计算机科学
COMPUTER SCIENCE

基于联盟链的细粒度安全访问控制机制

田洪亮, 宪明杰, 葛平

引用本文

田洪亮, 宪明杰, 葛平. 基于联盟链的细粒度安全访问控制机制[J]. 计算机科学, 2024, 51(6A): 230400080-7.

TIAN Hongliang, XIAN Mingjie, GE Ping. Fine Grained Security Access Control Mechanism Based on Blockchain [J]. Computer Science, 2024, 51(6A): 230400080-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230400080

基于联盟链的细粒度安全访问控制机制

田洪亮　宪明杰　葛　平
东北电力大学电气工程学院　吉林 吉林 132012
(xn_959697@163.com)

摘　要　针对工业物联网存在数据规模庞大、访问安全性差以及隐私安全的问题,提出了基于联盟区块链并使用零知识令牌返回授权的安全访问控制机制,同时,应用IPFS星际文件系统进行链下存储以拓展区块链的可存储性。通过Hyperledger Fabric平台部署区块链网络并编写智能合约,定义访问过程的形式化表达,以更细粒度的模式实现本地和全局的访问授权,并对访问控制的模型和流程进行详细的阐述。最后,通过实验说明区块链网络对访问授权的延迟情况以及策略生成的平均延迟情况,并对比分析了模型的安全性和有效性。结果表明,所提机制在物联网访问控制方面具有安全性、有效性和低延迟性。

关键词:区块链;访问控制;物联网;智能合约;IPFS
中图分类号　TP393

Fine Grained Security Access Control Mechanism Based on Blockchain

TIAN Hongliang,XIAN Mingjie and GE Ping
School of Electrical Engineering,Northeast Electric Power University,Jilin,Jilin 132012,China

Abstract　To solve the problems of huge data scale,poor access security and privacy security in industrial IoT,a data security access control mechanism based on blockchain combined with zero-knowledge token is proposed,while IPFS interstellar file system is applied for off-chain storage to expand the storability of blockchain. A blockchain network is built and smart contracts are deployed through the Hyperledger Fabric platform to define a formal representation of the access process to achieve local and global access authorization in a more fine-grained model,while the model and process of access control are elaborated. Finally,the security and effectiveness of the model are compared and analyzed,and the latency of the blockchain network for access authorization is illustrated through experiments. The results show that the proposed mechanism has security,effectiveness and low latency in IoT access control.

Keywords　Blockchain,Access control,IoT,Smart contract,IPFS

1　引言

在中国制造2025战略[1]的大背景下,随着科技革命和产业变革的蓬勃兴起,工业物联网作为一种实现工业4.0[2]的方法,已经成为学术界和产业界的一个热点,它将是未来工业系统[3-4]的一个重要组成部分。在工业物联网兴起的过程中,物联网也承接着来自工业的海量数据。预计到2025年,我国物联网设备的数量将增长到53.8亿台,这意味着物联网系统及其潜在的应用领域的使用将大规模增长。然而,由于物联网设备的数量众多、规模庞大、分布广泛,设备资源的访问控制面临着巨大挑战。物联网设备产生的资源往往包含隐私和敏感数据,因此,非法获取这些资源将带来严重后果。

访问控制技术是保护资源的重要手段,其主要目的不仅包括防止非授权用户对资源的访问,还包括防止合法用户以非授权方式访问资源,目前已广泛应用于各种系统和环境[5]。但传统访问控制是通过使用中央服务器进行访问授权[6],存在单点故障风险,且在不可信环境下的访问控制难以解决。同时,虽然在同一系统下的设备可以进行互联,也能够进行数据传输,但由于其架构限制,在不同系统下的设备无法实现互联互通,这就造成了设备成本的虚高。区块链技术在访问控制方面有4个优点[7],即去中心化、数据加密、可扩展性和防篡改。目前,区块链技术已经发展到3.0时代,智能合约作为其核心技术,为应用构建了安全可靠的运行环境,赋予了区块链更强大的功能。因此,本文在基于区块链的解决方案中结合了基于属性的访问控制方案(Attribute-Based Access Control,ABAC)和零知识证明(Zero-knowledge Proof),以实现物联网中的安全访问控制。其主要工作和创新之处是:

1)结合基于属性的访问控制方法和零知识证明的区块链解决方案,利用分布式存储机制(InterPlanetary File System),解决了物联网数据的细粒度安全访问控制;

2)利用零知识证明机制,将零知识令牌引入访问控制机制,并将智能合约作为属性库、策略库及执行库,保证系统的隐私安全。

2　相关工作

访问控制技术是通过设置访问限定条件来达到对数据资源的安全访问。经典的访问控制方法大体分为基于角色的访问控制(Role-Based Access Control,RBAC)[8]、基于属性的访问控制[9]以及基于能力的访问控制(Capability-Based Access Control,CapBAC[10])。但是,以上的模型都是采用集中授权

通信作者:宪明杰(xianmj97@163.com)

的模式，容易引起单点故障。

自从比特币的相关概念被首次提出后，区块链技术就被广泛应用于多个领域。物联网的快速发展对分布式访问控制也提出了更高的要求。因此，许多学者在现有访问控制方法的基础上，结合区块链和智能合约提出了物联网访问控制的新方式。

为了解决传统访问控制中存在的单点故障问题，Zhang等[11]提出了基于以太坊的分布式访问控制框架。该框架由访问控制合约、判断合约和注册合约组成，通过3种合约的配合进行访问控制，以实现物联网系统的分布式环境可信访问控制。

Novo[12]提出了一种基于区块链的物联网系统全分布式访问控制方案。该方案使用智能合约来降低节点之间的通信成本。物联网设备以网关节点作为代理参与到区块链的交易过程，避免区块链和设备之间的直接交互。访问控制系统的策略规则通过生成单个智能合约来定义，访问控制策略通过创建针对该智能合约的交易来执行。

为了解决传统的方法难以抵御恶意攻击的问题，Zhang等[13]提出了一种结合区块链与基于属性的访问控制方案。他们设计了一种可核查的协作机制，以满足紧急情况下受控访问授权的需要，并构建权限节点以执行主要计算任务并与区块链交互。Bouras等[14]提出了一种基于能力的分布式访问控制体系结构，并将其命名为IoT-CCAC。IoT-CCAC模型引入了组能力令牌的符号作为改进传统基于能力的解决方案和工作措施，并提出了基于区块链的数据库集成架构，从而实现快速、安全、可扩展的访问控制系统。

Novo[15]提出了一种边缘链，利用区块链的交易体系将边缘计算资源与账户和设备之间的资源使用联系起来。边缘链建立了基于设备行为的信任模型，控制物联网设备从边缘服务器获取资源。Qi等[16]提出了一个用于外包数据的安全细粒度访问控制系统，该系统支持对数据的读写操作。系统使用基于属性的加密(Attribute-Based Encryption，ABE)[17]方案，实现了外包数据的安全和细粒度访问控制。此外，该方案考虑了不同类别的数据用户，并通过对云存储库中相应密文的动态高效策略更新，对外包数据的不同访问角色和允许的操作做出规定。

Sun等[18]为解决基于单服务器体系结构的跨域访问控制机制在安全性和可靠性以及完整性和机密性方面存在局限性的问题，构建了一个基于区块链的可信且高效的跨域访问控制系统，以提供可靠且可验证的跨域访问过程。该方案将区块链与角色映射技术相结合，使用区块链来记录用户角色、角色映射规则、访问策略和审计记录，并设计了一个高效的智能合约，根据用户的访问历史做出访问决策，实现了用户的自我验证和访问控制。Xie等[19]为了提高数据访问流转控制的透明性并解决访问流转的可溯源问题，提出了一种基于区块链的可溯源访问控制机制，采用链下与链上相结合的方式，将访问控制策略以智能合约的形式部署在链上，通过执行智能合约实现访问控制决策，确保整个访问授权过程的无中心、透明性和可溯源。

目前，尽管已经有很多关于利用区块链实现物联网访问控制及探索其匿名访问的研究，但在许多设计中仍存在以下问题：1)更改权限的方式复杂，难以实现细粒度控制；2)计算量巨大，区块链的计算能力没有得到充分利用，导致产生大量资源消耗；3)由于物联网设备的计算能力较低，大多数策略很难在实践中推广；4)许多匿名访问方法很难与以太坊智能合约集成。鉴于上述考虑，本文提出了一种新的基于超级账本的细粒度访问控制管理机制。

3 系统模型

3.1 模型总体设计

系统的总体模型如图1所示。基于联盟区块链设计数据细粒度安全访问控制机制，总体模型分为终端部分和网络部分。网络部分由区块链网络和分布式存储机制组成，其中区块链网络包含信息区块链和访问控制区块链，分别负责访问控制过程中的信息存储与访问验证授权；终端部分包含大量的物联网设备，设备根据位置以及网关等信息组成不同的管理域，各个管理域中的设备通过身份认证后发布区块链账户，用于维护属于本组织的信息区块链。

上述的访问控制模型框架涉及的元素如表1所列。

表1 访问控制模型的元素及描述

Table 1 Elements and descriptions of access control model

元素	描述
$A=\{A_o\}\_o=1,2,\cdots,n$	所有设备的属性集合
$DO=\{DO_i\}\_i=1,2,\cdots,n$	管理域的集合
$S=\{S_i\}\_i=1,2,\cdots,n$	访问主体的集合
$O=\{O_j\}\_j=1,2,\cdots,n$	资源客体的集合
$OP=\{OP_k\}\_k=1,2,\cdots,n$	访问操作的集合
$E=\{E_l\}\_l=1,2,\cdots,n$	访问环境的集合
$ToK=\{ToK_m\}\_m=1,2,\cdots,n$	授权令牌的集合

在图1的总体模型结构中，区块链网络结构分别引入了5种区块链节点，其各自的功能如下。

1)普通节点为信息区块链的主要组成节点，代表单个管理域中的设备，与其他普通节点组成并维护信息区块链，用户通过客户端与之交互。

2)组织节点为各个管理域的父节点，部署和运行属性管理合约，负责将节点信息向区块链上传、下载以及验证等操作，对来自属于本管理域以内的访问申请进行处理，实现本地数据资源的访问控制与查询。

3)跨域节点由信息区块链中的任一普通节点担任，与其他管理域中的跨域节点共同维护访问控制区块链，部署和运行智能合约，对来自其他管理域的访问申请进行委派授权，实现多个管理域间的数据资源的访问控制。

4)授权节点为访问控制链上的普通节点，部署和运行访问授权管理合约，负责访问控制过程的授权以令牌形式进行返回操作，并以广播形式将授权信息发送给其他节点，保证授权结果的共识一致。

5)审计节点为访问控制链上的管理节点，部署和运行访问策略管理合约，负责管理访问控制链产生的每一次访问记录，保证用户能追溯到历史授权请求的访问记录，降低区块链的吞吐量，防止恶意请求行为的发生。

区块链作为一个开放式的数据中心，能以去中心化的形式安全地登记和更新交易。它记录了网络中产生的所有交易，并维护一个分布式账本，以提高安全性和隐私性。一个区块通常由两个必要的部分组成：区块头以及区块体。交易的认证通过数字签名进行加密处理，在交易被签署后，它们被打

包到一个被称为区块的加密防窜改结构中，这些区块通过哈希指针按时间顺序连接起来，形成一个链。共识算法用以产生关于区块顺序的协议，同时也是为了验证区块交易的正确性与一致性。访问控制链利用区块存储结构来存放访问控制所需信息；此外，信息区块链存储各类组织或设备的属性数据，如设备 MAC 地址信息、组织方位信息以及产品身份信息等，实现数据的分布式安全存储。区块链结构如图 2 所示。

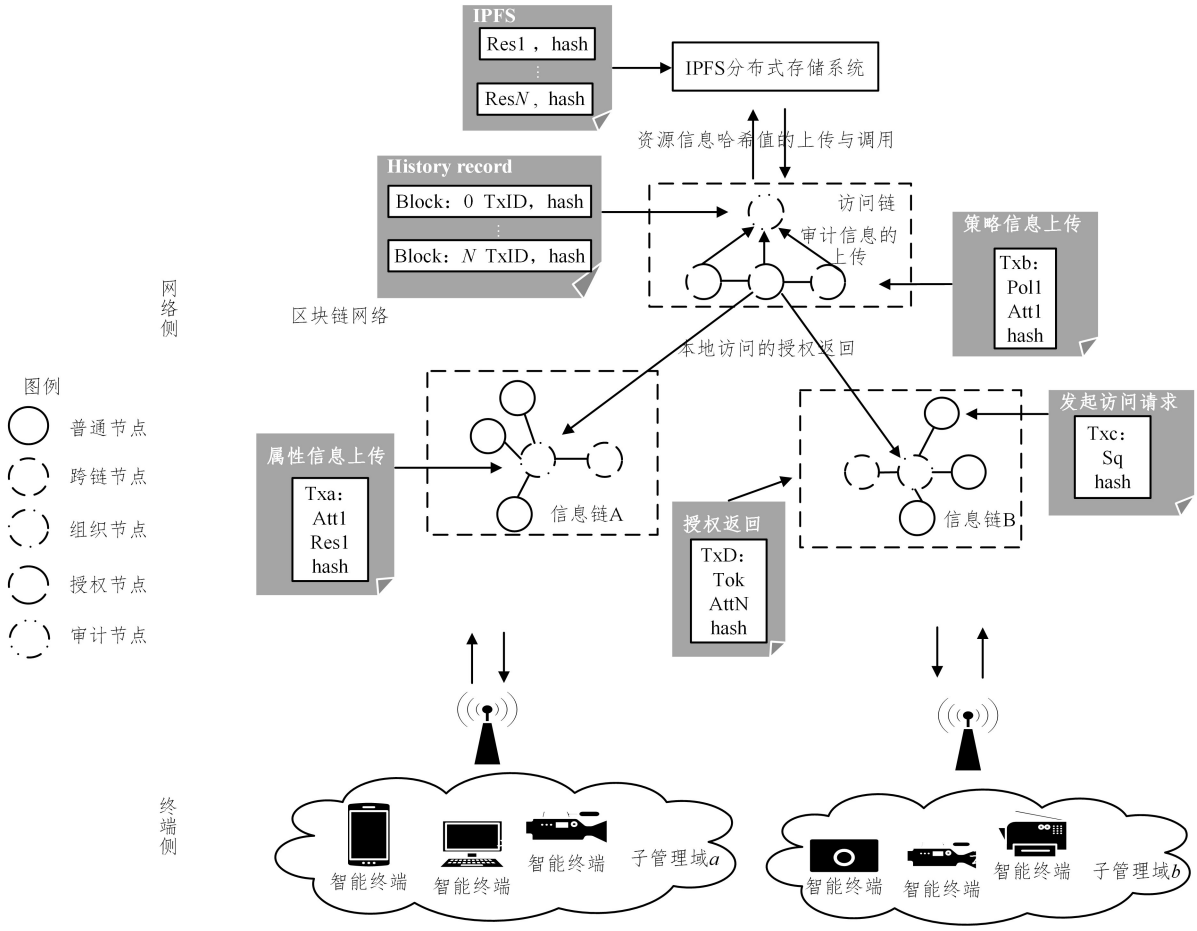

图 1　访问控制模型的总体架构

Fig. 1　Overall architecture of access control model

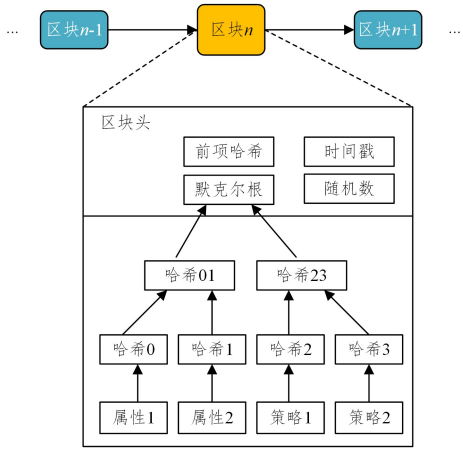

图 2　区块存储结构示意图

Fig. 2　Diagram of block storage structure

网络部分由区块链和 IPFS 组成。访问控制区块链是网络部分的主体，通过跨域节点连接不同管理域 DO_i，链内包含授权节点和审计节点。IPFS 用于存储终端部分产生的资源数据，且将其返回的哈希值进行上链操作，授权时只需要提供对应文件的哈希值就能在 IPFS 中查询到相应的文件。IPFS 与区块链网络的交互如图 3 所示。

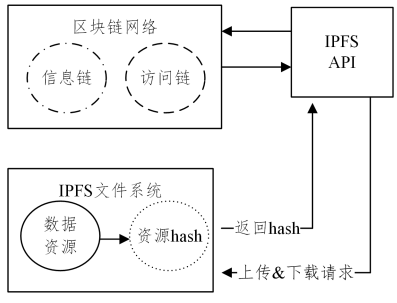

图 3　IPFS 与区块链交互

Fig. 3　IPFS and blockchain interaction

3.2　智能合约设计

智能合约是实现基于区块链系统的访问控制机制的核心。本文将智能合约设计分为访问控制管理合约以及访问控制执行合约。为方便叙述访问授权的过程，引入以下定义。

定义 1　访问过程的形式化表达如式(1)所示：

$$F\{P=(DO_i \cup \langle S_i, O_j, E_l, OP_k \rangle) \rightarrow R \Rightarrow TOK\{1,0\}\} \quad (1)$$

其中，$S_i \in S, O_j \in O, E_l \in E, OP_k \in OP$。

该形式化表达中，P 表示多元组组成的访问策略；DO 表示访问请求的所属组织，包含本域的访问请求或者属于跨组织的访问请求；S 代表主体属性；O 代表客体属性，如资源 id；

OP 代表访问操作，其中包含读(R)、写(W)、删除(D)等操作；E 代表访问环境，例如访问位置信息和请求时间信息等；F 表示对访问策略进行判定，R 为判定结果，若允许访问则返回Y，并以令牌 TOK 的形式进行访问授权，若拒绝访问则返回N，并记录无效访问。

访问控制管理合约包含属性库管理合约(Attribute Database Contract，ABC)和策略库管理合约(Policy Database Contract，PBC)。

ABC 合约负责对主体以及对象的属性信息数据进行存储和管理，包含上链以及查询等操作。上链操作负责将主体以及客体的关键属性信息在数据区块链中进行上传并存储；查询操作通过数据的验证签名在链上查找数据并返回有效资源信息。

PBC 合约负责对访问控制策略进行存储与管理，其中包含策略查询、添加以及更新等功能。在本模型中，访问策略由主体属性 S_i、对象属性 O_j、环境上下文 E_l 和访问操作 OP_k 组合，如定义 1 中式(1)所示。在管理域 DO_i 中设置参数 γ，如果 γ 的值为 0，则表示此访问策略为本地的访问策略；如果 γ 值为 1，则表示此访问策略为全局的访问策略，需要再设置访问的委托操作，形式化表达如式(2)所示。

$$R_{sq}=F_{DO_i}(\gamma),\gamma=\{0,1\} \tag{2}$$

访问控制执行合约(Access Control Contract，ACC)主要负责访问请求的授权与审计。主体发起访问请求 S_q 时，需要将请求信息以事务的形式发送给 ACC 合约，访问请求的格式如式(3)所示。

$$S_q=\{DO\cup\langle O_i,E,OP\rangle\}\triangleright ACC \tag{3}$$

ACC 合约接收到此访问请求后，会结合 ABC 与 PBC 分别查询访问请求的主体签名和 S_q 中涉及的元素信息以及对应的访问控制策略，如式(4)所示。

$$F=\{ACC\triangleright(ABC\cup PBC)\} \tag{4}$$

紧接着，ACC 合约会进一步查询主体对于该资源的授权令牌 TOK，如果该主体的访问请求 S_q 对于访问该对象为内部访问请求 NQ，则直接通过访问请求并返回访问令牌；若为全局访问请求 GQ，那么 ACC 合约则会基于这些属性和访问策略，委派跨域节点进行委派，最终将授权结果返回给主体。

3.3 访问控制流程

本文的访问控制机制工作流程参照基于属性的访问方法，应用区块链网络作为属性库、策略库和执行库，具体流程如图 4 所示。

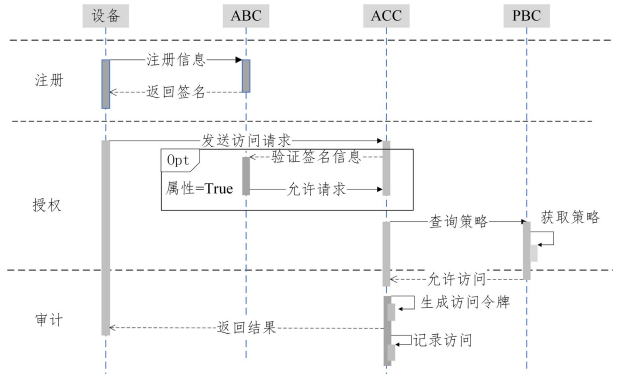

图 4 访问控制流程示意图

Fig. 4 Schematic diagram of access control process

STEP1 注册阶段：对于注册，设备所属的属性机构将在验证其身份后，在基于身份的加密的安全通道中向其颁发一对密钥，同时通过零知识证明生成的数字签名来证明属性的所有权并以区块交易的形式上传到信息区块链。采用零知识证明生成数字签名的过程如下所示。

首先，基于椭圆曲线循环群选取随机多项式 $\alpha,\beta,\gamma,\lambda$ 与随机数 x 构成集合 η,μ，如式(5)－式(8)所示。

$$\eta=(\alpha,\beta,\gamma,\lambda,x) \tag{5}$$

$$\mu=([\mu_1]_1,[\mu_2]_2) \tag{6}$$

$$\mu_1=(\alpha,\beta,\lambda\ \{x^i\}_{i=0}^{n-1},\{\frac{\beta u_i(x)+\alpha v_i(x)+w_i(x)}{\gamma}\}_{i=0}^{l},\{\frac{\beta u_i(x)+\alpha v_i(x)+w_i(x)}{\lambda}\}_{i=l+1}^{m},\{\frac{x^i t(x)}{\lambda}\}_{i=0}^{n-2}) \tag{7}$$

$$\mu_2=(\beta,\gamma,\lambda\{x^i\}_{i=0}^{n-1}) \tag{8}$$

在证明生成阶段选取参数 y,z，根据式(9)生成证明。

$$\pi=\Pi\lambda=([A]_1,[B]_2,[C]_1) \tag{9}$$

其中 A,B,C 为椭圆曲线的 3 个点，其计算式如(10)－式(12)所示。

$$A=\alpha+\sum_{i=0}^{m}\alpha_i u_i(x)+y\lambda \tag{10}$$

$$B=\beta+\sum_{i=0}^{m}\alpha_i u_i(x)+z\lambda \tag{11}$$

$$C=\frac{\sum_{i=l+1}^{m}a_i(\beta u_i(x)+\alpha v_i(x)+w_i(x))+h(x)t(x)}{\lambda}+Az+yB-yz\lambda \tag{12}$$

在上面的计算式中，生成的结果是椭圆曲线上的 3 个点(B 点需要计算两次)，然后将这 3 个点交给验证者进行验证，验证计算式如式(13)所示。

$$A\cdot B=\alpha\cdot\beta+\frac{\sum_{i=0}^{l}a_i(\beta u_i(x)+\alpha v_i(x)+w_i(x))}{\gamma}\cdot\gamma+C\cdot\lambda \tag{13}$$

将属性信息写入区块链后，每次调用属性信息时，都要通过验证签名来确认属性的来源，如式(14)所示，以此作为参与访问控制过程的凭证，确保每个参与访问的设备合法化，在初始阶段排除未经处理的设备非法请求。

$$C=\frac{AB-\alpha\beta-\sum_{i=0}^{l}a_i(\beta u_i(x)+\alpha v_i(x)+w_i(x))}{\lambda} \tag{14}$$

STEP2 授权阶段：首先，ACC 会接收主体对客体资源的访问信息请求 S_q，并从 ABC 中查询访问请求的主体签名和 S_q 中涉及的元素信息进行主体以及访问对象的签名验证，若验证成功则进入策略查询阶段，否则终止访问请求并保存记录此次访问记录的具体信息；接着，ACC 会从 PBC 中查询访问请求类型(本地请求 NQ 或跨域请求 GQ)，若为 NQ，那么 ACC 就会从 ABC 中查询访问对象的存储资源的地址信息，若为 GQ，那么访问授权需要跨域节点的辅助；最后，在查询到相关地址信息后，ACC 会根据主体信息和访问对象信息，再从 PBC 中查询判断是否拥有相关的访问策略，若返回无可用的访问策略，那么 ACC 就会终止访问并将该结果返回给主体，确保访问授权阶段主体的访问请求细粒度化，在访问授权过程中避免越权的访问请求。

STEP3 审计阶段：该阶段主要进行授权令牌的返回以

及访问授权的保存记录。如果访问请求为本地请求(NQ)，在查询到存在相关访问策略后，ACC 会生成此管理域特有的访问令牌，将允许访问的结果返回给主体，在令牌因异常而无效之前，主体都可通过令牌在合法权限内访问资源；如果访问请求为跨域请求(GQ)，需要跨域节点进行访问权限的委派，ACC 会生成相应的跨域节点的委派令牌，通过跨域节点调用存储在 PBC 合约的委派令牌，进行主体访问请求的委派，仍然通过 ACC 将响应结果返回给主体；最后，无论是本地的访问请求还是跨域的访问请求，都要把每次访问记录的主体信息、客体信息以及访问时间等相关信息打包成区块以交易的形式存储上链，确保访问授权返回过程中以及访问记录的隐私安全。

4 实验分析

4.1 实验环境配置

基于 Hyperledger Fabric 区块链平台对本文所提数据细粒度安全访问控制机制的系统性能进行验证。作为一个开源的平台，Hyperledger 具有可定制的特点，并在区块链部署中被广泛采用。实验涉及的相关参数如表 2 所列。

表 2 相关软硬件参数

Table 2 Relevant software and hardware parameters

软硬件	参数
操作系统	Ubuntu 18.04 LTS
处理器	Intel Core i7-10510U CPU @ 2.30GHz
内存大小/GB	16
Hyperledger Fabric 版本	2.0.0
Golang 版本	1.19
Docker 版本	18.09.3
node.js 版本	16.3.1

在 Ubuntu 系统下配置超级账本环境，配置两个组织域以及 Order 节点和 peer 节点模拟不同的管理域，将采用 Java 编写的智能合约通过添加 fabric-chaincode 的相关依赖部署到区块链网络中。区块链网络的配置过程以及启动过程如图 5 及图 6 所示。

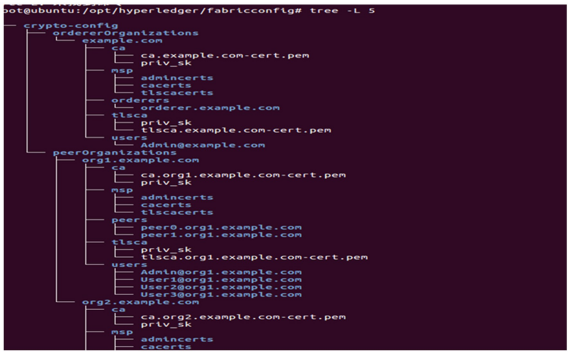

图 5 区块链网络配置树状图

Fig. 5 Blockchain configuration tree

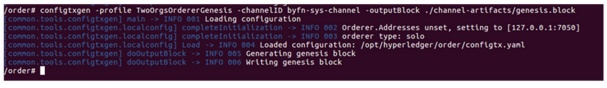

图 6 启动网络

Fig. 6 Start network

4.2 网络性能分析

访问延迟是评价访问控制模型执行效率的一个重要指标。访问延迟包括访问授权响应、注册阶段以及策略生成等阶段的时间延迟。本节采用 Hyperledger Caliper 工具对系统性能开展测试，分别对访问控制策略生成时间的应用性能以及系统授权响应进行测试与分析，并且对本文所设计的基于联盟区块链的访问控制机制与文献[14]所用方案在系统性能上进行了对比实验与分析。

为了验证所提系统中访问策略生成时间延迟情况，本次实验测试工况为同一管理域内不同主体进行多次并发访问时的访问策略的生成时间情况，设置访问次数分别为 100，200，400，600，800，1000。得出不同访问次数下访问策略的生成时间并计算平均值，且与对比方案进行相同工况下访问策略的平均生成时间对比，实验结果如图 7 所示。

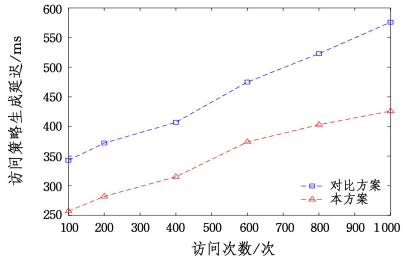

图 7 不同访问次数下访问策略生成的延迟情况

Fig. 7 Latency of access policy generation with different access times

从图 7 可知，本方案与对比方案在随并发访问次数增加的过程中，访问策略的平均生成时间均有所增长，但本方案的访问策略平均生成时间能够保持在较低的延迟水平。此外，随着并发请求次数的增加，本方案策略的生成时间近似线性增长，但在超过 500 次并发请求后访问策略的平均生成时间的增幅逐渐平稳，能够保持在 0.45 s 以内。这是由于整个区块链系统在每次的访问过程结束后都会更新访问策略库并以交易形式上链存储，使得多次并发访问后通过查询可直接调用访问策略进行授权，从而导致策略生成时间在多次并发请求后趋于平稳状态，这有助于保持系统的稳定性。

访问控制过程最终目的是实现访问授权，因此，测试访问授权的延迟情况具有一定的参考价值。为测试区块链系统访问请求的响应时间，测试了每秒内数量为从 0 到 5000 个的节点进行 500 次访问请求的响应时间情况。在联盟链设置两个组织，验证模型只进行域内访问和只进行域间访问响应的延迟情况，记录不同数量节点下访问授权的响应时间的平均值，实验结果如图 8 所示。

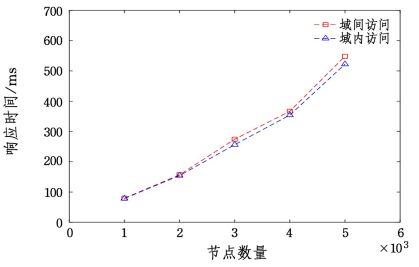

图 8 访问控制授权响应延迟

Fig. 8 Delayed response of access control authorization

从图 8 可以看出，当请求节点从 0 增加到 5000 时，进行

域间访问授权的响应时间与域内访问授权的响应时间均处于上升趋势，且当5000个节点进行访问时两种类型的访问授权响应时间均保持在0.6 s以下。此外，在节点数量增加的过程中，域间访问授权的响应时间比域内访问授权响应时间略微延时，但都处在较低的延迟水平。这是由于系统进行域间访问授权时，在授权阶段还需要通过跨域节点进行访问授权的委派交易，从而影响了授权的响应时间。

4.3 安全性分析

为评估本文所提方案的安全性，从而列举了分散系统中的几种常见攻击，并讨论了该系统避免此类攻击的方法。表3列出了抵御攻击涉及的几个关键符号。

表3 符号描述

Table 3 Symbol description

符号	描述
$H(*)$	抗碰撞哈希函数
$Sign(*)$	签名算法
$Enc_{pk}(*)$	非对称加密算法
$\{pk_u, sk_u\}$	设备密钥对
$Trx(*)$	区块交易
tok_{do}	授权令牌

1)伪造攻击：这是一种常见的攻击，通过篡改身份和交易数据来访问机密信息或者使用随机数据攻击系统。

本方案中攻击者以及系统内的参与者无法获取其他节点的相关信息。身份信息在注册阶段经过数字签名$Sign(*)$后将信息进行上链操作，并且加入网络的节点都会存在密钥对$\{pk_u, sk_u\}$，加大了伪造攻击的难度。交易数据会在审计阶段打包成区块以交易的形式$Trx(*)$进行上链，使得伪造数据或者篡改身份变得更困难，达到抵御伪造攻击的效果。

2)注入攻击：攻击者可以注入脚本文件来操纵授权过程，更改数据库记录或执行不需要的操作。

方案中将访问控制过程形式化表达为$F(s_q)$。对于每一次访问请求，通过智能合约的判断方法在访问数据存储之前运行不同的检查，以确保信息的合法性。同时，智能合约是以交易的形式$Trx(*)$存储在链上的资源，由访问控制链上的节点共同维护，若要进行注入攻击，首先要对抗网络的$H(*)$算法，这种存储方式使得脚本不易被操纵篡改，达到抵御注入攻击的效果。

3)中间人攻击：攻击者秘密站在两个通信实体之间，读取交换的数据。

在注册阶段，区块链网络采用$Enc_{pk}(*)$进行密钥的颁布分配，并且在授权返回的过程通过令牌tok_{do}传递。事实证明，零知识很难被非法破解，这大大增加了攻击者的成本。此外，访问者的访问行为存储在历史访问记录中，攻击者无法隐匿于通信实体之间进行数据的拦截。

攻击行为是攻击者利用网络的弱点使系统的安全状态发生变化的动作。本节通过定义多元函数将攻击行为进行形式化表达，如式(15)所示。

$$AT=\{action\text{-}name, precondition, effect\} \tag{15}$$

其中，$action\text{-}name$，$precondition$和$effect$分别表示攻击名称、攻击的前置条件以及攻击的后果效应。只有满足攻击的所有前置条件，才能对系统中的区块链节点产生影响。设置成功抵御攻击的概率为P，对比不同方案抵御不同类型攻击的性能情况，具体结果如图9所示。

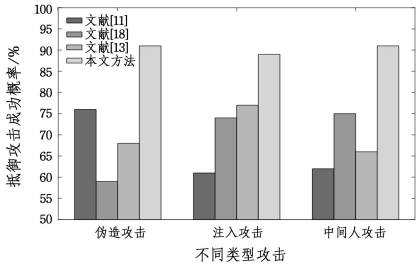

图9 不同类型攻击下抵御成功概率的比较

Fig. 9 Comparison of probability of successful defense with different types of attacks

本方案在访问控制的3个阶段过程都有抵御恶意攻击的能力。

4.4 对比分析

分别从访问授权类型、架构基础、灵活性、可扩展性、授权透明性这5个角度对本文模型和目前已有的研究进行对比，具体如表4所列。

表4 本方案与现有方案的不同角度对比

Table 4 Comparison between the proposed scheme and existing schemes from different perspectives

方案	基于属性	基于超级账本	细粒度性	支持链下存储	授权透明
文献[11]	是	否	不具备	否	是
文献[17]	否	是	不具备	否	否
文献[13]	是	是	具备	否	是
本方案	是	是	具备	是	是

结合表4分析，本文所述方案具有以下几个方面的优势。

1)安全性：本模型的数据信息区块链由多节点共同维护，令数据更可信，链上数据动态增长，攻击难度不断加大，能有效防止恶意节点攻击；同时，采用零知识令牌返回授权请求对隐私信息进行加密处理，从而保障隐私安全。

2)细粒度性：本模型对访问控制进行了形式化的表达，结合访问控制区块链中相关的智能合约，建立访问请求，对访问控制授权进行具体描述，易于准确识别各个组织域访问请求，便于用户访问，系统管理更灵活。

3)链下存储：本模型使用IPFS对区块链的可存储性进行拓展，把资源信息与参与访问过程的信息分类存储。将资源存储在IPFS中，从而减少区块的存储压力，降低模型的量级。

4)授权透明：属性信息需要进行链上存储，保证访问授权前验证的透明可信；访问信息，包括策略执行过程和审计过程，也存储在区块链中，在保障访问记录真实可信的同时能有效防止恶意节点在访问执行阶段的恶意攻击。

结束语 针对目前工业物联网的安全访问控制问题，本文提出了一个基于联盟区块链的细粒度安全访问控制模型，结合了ABAC访问控制方法与零知识令牌，并借助超级账本平台搭建区块链网络，使用链码参与访问控制的核心环节；同时为扩展模型的存储能力，利用分布式存储机制将资源信息进行链下存储。最后，通过分析模型的时延特性，说明了模型在互联网环境中的可行性，并从不同角度分析了模型的安全性。与现有的基于区块链的访问控制方案相比，本方案能够在实施多域访问控制的前提下进行更灵活的访问授权与

返回。未来,将对访问策略的动态更新做进一步的优化,以实现更好的性能。

参 考 文 献

[1] ZHANG P,LIU H Y,LI W J,et al. Industrial intelligent network-deepening and upgrading of industrial Internet [J]. Journal of Communications,2018,39(12):134-140.

[2] SIKORSKI J,HAUGHTON J,KRAFT M. Blockchain technology in the chemical industry: Machine-to-machine electricity market[J]. Applied Energy,2017,195(JUN. 1):234-246.

[3] LI Z,KANG J,YU R,et al. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things [J]. IEEE Transactions on Industrial Informatics,2017,PP(99):1-1.

[4] QIU C,YU F,YAO H,et al. Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep Q-Learning Approach[J]. IEEE Internet of Things Journal,2019,6(3):4627-4639.

[5] WANG J,HAN W,ZHANG H,et al. Trust and Attribute-Based Dynamic Access Control Model for Internet of Things [C]// 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery(CyberC). 2017.

[6] LENG J,YE S,ZHOU M,et al. Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey[J]. IEEE Transactions on Systems,Man,and Cybernetics:Systems,2021,51(1).

[7] YANG Q,LU R,RONG C,et al. Guest Editorial The Convergence of Blockchain and IoT: Opportunities,Challenges and Solutions[J]. IEEE Internet of Things Journal,2019,6(3):4556-4560.

[8] LIU Q,ZHANG H,WAN J F,et al. An Access Control Model for Resource Sharing based on the Role-Based Access Control Intended for Multi-domain Manufacturing Internet of Things [J]. IEEE Access,2017,5:7001-7011.

[9] NING Y E,YAN Z,WANG R C,et al. An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things[J]. Applied Mathematics & Information Sciences,2014,8(4).

[10] GUSMEROLI S,PICCIONE S,ROTONDI D. A capability-based security approach to manage access control in the Internet of Things[J]. Mathematical & Computer Modelling,2013,58(5/6):1189-1205.

[11] ZHANG Y,SHOJI K,SHEN Y,et al. Smart Contract-Based Access Control for the Internet of Things[J]. IEEE Internet of Things Journal,2019,6(2):1594-1605.

[12] OSCAR N. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT[J]. IEEE Internet of Things Journal,2018,5(2):1184-1195.

[13] ZHANG Y,LI B,LIU B,et al. An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices[J]. Electronics,2020,9(2):285.

[14] BOURAS M,XIA B,ABUASSBA A,et al. IoT-CCAC: a blockchain-based consortium capability access control approach for IoT[J]. PeerJ Computer Science,2021,7(3):e455.

[15] NOVO O. Scalable Access Management in IoT using Blockchain: a Performance Evaluation[J]. IEEE Internet of Things Journal,2019,6(3):4694-4701.

[16] QI X,SIFAH E,AGYEKUM O,et al. Secured Fine-Grained Selective Access to Outsourced Cloud Data in IoT Environments [J]. IEEE Internet of Things Journal,2019,6(6):10749-10762.

[17] BETHENCOURT J,SAHAI A,WATERS B. Ciphertext-Policy. Attribute-Based Encryption[C]// IEEE Symposium on Security & Privacy. IEEE,2007.

[18] SUN S,CHEN S,DU R. Trusted and Efficient Cross-Domain Access Control System Based on Blockchain[J]. Scientific Programming,2020,2020(10):1-13.

[19] XIE R N,LI H,SHI G Z,et al. Traceable access control mechanism based on blockchain [J]. Journal of Communications,2020,41(12):82-93.

TIAN Hongliang, born in 1981, Ph. D, associate professor. His main research interests include IoT and blockchain.

XIAN Mingjie, born in 1997, postgraduate. His main research interests include blockchain and access control.