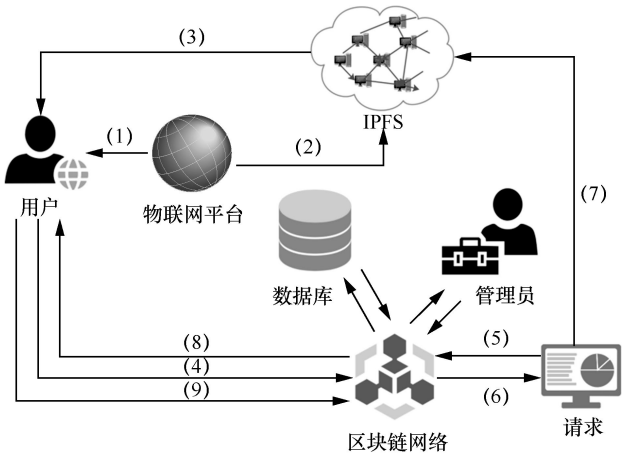


图 2　用户和私有数据之间的关系

工作流程如下。

步骤 1　物联网设备的所有者从物联网平台获取私有数据的信息。

步骤 2　物联网平台上传公共数据到 IPFS。

步骤 3　IPFS 返回公共数据的 IPFS 地址。

步骤 4　数据所有者把私有数据和IPFS地址存储在区块链网络中。

步骤 5　数据请求者通过区块链网络请求访问私有数据。

步骤 6　区块链网络经过身份验证后，立即返回私有数据和请求者所需的 IPFS 地址。

步骤 7　数据请求者通过 IPFS 地址获取公共数据。

步骤 8　数据所有者从区块链网络中获得请求记录、响应记录和私有数据的访问记录。

步骤 9　数据所有者根据访问记录、请求记录和响应记录管理与私有数据相关的访问策略。

2.3　可审计的访问控制模型

本文将基于属性的访问控制方法与区块链上的物联网数据实际应用场景结合，提出了一种可审计的访问控制模型，可以对物联网上的私有数据进行访问控制管理。

1) 模型组件

本文所述模型由以下 3 个部分组成。

- 数据存储部分{resource}

R={resourceId, data，Ipfs}，R 表示物联网私有数据集，resourceId 表示资源的唯一标识，data 表示物联网生成的私有数据，Ipfs 表示公共数据上传到星际文件系统后返回的 IPFS 地址。

- 策略部分{policy}

P={AS，AO，AP，AE}，AS={userId, role, PK}，AO={dataId, signer, sign_data, resourceKey, Ipfs}，AP={auth_sign，p_Ipfs，p_data}，AE={createTime, endTime, address, sign_PKuser}。P 表示基于属性的访问控制策略，用户必须通过该策略才能访问私有数据。AS 表示主体的属性，即系统用户；用户是区块链网络中的一个真人所拥有的一个虚拟角色。它们具有以下属性：userId 表示用户的 ID，role 可分为数据所有者和数据请求者的用户角色，PK 则表示与该策略关联的用户的公钥。AO 表示一个对象的属性，主要表示私有数据，并具有以下属性：dataId 表示私有数据的 ID，signer 表示私有数据的数据所有者，sign_data 表示由 Hash( )计算的私有数据的哈希值，以确保私有数据的完整性，resourceKey 是区块链网络中私有数据对应的密钥值。最后，Ipfs 表示公共数据存储在星际文件系统中的地址。AP 是指权限属性，主要用于私有数据的访问权限和物联网中公共数据的 Ipfs 地址，具有以下属性：p_Ipfs 和 p_data 分别表示 IPFS 地址和私有数据的访问控制权限。访问控制权限的值 0 表示“拒绝”，1 表示“允许”。auth_sign 表示数据所有者在 p_Ipfs 和 p_data 上的签名，以确保权限没有被篡改。AE 是指数据请求者的环境的属性，当请求者发送请求时，确定请求实体是否符合访问控制策略

中定义的访问环境，它主要包括以下属性：createTime 表示制定策略的时间，endTime 表示策略超时的时间，address 表示用户提交请求的节点的 IP 地址，最后 sign_PKuser 是指数据所有者的签名，以确保策略没有被篡改。

- 记录部分{record}

RE={REQ, RES, HIS}，REQ={AS, AO}，RES={policyId, owner, requestId, status, endTime, timestamp}，HIS= {resourceId, requester, version}。RE 表示用于审计的记录，其中包括请求记录、响应记录和访问记录。REQ 表示数据请求者请求访问私有数据的请求记录，其中包含数据请求者的属性和私有数据的属性。RES 表示所有者对请求者的响应记录，其中包含以下属性，其中 policyId 表示策略存储在区块链网络中的键值，owner 是指数据所有者，requestId 是指数据请求者的 ID，以及 timestamp 表示数据所有者对数据请求的响应时间。最后，HIS 表示私有数据的访问记录。每当数据请求者成功请求名为 resourceId 的私有数据时，requester 表示数据请求者被自动记录在区块链网络中，并指定为 version 访问者。

2) 相互关系

本文提出的模型主要包括 3 组流程：用策略访问数据、生成访问记录以及用审计记录管理策略，可审计的私有数据访问控制模型如图 3 所示。

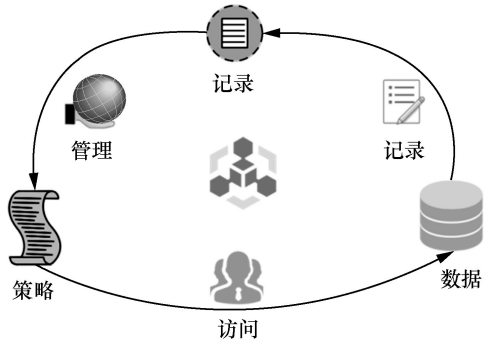


图 3　可审计的私有数据访问控制模型

- 策略–数据

在检索区块链网络的私有数据之前，智能合约必须将数据请求者的属性与访问控制策略中的相关属性进行身份验证。如果通过了身份验证，数据请求者将通过密钥资源从区块链网络获取私有数据，否则，将返回身份验证错误信息。相关策略示例见表 3。

表 3　　相关策略示例

Policy.json
{“AS”：{“$_{user}$ Id”:”“$_{user}$1”,”role”:”owner”,”PK”:”PK_{owner}”}, “AO”:{“dataId”:”R0001”,”signer”:”user1”,”sign_data”:Hash($Data_{Pub}$), “$_{resource}$Key”:”$Key_{resource}$”,”Ipfs”:”http://10.10.39.70”}, “AP”:{auth_sign”:Sign(SK_{owner},AS.$_{user}$Id+AP.p_data),”p_Ipfs”:1,”p_data”:1}, “AE”:{“createTime”:2178728，“endTime”:3178728, “address”:”10.10.39.70”,”sign_PK_{user}”:Sign(SK_{owner},AS.PK)}}

- 数据–记录

当请求者通过访问控制策略访问私有数据时，会根据数据请求者的属性生成访问记录，并将访问记录存储在区块链上。由于区块链的难以篡改性，存储在区块链上的访问记录可以有效地防止恶意更改。生成的访问记录见表 4。

表 4　　生成访问记录

resource.json
{”$_{resource}$Id”:”user1_R0001”,”data”:”$Data_{pri}$”,”Ipfs”:”$Data_{Ipfs}$”}

- 记录–策略

本阶段实现了访问控制模型的可审计性。当数据请求者发送访问私有数据的请求时，数据请求者的 ID 被记录在区块链网络上，形成一个访问记录。此外，数据请求者在请求存储在区块链网络中的私有数据的访问控制权限之前，需要向数据所有者发送访问请求，形成一条访问请求记录。当数据所有者传递数据请求者的访问请求之后，会制定相关的访问控制策略并存储在区块链网络中，然后将响应发送给数据请求者，并存储在区块链网络中，形成响应记录。数据所有者主要从区块链网络获取的私有数据访问记录、请求记录和响应记录来检查私有数据访问者的访问请求是否合法。

判断基础评估访问记录中的访问者是否具有相应的请求记录和响应记录，以及响应记录的 RES 状态是否为 1。如果不满足判断依据，则删除访问控制策略。此外，访问记录和私有数据之间的一对一关系有助于数据所有者进行审计，并将访问记录以键值对的形式存储在区块链网络中。

3　访问控制系统设计

3.1　系统架构

基于区块链的可审计访问控制系统结构如图 4 所示。

1) 物联网平台：它包括摄像机和传感器等设备，可以产生视频、音频和文本 3 种形式的数据。物联网数据集群为私有或公共数据，公共数据上传到 IPFS 上。

2) 用户：它被分为数据所有者和数据请求者。值得注意的是，数据所有者也可能是数据请求者。数据所有者可以上传区块链网络中的私人数据资源集和公共数据的 IPFS 地址，并管理关联的访问控制策略合集响应来自数据请求者的事务。数据请求者可以通过访问控制策略来访问私有数据。为了执行本系统中的审计功能，数据所有者只能对其私有数据进行访问控制策略审计。

3) 管理员：负责管理整个区块链网络。管理员仅具有区块链网络启动和智能合约安装权限，不能更改区块链网络的信息。

4) CA：区块链网络中的证书颁发机构，通过颁发证书来标识新节点。每个用户都需要一个 CA 证书，以便客户端可以通过区块链网络实现许多进程。

5) 区块链网络：整个系统的关键部分，主要包括数据存储和认证。其功能包括存储私有数据资源、访问控制策略、访问记录、请求记录和响应记录；用户访问私有数据资源的认证管理；审计访问控制策略和私有数据资源。

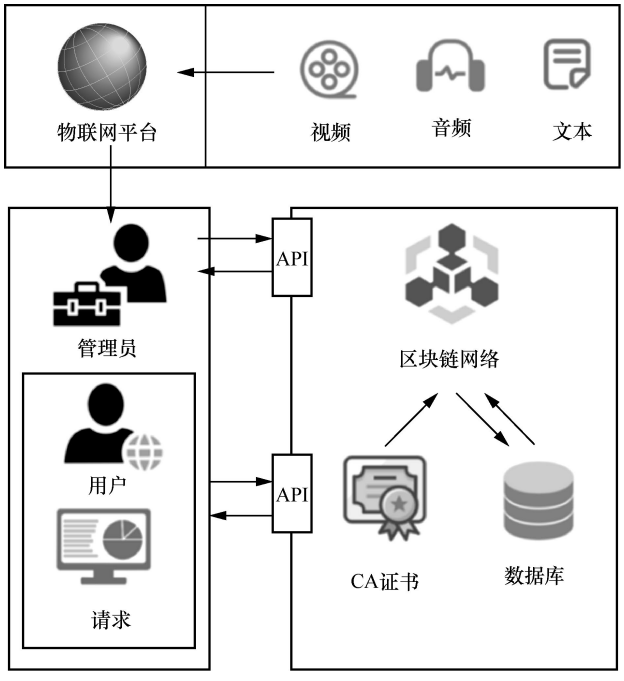


图 4　基于区块链的可审计访问控制系统结构

3.2　智能合约设计

本文在基于区块链的可审计访问控制系统的基础上，设计了 4 个智能合约：访问控制策略合约（ACPC，access control policy contract）、数据访问管理合约（DAMC，data access management contract）、私有数据控制合约（PDCC，private data control contract）和访问记录管理合约（ARMC，access record management contract）。接下来将分别介绍每一个智能合约的功能。

1) ACPC

它主要实现了访问控制策略的管理功能，由以下几种方法组成。

Auth( )：验证新创建策略的有效性。对于新创建的策略，需要验证“两个签名，两次”。这两个签名是指访问控制权限和整个访问控制策略的签名，它们都是由数据所有者签名的。两次是指策略创建时间与策略有效期之间的时间间隔。如果签名和时间满足要求，则新创建的策略验证成功，否则验证失败。

AddPolicy( )：当私有数据被上传到区块链网络或数据请求者向数据所有者发出请求时，数据所有者会调用此方法来制定相关的访问控制策略。新创建的策略需要由 Auth( )认证，如果符合规则，则此策略存储在区块链网络中，否则将返回错误消息。

UpdataPolicy( )：数据所有者调用此方法来更改数据请求者的访问控制权限，并更新访问控制策略。该方法还可以用于在数据请求者的访问超时的时候延长数据请求者的访问时间。

QueryPolicy( )：数据所有者可以根据私有数据和数据请求者的属性查询相关的访问控制策略。

DeletePolicy( )：当数据请求者有违规行为或非法访问私有数据时，数据所有者将使用此方法来删除数据请求者与私有数据资源之间的访问控制策略。

2) DAMC

它是数据请求者和数据所有者之间的请求交互，是数据所有者审计记录的重要组成部分，它包括以下 5 种方法。

RequestAccess( )：数据请求者需要封装用户属性和所请求的私有数据属性，以形成请求记录并将其上传到区块链网络，并请求数据所有者创建相关策略以获取访问控制权限。如果在验证后发现错误的用户属性，则该请求将被拒绝。

ResponseAccess( )：数据所有者将数据请求者的响应记录上传到区块链网络。当允许或拒绝数据请求者的请求时，将根据数据请求者的属性生成相

关的响应记录，从而将访问控制策略的密钥策略存储在区块链网络中，然后数据所有者将响应记录上传到区块链网络。

CheckAccess( )：数据请求者可以根据数据所有者返回的密钥策略检查对私有数据的访问控制权限。

GetRequest( )：获取访问控制策略的请求记录。

GetResponse( )：获取访问控制策略的响应记录。

3) PDCC

主要用于控制私有数据和公共数据的 IPFS 地址。数据所有者可以通过调用本合约上传私有数据、下载私有数据和公共数据的 IPFS 地址。本合约主要包括以下几种方法。

AddData( )：数据所有者通过上传私人数据和一个 IPFS 地址到区块链网络中来调用此方法。

GetData( )：数据所有者通过 Key_{policy} 获取私有数据。如算法 1 所示，当数据请求者根据密钥策略获取私有数据时，首先通过 QueryPolicy( )获取存储在区块链网络中的访问控制策略。然后，它评估数据请求者的访问控制权限，以验证私有数据的所有者是否制定了访问控制策略，如果满足访问控制权限的有效性和访问控制策略的合法性，则记录数据请求者的身份，通过 UpdateRecord( )生成访问记录，并返回私有数据 $Data_{Pri}$。

GetIPFS( )：数据请求者通过访问控制策略获得对公共数据 IPFS 地址的下载权限，区块链网络返回 $Data_{IPFS}$。

4) ARMC

主要用于记录数据请求者对私有数据的访问，获取私有数据的访问记录，便于审计流程的后续实现。此智能合约包括以下两种方法。

UpdateRecord( )：此方法不支持外部客户端的调用，也不为外部客户端调用提供接口。当数据请求者访问来自数据所有者的私有数据时，智能合约会自动调用此方法来记录数据请求者的访问权限。

GetRecord( )：数据所有者获取私有数据的访问记录。每个私有数据都有一个唯一的访问记录，每个访问者的访问记录都将进行更新。数据所有者获取的私有数据的访问记录按照访问时间进行排序，最新访问者排名第一。区块链的不变性可以保证访问记录的完整性。

算法 1　获取私有数据

PDCC.GetData( ): Get Private Data From Database According to the Policy.

Input: Key_{policy}

Output: $Data_{Pri}$ or error

p_data←0

p_Ipfs←0

policy←ACPC.QueryPolicy(Key_{policy})// 查询访问控制策略

<AS,AO,AE,AP>←policy

signer_PK←APIstub.GetState(AO.signer)// 获取 signer 的公钥

p_data←AP.p_data

p_Ipfs←AP.p_Ipfs

If time.Now( )>AE.endTimethen//判断访问时间是否超时

return,“Access Time Out”

end if

If !Verify(AS.userId+p_data + p_Ipfs , AP.auth_sign,//验证签名

signer_PK)then

return,“Sign Error”

end if

if !Verify(AS.PK,AE.signer_PKuser,signer_PK)//验证签名

then

return,“Sign Error”

end if

resource←APIstub.Getstate(AO.resourceKey)//获取访问资源

<data,Ipfs>←resource

ARMC.UpdateRecord(AS.user Id)

return data.

4　实验结果

本节介绍了实验程序和结果，包括评估讨论和仿真测试，以证明所提出的系统的功能和性能的有效性。

4.1　实验环境

单台机器的环境基于 1 台 PC 和 1 台笔记本计算机进行，前者用于构建区块链网络环境，后者用于模拟多个请求的客户端。略有不同的是，多链环境由 1 台 PC 和 3 台树莓派计算机组成，它们使用相同的硬件和软件来部署区块链网络。树莓派是一款 ARM 指令集计算机，例如安卓或 iOS 手机，以及 Mac 计算机。

4.2 系统和功能显示

实验系统由单机和多机环境的架构和部署体系以及区块链网络的节点组件组成。系统初始化和建立过程通过执行区块链网络生成脚本和启动脚本完成。本节描述了系统的功能显示和智能合约测试。从系统的工作流程出发，接下来是智能合约的功能显示和测试。

1) 私有数据存储测试：在 PDCC 中调用 Adddata( )，将私有数据上传到区块链网络，获得相应的密钥资源值，为数据所有者用户 1 和私有数据 R0001 制定访问控制策略，然后在 ACPC 中调用 AddPolicy( ) 上传到区块链网络，获得相应的密钥策略。

2) 请求进程测试：数据请求者用户 2 对数据所有者用户 1 的私有数据 R0001 进行访问。根据用户 2 和 R0001 的属性制定访问请求，在 DAMC 中调用 RequestAccess( )，返回请求的键值，上传到区块链网络。在数据所有者接收到来自数据请求者的请求之后，将调用 DAMC 中的 GetRequest( )，通过计算用户 1 和用户 2 的哈希值来查看数据请求者的请求记录。然后，通过调用 ACPC 中的 AddPolicy( )获得相应的关键策略，制定与数据请求者的私有数据 R0001 相关的访问控制策略并上传到区块链网络。通过调用 DAMC 中的 ResponseAccess( )，将生成相应的响应记录并上传到区块链，得到相应的密钥响应值。

3) 审计过程测试：数据所有者用户 1 通过在 ARMC 中调用 GetRecord( )来获取私有数据 R0001 的访问记录。根据私有数据的访问记录，审核近期数据请求者的访问记录是否合法。以用户 2 为例，通过在 DAMC 中调用 GetRequest( )和 GetResponse( )来获得相关的请求记录和响应记录。如果其中一个请求记录和响应记录显示为空或 RES 状态=0，数据所有者将调用 ACPC 中的 DeletePolicy( )来删除相关的访问控制策略。

4.3 实验分析

1) 安全性分析

在该访问控制系统中，可以保证物联网私有数据的隐私性和安全性。因为存储数据的区块能够通过任何节点获得，这会导致透明区块链网络中的数据泄漏。本文提出的私有数据资源存储模型将私有数据存储在区块链网络的数据块中，区块链网络的透明度不会威胁到它，因为本文提出的系统是基于 Fabric 平台的。Fabric 的数据存储模式主要是区块的事务和世界状态，区块的事务包含所有数据，世界状态会在区块链网络中存储数据的最新状态，以快速查询数据。本文通过解码检索块和世界状态事务中的数据，发现存储在其中的数据都是密文的形式，保密性较强。此外，智能合约中的私有数据只能通过对访问控制策略的身份验证来调用。因此，可以有效保证私有数据的安全性。

2) 兼容性分析

该系统具有良好的兼容性。从软件的角度来看，本文使用 Docker 技术来提高系统的可移植性，用户可以直接通过 Docker 映像创建系统运行所需的环境。在硬件方面，Fabric 平台只提供了 AMD 处理器架构的 Docker 映像。因此，本文在 ARM 处理器架构下进一步编译了 Docker 图像，以构建环境。在多机器实验中，本文在具有 AMD 和 ARM 处理器架构的设备上执行了所提出的系统，并展示了该系统的兼容性。因此，该系统可以更好地保证数据的完整性和安全性。

3) 可靠性分析

区块链网络采用 Kafka 共识算法。Kafka 是一个分布式消息传递系统，用于高并发性、高吞吐量的日志处理。如果有一个节点不能正常工作，则不会导致数据丢失，其他节点可以在引线处复制数据。此外，如果引线不能正常工作，其中一个节点将自动转换为引线。因此，如果其中一个节点崩溃，Kafka 集群中的领导节点将保持节点之间的状态同步，而不影响整个系统的操作。因此，该系统具有较好的可靠性，不会因节点的异常而崩溃。

4) 综合比较分析

为了展示该系统的创新性和实用性，所提模型与已有研究模型对比分析见表 5。这些属性显示在第一列中。隐私性是指数据是否受到保护。在文献[21]中，虽然数据受访问控制保护，但访问控制如果不加密的话，无法确保数据的安全性。在文献[25]中，通过秘密共享给数据提供隐私保护是不可靠的。可撤销性是指能否采取措施处理访问控制中的违法行为。文献[22]和文献[25]并没有做到这一点。文献[21]和文献[24]虽然具有可撤销性，但提出的模型将所有数据存储在区块链网络中，增加了区块链网络的负担。可审计性是指检查数据的访问记录和管理访问控制策略。文献[21]和文献[24]并没有实现检查数据的访问记录，而文献[24]使用的不当行为检测并

表 5　　**所提模型与已有研究模型对比分析**

属性	模型				
	文献[21]	文献[22]	文献[24]	文献[25]	所提模型
隐私性	×	√	√	×	√
可撤销性	√	×	√	×	√
云存储	×	×	√	√	√
兼容性	×	×	×	√	√
可审计性	×	√	×	×	√
区块链	公有	私有	私有	联盟	联盟

不是一种真正意义上的审计方法。物联网设备在文献[21]和文献[22]所采用的以太坊平台上没有客户端，它们只是物联网网关的代理。区块链表示的是所使用的实验测试平台的类型，本模型采用的是联盟链，联盟链由多个机构组成的联盟构建，账本的生成、共识、维护分别由联盟指定的成员参与完成。公有链的完全开放与去中心化特性并非必须，其低效率更无法满足物联网访问控制需求，私有链相较联盟链而言中心化程度更高，其数据的产生、共识、维护过程完全由单个组织掌握。而联盟链的优势在于能够在不同的管理域间进行信任管理并共享数据，而不需要可信第三方进行仲裁，能够有效解决物联网中的访问控制问题。目前，全球主要的联盟链平台有超级账本（Hyperledger Fabric）、企业以太坊联盟（EEA）、R3 区块链联盟（Corda）和蚂蚁开放联盟链，其中影响力较大的是Hyperledger Fabric。Hyperledger Fabric 是一个开源的区块链开发平台，它不仅具有区块链的去中心化账本、不可变、群体共识等特点，而且还提供了更高效的共识机制、更高的吞吐量、智能合约，以及对多个组织和账本的支持。本文提出的模型基于 Hyperledger Fabric 平台，利用分布式网络架构跟踪访问记录，提供动态访问控制管理，难以篡改性确保了已经写入区块链的数据不能被恶意伪造或修改，公开透明性确保了区块链上的信息是开放的，所有参与者随时可进行查询。

4.4　性能测试

为了验证访问控制系统的性能，本文进行了 4 组实验来测试系统的性能。

（1）单机器实验

在第 1 组实验中，系统在单机区块链网络环境中进行测试，计算不同并发请求的相关智能合约吞吐量。所选择的并发请求数分别设置为 5、10、50、100、200、300、400、500、600、700、800、1 000，ACPC、DAMC 和 PDCC 在不同并发环境中请求的吞吐量性能如图 5 所示。

- 写入操作比智能合约中的读取操作消耗更多的时间。写入操作和读取操作都会根据索引值来查找数据的位置。当新数据写入当前位置时，旧数据必须生成历史版本才能实现数据的可追溯性，但是，读取操作只能直接返回数据的实际值。
- 查询操作的吞吐量是高于更新操作和添加操作的吞吐量。查询操作是一种读取操作，而更新操作和添加操作包括写入操作。
- 由于区块链网络的连接池中的连接数量已经达到了上限，因此该系统的吞吐量趋于稳定。然而，每个事务都以队列的形式完成，而不影响每个节点的事务。
- 如图 5(a)所示，当执行 ACPC 时，Query Policy( )的吞吐量优于 AddPolicy( )和 Update Policy( )，AddPolicy( )和 Update Policy ( )的吞吐量接近。
- 如图 5(b) 所示，当执行 DAMC 时，Check Access( ) 的吞吐量优于 RequestAccess( ) 和 ResponseAccess( ) 的吞吐量，并且 Request Access( )和ResponseAccess( )的吞吐量接近。
- 如图 5(c)所示，当执行 PDCC 时，GetIPFS( ) 和 GetData( )属于查询操作。然而，吞吐量是以 AddData( )>GetData( )的形式出现的。这是因为对私有数据的进行访问需要通过身份和权限进行验证，但对于签名的验证需要很长时间，因此，GetData( )的吞吐量比 AddData( )低。

2）多机器实验

在本实验中，我们提出的系统在与第 1 组实验相同数量的并发请求环境下进行测试，主要比较了在多机器环境下吞吐量的变化情况。

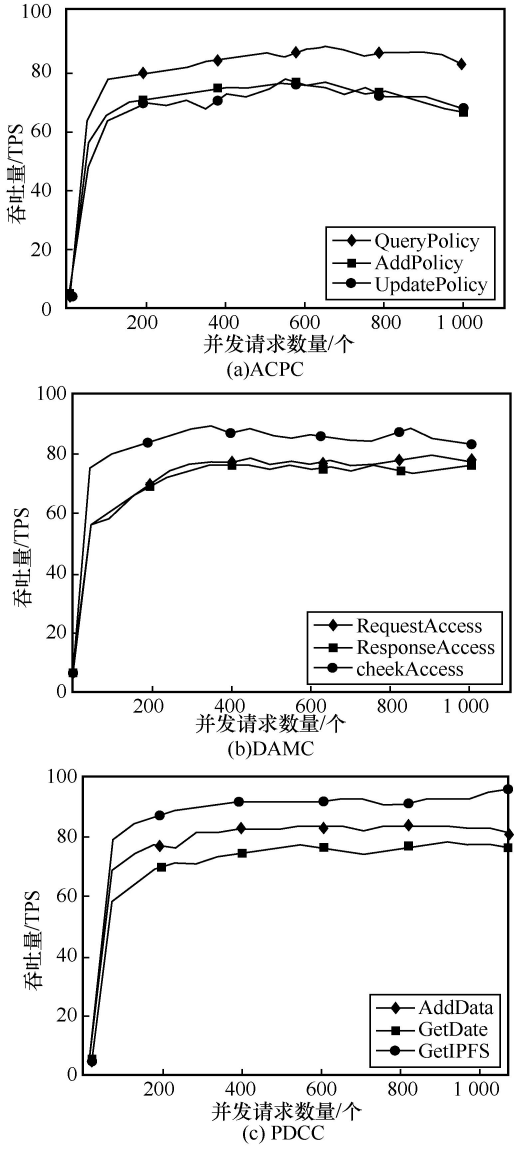


图 5　ACPC、DAMC 和 PDCC 在不同并发环境中请求的吞吐量性能

通过单机和多机器环境验证了该系统在实际应用中具有良好的性能。ACPC、DAMC 和 PDCC 在单机器和多机器环境中不同并发请求的性能比较如图 6 所示，其中 XXX-singe 和 XXX-Multi 分别表示 XXX 方法在单机环境和多机器环境下在 ACPC、DAMC、PDCC 下的实验分析结果。

多机器环境下系统的吞吐量比单机器环境下要好得多。在多机器环境中，吞吐量也受到区块链系统连接池中的连接数量的限制，最终趋于稳定。在多机器环境中，DAMC 中的 CheckAccess( )吞吐量低于 DAMC 中的其他方法，这与单机器环境不同。可以看出，在多机器环境中，通过智能合约中的一种方法调用另一个智能合约的方法会消耗大量的性能，因此，在极端条件下，最好避免这种调用方式。在多机器环境下，GetData( )在 PDCC 中的吞吐量对比其他方法没有显著提高，因此，智能合约中签名和验证操作的性能消耗相对较大，但它在很大程度上保证了数据所有者私有数据的安全性。

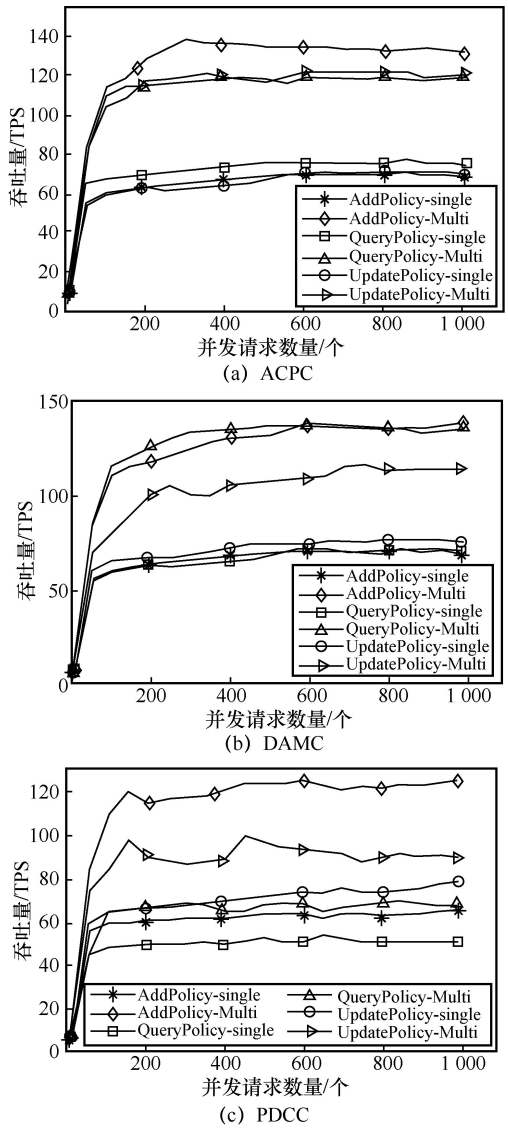


图 6　ACPC、DAMC 和 PDCC 在单机器和多机器环境中不同并发请求的性能比较

3) 区块大小的实验

第 3 组实验在不同的区块大小下测试了该系统的吞吐量。在结构中，区块大小与最大信息计数和绝对最大字节数设置有关。在相同的硬件条件下，本文进行了两组软件实验，设置 MaxMessageCount 的参数为 10、50、100、150、200、350、300、350、400、450、500，AbsoluteMaxBytes 的参数为 5M、15M、30M 和 45M 和 60M。实验结果表明，区块尺寸越大，系统的吞吐量就越大。系统在不同最大信息计数条件下的吞吐量性能如图 7 所示，系统在不同绝对最大字

节数条件下的吞吐量性能如图 8 所示，可以在实际物联网环境中根据需求来调整区块的大小，以增加系统的吞吐量。但是，区块的大小应根据需求进行合理的调整，以避免资源的浪费。

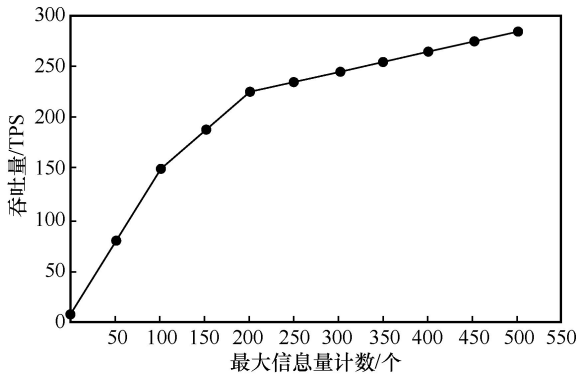


图 7　系统在不同最大信息计数条件下的吞吐量性能

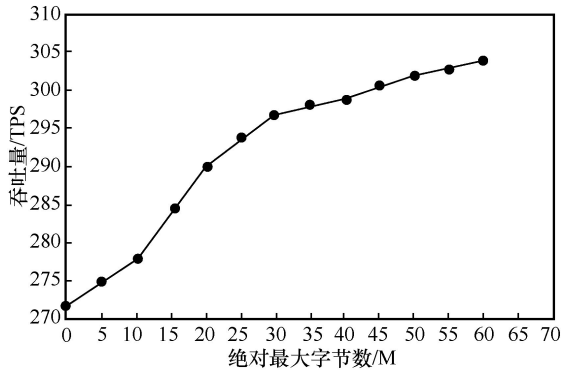


图 8　系统在不同绝对最大字节数条件下的吞吐量性能

4) 基于共识算法的实验

第 4 组实验在不同的共识算法中测试了该系统的吞吐量。结构平台上有 3 种共识算法，分别是 Solo、Kafka 和 Raft。Solo 是一种不适合物联网环境的单节点模式。本文比较测试了 Kafka 和 Raft 在不同并发请求数量下的吞吐量。系统在不同的共识条件下的吞吐量性能比较分析如图 9 所示。

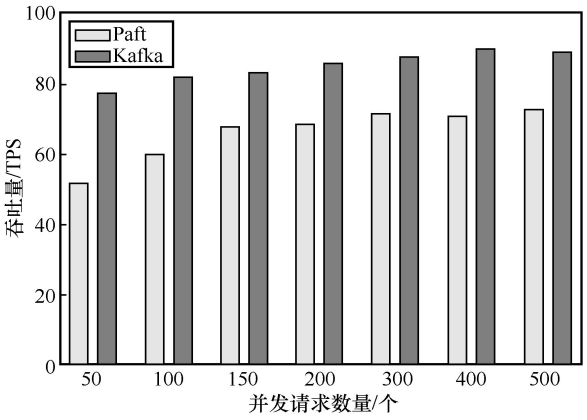


图 9　系统在不同的共识条件下的吞吐量性能比较分析

实验结果表明，Fafka 的吞吐量高于 Raff 的吞吐量。同时，Kafka 具有与 Raft 相同的容错能力，可以保证该系统在高吞吐量条件下的可靠性。因此，Kafka 的高吞吐量可以满足该系统在物联网环境下的需求。

5　结束语

本文提出了一种基于区块链的物联网访问控制框架和私有数据访问控制模型，将 ABAC 模型和区块链技术相结合，以解决物联网环境中的私有敏感数据的访问控制问题。根据物联网设备实际生成的数据，将私有数据存储在区块链网络上，公共数据存储在 IPFS 中。此外，在基于 ABAC 模型的基础上，提出了一种可审计的访问控制系统，以实现对物联网中私有数据的控制、跟踪和管理访问。

总体而言，本文设计了一个基于区块链的开源可审计访问控制系统，可以对物联网中的私有数据进行细粒度访问控制管理。实验结果表明，该方案能够解决物联网数据存储的安全性和细粒度访问控制等问题。因此，该系统满足了物联网的实际运行要求，并达到了预期的目标。对于未来的研究工作和方向，本团队提出以下展望。

1) 该方案获得了实验室的仿真数据和分析结果，对于物联网的访问控制和私有数据的隐私保护有很大的实际应用价值。

2) 由于 Fabric 平台的特点和局限性，该系统所采用的共识算法在容错方面表现突出，但在抵抗恶意攻击方面效率低下。因此，本团队将进一步分析在其他平台上实现的可能性。同时，采用零知识证明的方法来解决外部安全威胁。

3) 为了提高系统的可伸缩性，增加系统连接池中的连接数，在保证系统安全性和稳定的同时提高系统吞吐量性能。

参考文献：

[1] LIU H, HAN D Z, LI D. Fabric-IoT: a blockchain-based access control system in IoT[J]. IEEE Access, 2020(8): 18207-18218.

[2] BABUN L, DENNEY K, CELIK Z B, et al. A survey on IoT platforms: communication, security, and privacy perspectives[J]. Computer Networks, 2021, 192: 108040.

[3] YANG Y S, ZHONG M S, YAO H Q, et al. Internet of things for smart ports: technologies and challenges[J]. IEEE Instrumentation & Measurement Magazine, 2018, 21(1): 34-43.

[4] 史锦山，李茹. 物联网下的区块链访问控制综述[J]. 软件学报, 2019, 30(6): 1632-1648.

SHIJ S, LI R. Survey of blockchain access control in Internet of Things[J]. Journal of Software, 2019, 30(6): 1632-1648.
[5] HU V C, KUHN D R, FERRAIOLO D F, et al. Attribute-based access control[J]. Computer, 2015, 48(2): 85-88.
[6] ZENG S A, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications. 2020,41(01): 134-151.
[7] 田国华, 胡云瀚, 陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报, 2021, 32(5): 1495-1525.
TIAN G H, HU Y H, CHEN X F. Research progress on attack and defense techniques in block-chain system[J]. Journal of Software, 2021, 32(5): 1495-1525.
[8] 房梁, 殷丽华, 郭云川, 等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报, 2017, 40(7): 1680-1698.
FANG L, YIN L H, GUO Y C, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers, 2017(7): 1680-1698.
[9] SUDARSAN S V, SCHELÉN O, BODIN U. Survey on delegated and self-contained authorization techniques in CPS and IoT[J]. IEEE Access, 2021(9): 98169-98184.
[10] BELIM S, BELIM S. Implementation of mandatory access control in distributed systems[J]. Automatic Control and Computer Sciences, 2018, 52(8): 1124-1126.
[11] KAMBOJ P, KHARE S, PAL S. User authentication using Blockchain based smart contract in role-based access control[J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2961-2976.
[12] AGHILI S F, SEDAGHAT M, SINGELÉE D, et al. MLS-ABAC: efficient multi-level security attribute-based access control scheme[J]. Future Generation Computer Systems, 2022, 131: 75-90.
[13] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
LIU M D, CHENZ N, SHIY J, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1-27.
[14] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data[C]//Proceedings of 2015 IEEE Security and Privacy Workshops. Piscataway: IEEE Press, 2015: 180-184.
[15] KOŠŤÁL K, HELEBRANDT P, BELLUŠ M, et al. Management and monitoring of IoT devices using blockchain [J]. Sensors (Basel, Switzerland), 2019, 19(4): 856.
[16] DING S, CAO J, LI C, et al. A novel attribute-based access control scheme using blockchain for IoT[J]. IEEE Access, 2019(7): 38431-38441.
[17] ZHOU L, WANG L, AI T, et al. BeeKeeper 2.0: confidential blockchain-enabled IoT system with fully homomorphic computation[J]. Sensors (Basel, Switzerland), 2018, 18(11): E3785.
[18] HENRY R, HERZBERG A, KATE A. Blockchain access privacy: challenges and directions[J]. IEEE Security & Privacy, 2018, 16(4): 38-45.
[19] CAI Z P, ZHENG X. A private and efficient mechanism for data uploading in smart cyber-physical systems[J]. IEEE Transactions on Network Science and Engineering, 2020, 7(2): 766-775.
[20] KUZMIN A. Blockchain-based structures for a secure and operate IoT[C]//Proceedings of 2017 Internet of Things Business Models, Users, and Networks. Piscataway: IEEE Press, 2017: 1-7.
[21] ZHANG Y Y, KASAHARA S, SHEN Y L, et al. Smart contract-based access control for the internet of things[J]. IEEE Internet of Things Journal, 2019, 6(2): 1594-1605.
[22] PAL S, RABEHAJA T, HITCHENS M, et al. On the design of a flexible delegation model for the internet of things using blockchain[J]. IEEE Transactions on Industrial Informatics, 2020, 16(5): 3521-3530.
[23] SONG L H, LI M C, ZHU Z K, et al. Attribute-based access control using smart contracts for the internet of things[J]. Procedia Computer Science, 2020, 174: 231-242.
[24] SAINI A, ZHU Q Y, SINGH N, et al. A smart-contract-based access control framework for cloud smart healthcare system[J]. IEEE Internet of Things Journal, 2021, 8(7): 5914-5925.
[25] YANG W T, GUAN Z T, WU L F, et al. Secure data access control with fair accountability in smart grid data sharing: an edge blockchain approach[J]. IEEE Internet of Things Journal, 2021, 8(10): 8632-8643.
[26] FOTIOU N, PITTARAS I, SIRIS V A, et al. Secure IoT access at scale using blockchains and smart contracts[C]//Proceedings of 2019 IEEE 20th International Symposium on. Piscataway: IEEE Press, 2019: 1-6.

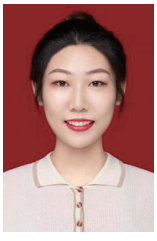
[作者简介]

蒋伟进（1964− ），男，博士，湖南工商大学计算机学院二级教授，主要研究方向为网络安全、社会计算、区块链技术和群体智能感知。

罗田甜（1998− ），女，湖南工商大学前沿交叉学院硕士生，主要研究方向为区块链技术、网络安全和社会计算。

杨莹（1999− ），女，湖南工商大学计算机学院硕士生，主要研究方向为复杂网络、网络安全和区块链技术。

李恩（1995− ），男，湖南工商大学计算机学院硕士生，主要研究方向为网络安全和区块链技术。



周文颖（1999− ），女，湖南工商大学计算机学院硕士生，主要研究方向为网络安全、区块链技术和社会计算。