一种基于区块链的物联网访问控制方案

杨久华[1],沈苏彬[2]
(1. 南京邮电大学 计算机学院,江苏 南京 210046;
2. 南京邮电大学 通信与网络技术国家工程研究中心,江苏 南京 210046)

摘 要:区块链技术应用于物联网资源管理领域得到了广泛的关注,致力于解决物联网环境下集中式资源存储和管理存在的单点故障、隐私和信任等问题。通过研究区块链技术底层原理,结合现有的研究工作成果和其他数据安全技术,提出一种基于区块链和基于属性访问控制的物联网访问控制方案。为了权衡资源安全和访问控制过程透明化,提出双链的去中心化访问控制模型,将资源元数据信息和访问控制信息分开存储和管理,有利于高效地查询所需信息。为了提高访问控制评估和权限验证速度,划分属性并提出静态属性令牌和引入多项式函数的访问树策略表达方式。最后,利用智能合约实现访问控制逻辑,仿真实验表明方案能够有效地保护资源的隐私和安全,是一种动态的、可信的访问控制方案。

关键词:物联网;区块链;资源存储;访问控制模型;智能合约
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1673-629X(2023)12-0136-07
doi:10.3969/j.issn.1673-629X.2023.12.019

An Access Control Scheme of Internet of Things Based on Blockchain

YANG Jiu-hua[1], SHEN Su-bin[2]
(1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210046, China;
2. National Engineering Research Center on Communication and Networking, Nanjing University of Posts and Telecommunications, Nanjing 210046, China)

Abstract: The application of blockchain technology in the resource management field of the Internet of Things has received wide attention, and is committed to solve the single point of failure, privacy, trust and other problems of centralized resource storage and management in the Internet of Things environment. By studying the underlying principles of blockchain technology, combining with existing research achievements and other data security technologies, a blockchain based and attribute based access control scheme for the Internet of Things is proposed. In order to balance resource security and transparency of access control processes, a dual chain decentralized access control model is proposed, which stores and manages resource metadata information and access control information separately, which is conducive to efficiently query the required information. In order to improve the speed of access control evaluation and permission verification, attributes are divided and static attribute tokens are proposed, as well as an access tree policy expression method that introduces polynomial function. Finally, the smart contract is used to implement access control. Simulation experiments show that as a dynamic and reliable access control scheme, it can effectively protect the privacy and security of resources.

Key words: Internet of Things; blockchain; resource storage; access control model; smart contract

0 引 言

随着互联网和传感技术的快速发展,物联网在实现物与物相连、人与物相连的基础上被广泛应用于智能家居[1]、医疗健康监测[2]等领域。据预测 2025 年物联网将连接 300 亿台设备,而物联网数据将呈现指数级增长[3]。这些隐私数据一旦泄漏,会给用户带来不必要的骚扰,或造成巨大经济损失。访问控制是保障数据安全的关键性技术之一,其主要作用是阻止未授权的用户操作以及限制授权用户在非授权范围内的操作,只有具备操作权限的用户才能访问控制机制并访问数据,以保障数据安全[4]。因此,访问控制成为物联网环境保护数据安全的研究热点之一。

物联网环境下的访问控制需要考虑三个问题[5]:

(1)轻量级的终端设备;

收稿日期:2023-03-16 **修回日期**:2023-07-19
基金项目:江苏省未来网络前瞻性研究项目(BY20130951108)
作者简介:杨久华(1997-),女,硕士研究生,通讯作者,研究方向为区块链;沈苏彬(1963-),男,博士生导师,研究员,CCF 高级会员(E200005482S),研究方向为物联网及其应用、未来网络及其应用。

(2)设备异构且数量逐渐增多;

(3)动态性,如设备的移动性。

访问控制模型是由主体、客体、操作和策略之间进行交互,从而制定和实施访问控制决策[6]。物联网主流的访问控制模型主要包括基于角色的访问控制(Role-Based Access Control,RBAC)模型和基于属性的访问控制(Attribute-Based Access Control,ABAC)模型。ABAC 作为 RBAC 的补充和扩展,无需提前设置角色权限表,将角色或身份抽象成一组属性,用户通过属性与权限对接。定义相对少的中间变量和权限赋予就能达到控制大量节点的目的,即 n 个属性能拥有 2^n 个中间变量[7]。因此,ABAC 提供了细粒度和灵活的访问控制能力,能满足物联网访问控制的需求。

但是,物联网设备通常将收集和产生的数据上传至第三方可信机构,进行集中式存储和管理,容易带来单点故障和内部操作不透明等问题。应运而生的是基于权能的分布式访问控制(Capability-Based Access Control,CapBAC)模型[8],由物联网设备自身执行权限的决策和验证,但是大部分轻量级的物联网设备不具备决策的能力。由此可见,物联网环境下资源的访问控制面临的问题是为了适应物联网的三大特性而依赖于中心化存储和控制模式导致的信任问题。

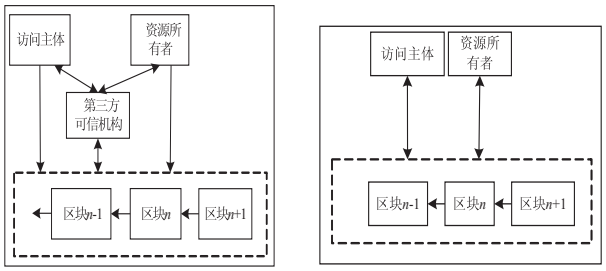
区块链是一种去中心化的信任管理机制,由“中本聪”在构建全球去中心化数字货币比特币的过程中设计和实现[9]。在区块链中,利用交易实现价值的转移或消息的传递,区块记录交易信息,区块之间通过密码学哈希以引用的方式链接。利用密码学技术实现身份的验证,通过时间戳和哈希函数保证数据的可追溯和不可篡改特性,依据共识算法实现节点间账本一致性[10]。Vitalik Buterin 提出了以太坊区块链平台,其中,智能合约是通过事件驱动的计算机程序,具有数据透明和不可篡改的特性,确保智能合约的可信性[11]。

为了解决上述提到的信任问题,区块链技术的去中心化、不可篡改、可审计性和可编程的优势开始显现。将区块链技术应用于物联网资源的安全保护,设计了一种去中心化模式下的访问控制方案。将资源管理界定为资源存储、访问控制这两个方面,将其涉及到信任管理的关键信息存储到区块链,以实现资源的可信管理。

首先,为了减缓区块链存储压力和保护数据的隐私,提出使用区块链结合星际文件系统实现资源存储。其次,以数据所有者为中心,为了使访问控制过程正确且可信,提出区块链结合 ABAC 实现资源的访问控制,以保证资源的安全性、保密性和可用性。最后,基于以太坊区块链平台的仿真实验,验证了方案的正确性和可行性。

1　相关工作和问题分析

目前,引入区块链技术的访问控制研究工作分为两类,第一类是区块链作为传统访问控制模型的可信实体,如图 1(a)。第二类是一种完全基于区块链的物联网访问控制模型。区块链记录访问控制信息和资源信息,还作为访问决策点,如图 1(b)。



(a)存在第三方可信机构　　(b)去中心化

图 1　两类研究工作

Kshetri[12]全面地分析了利用区块链技术使物联网具备设备接入可缩放能力、防范设备被恶意攻击及数据篡改的能力,同时提供可信本地数据存储和管理能力。Hu[13]结合自主访问控制模型将数据存储在第三方可信机构,利用区块链的难篡改和透明化的特性来记录访问决策的过程,提高了决策过程的可信度。Ding[14]利用 ABAC 与区块链相结合,提出新的访问控制模型,使用区块链作为存储平台,存储设备的属性和访问信息,由第三方可信机构决策访问请求,将决策结果记录在区块链。Maesa[15]扩展了 ABAC 的标准工作流,由区块链代替传统的数据库来存储属性及策略并以交易的形式管理。

对于第二类研究工作,Ouaddah[16]提出令牌优化访问流程,节省了再次访问花费的时间和计算开销。将访问权限以脚本的形式保存在区块链,访问者通过解锁脚本来获得访问权限,但是脚本的计算能力有限,无法处理复杂的访问控制逻辑。而且,令牌是对特定资源的访问权限凭证,意味着权限的修改涉及到令牌的更换,复杂性高。Xu[17]提出 BlendCAC 方案,将 CapBAC 模型与区块链技术结合,由数据所有者在智能合约中定义访问控制矩阵,访问者通过提供的合约地址和远程调用接口与智能合约交互,使物联网设备利用智能合约实现自动化的决策和结果响应。Liu[18]提出了 Fabric-IoT,使用三种智能合约来实现物联网环境下自动化的 ABAC 和数据管理:(1)存储设备产生的数据的 URL;(2)存储访问控制策略;(3)实施访问控制。Xu[19]提出一种基于以太坊和 IPFS 的去中心化社交网络系统,使用 IPFS 来保存大量的文件数据,区块链中存储文件数据的链接地址,大大减轻区块链的存储压力。

由上述分析可知,保留第三方可信机构的数据存

储和访问控制决策功能,降低访问决策的复杂性。由区块链记录访问控制过程,保证过程的透明可见性和可审计性。但是存在单点故障、低可扩展性和可否认性的问题。将访问控制策略以智能合约编码的形式存储在区块链,交易触发智能合约执行得到权限,并由各节点验证访问权限,达成共识后将其记录在区块链。访问决策效率偏低,但是能够保障访问控制的安全性和可靠性。

总结现有研究工作存在的问题:(1)维护区块链需要高存储能力和计算能力,难以适应轻量级的设备;(2)所有参与者共同维护单一区块链,交易信息冗杂导致信息检索困难。并且,将资源直接存储在区块链不利于资源的保密性,也会增加区块链的存储负担;(3)过于依赖基于交易的权限验证和更改方式,效率低且细粒度不够。因此,权衡访问控制的安全性和效率,提出一种基于区块链的物联网去中心化的访问控制方案并梳理出需要解决的技术问题。

第一,资源的存储的安全标识。去中心化模式下,节点之间的信任难以保证。为保证资源的安全存储,首先确保参与方身份的真实性。假设所有参与方都需要通过物联网设备作为物理媒介参与到资源的存储和访问控制过程,因此对参与方的身份标识及验证,本质上都是对设备进行身份标识及验证。因此,根据能力对物联网设备进行分层管理,由网关管理与其连接的轻量级物联网设备;其次,采用区块链中的非对称加密体系,为参与方分配公、私钥对,以验证身份真实性。并将资源信息与参与方身份进行绑定,以实现对资源存储的安全标识。

第二,资源存储和访问控制相关信任操作的定义。区块链作为公共账本技术及信任管理机制,将方案中涉及的设备注册、资源存储和资源访问控制作为信任操作。首先,定义信任操作的交易数据结构,构建区块和区块链;其次,根据功能存储到不同的区块链以提高方案的效率。

第三,访问请求的评估和访问权限的获取的流程及可靠性验证。首先,根据区块链的技术特征的优势,设计相关操作的流程及验证过程,例如,策略评估的流程和正确性验证。其次,为了进一步提高访问控制效率,考虑物联网设备的动态性,根据静态和动态划分属性,将静态属性整合为静态属性令牌的数据结构,提高策略的验证速度。

2 方案设计

本节主要工作在于描述方案的模型,参与实体,资源存储和访问控制中的信任操作、区块和区块链的数据结构设计,访问控制流程及验证。

2.1 访问控制模型

基于上述研究,提出基于区块链结合 ABAC 的去中心化访问控制实现层面的模型,如图 2 所示。

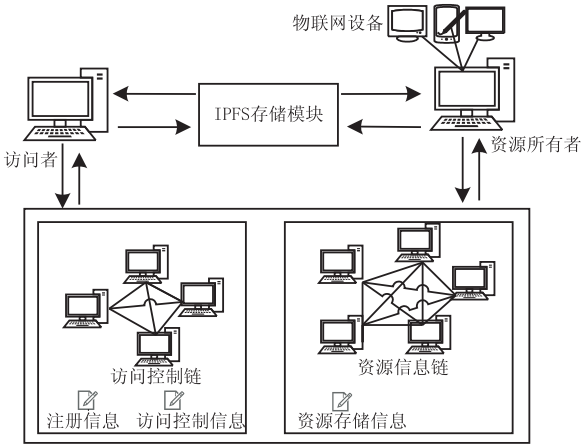


图 2 基于区块链的物联网去中心化访问控制模型

该模型由四类主要实体和两条区块链组成:

(1)资源所有者:也称设备所有者,通常是网关设备,负责管理设备及其数据、处理设备的访问请求、向网络中广播资源消息或访问控制消息。

(2)访问者:发起资源访问请求,在网络中广播访问请求信息,通常也是网关设备。

(3)物联网设备:如智能手环、网关等,负责数据收集、初步处理和传输、请求访问其他设备资源和处理请求操作。该文将设备的属性列举为设备标识、设备类型(读、写)、设备角色(设备管理者、轻量级设备)、时间、地理位置、操作类型。将前三种作为静态属性,后三种作为动态属性。动态属性用来描述主体因环境或操作而改变的属性,例如,访问者地理位置改变且不再符合访问控制策略规则时,无法获得原有的权限。假设静态属性具备稳定性,动态属性由物联网终端设备自动且实时获取。

(4)IPFS 存储模块,这类分布式存储系统通过基于内容的寻址方式来存储和定位资源,返回一个独特的加密哈希字符串 IPFS hash[20]。

(5)资源信息链,记录资源所有者发布的资源消息,任何访问者、资源所有者都可以作为该链的参与方并查找所需资源的信息。访问控制链,由资源所有者作为该链的参与方,参与方之间通过对等网络相互连接,避免中心化访问控制,将访问控制的评估和验证能力下放,摆脱传统信任模式和单点故障带来的影响。利用区块链记录设备的属性信息、访问请求和结果信息,保证访问控制可信及可审计。

双链的设计,将资源存储信息和控制信息分开,有利于资源的查找、策略的查找和访问控制过程的审计。访问控制链的优势有:(1)资源所有者暂时离开区块

链,其他参与方根据已有的策略评估访问请求,并将决策结果记录在区块链,便于资源所有者后期的审查工作,增强模型的可用性;(2)资源所有者作为参与节点共同维护访问控制链,相互监督,提高访问控制的可信和可验证。

将资源信息(公开信息和策略信息)与资源所有者的身份进行绑定,可以实现资源存储的安全标识。首先,与以往研究工作将设备资源加密后直接存储在区块链不同的是,该文将资源加密后的密文存储在IPFS,仅在资源信息链上记录资源的发布消息,有效地减缓了区块链存储压力。资源所有者使用哈希函数对IPFS hash 和资源对应的访问控制策略 policy 得到数字摘要 D_{res}。随后,使用私钥 SK_{own}对 D_{res}数字签名,生成资源存储的安全标识 $sign_{res}$,如式 1。其他参与方使用资源所有者的公钥 PK_{own}验证其身份。

$$sign_{res} = Sign(Hash(IPFShash, policy), SK_{own}) \tag{1}$$

同理,将属性信息和访问者的身份进行绑定,对访问者属性进行可信标识,同时保证属性的不可篡改性和真实性。

2.2　访问控制的数据结构

2.2.1　交易的定义及验证

该文将网络中传播的设备注册信息、资源存储信息和资源访问控制信息分别定义为三种交易。

设备注册交易由设备所有者对管理域内设备的属性信息签名完成。包含设备所有者身份标识 devOwner,设备标识 devId,设备类型 type,设备角色 role,物理位置 loc,设备执行的操作 oper,当前时间戳 timestamp,设备所有者数字签名 sign。

资源策略发布交易由资源所有者对设备产生的资源、资源的访问控制策略签名完成。包含资源链接 IPFShash,资源所有者身份标识 devOwner,是否要求访问者注册 shouldReg,时间的要求 time,地理位置的要求 loc,操作要求 oper,时间戳 timestamp,资源策略发布者数字签名 sign。

访问请求交易由访问者对所请求资源的标识、自身属性集合签名完成。包含资源链接 IPFShash,访问者的身份标识 devId,访问者的设备类型 type,访问者的设备角色 role,访问者的静态属性令牌 staticToken,访问者的地理位置 loc,访问者请求的操作 oper,时间戳 timestamp,访问者数字签名 sign。

前两种交易重点在于验证交易中的数字签名信息,判断策略发布者和设备的身份真实性。在第 2.3 节中重点关注访问请求交易及其验证。

2.2.2　区块和区块链结构

参考比特币系统,区块包含两个部分,区块头中有前一区块的哈希值、Merkle 树根哈希值、时间戳。Merkle 树根哈希值是当前区块体中所有交易进行分组哈希最终得到的根哈希值。对交易的任意更改,都会导致 Merkle 树根哈希值变化,保证数据的不可篡改。时间戳记录区块生成的时间。根据交易数据的不同,交易的类型不同,参与节点将验证通过的交易放到本地交易池中,当交易池中的交易达到一定数量时,选择多笔交易组装成区块,如图 3 所示。

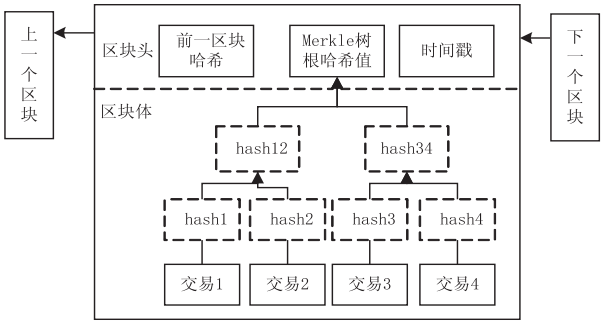


图 3　区块及区块链数据结构

由共识机制保证各参与节点的区块链公共账本上的数据一致性。常见的是工作量证明、权益证明以及实用拜占庭容错(Practical Byzantine Fault Tolerance,PBFT)等共识机制[21],该文不展开关于共识机制的具体研究。根据物联网环境的特性及访问控制所需的一定实时性,选定具有高性能且耗能低的 PBFT 共识机制。假设区块链参与节点总数是 $3f+1$,那么网络中容忍最多 f 个节点出现错误而不影响正确的共识。区块链中的所有交易都被认为是可信的、不可篡改的。

图 4 表示参与方与区块链交互的过程,资源所有者将网络中的设备注册交易和访问请求交易进行验证和打包记录到访问控制链。资源所有者和访问用户维护资源信息链,访问用户可以查询所需资源信息,并发布访问请求交易。

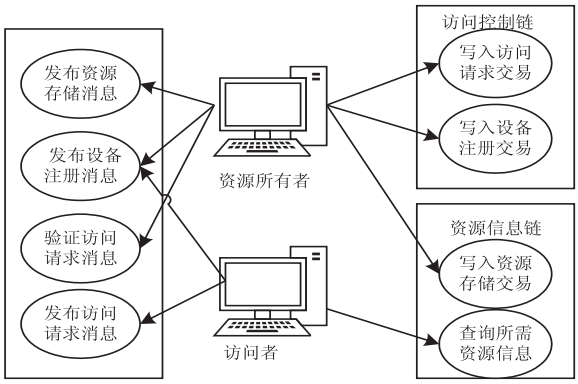


图 4　参与方与区块链交互的过程

2.3　访问控制流程及验证

访问控制的功能是正确处理访问请求并得到对应的访问权限。为了保证访问控制的可信和正确性,需要验证访问者身份真实性、访问请求中参数真实性、访

问请求评估正确性。验证过程中的交易字段参考 2.2.1 中的数据结构,访问者公私钥对(PK_{acc}, SK_{acc}),资源所有者公私钥对(PK_{own}, SK_{own})。步骤如下:

步骤 1:访问者提交与设备注册交易相关的字段,对设备进行注册。访问者使用哈希算法对设备注册相关字段进行计算并进行数字签名,如式 2。对设备的静态属性信息进行哈希计算得到静态属性令牌 staticToken,如式 3。

$$sign_{acc\_reg} = Sign(Hash(devId, type, role, loc, oper), SK_{acc}) \quad (2)$$

$$staticToken = Hash(devId, type, role) \quad (3)$$

步骤 2:资源所有者根据访问者的注册消息,验证访问者的身份。访问者的 PK_{acc} 验证 $sign_{acc\_reg}$,Verify()返回 true 则表明注册信息是真实可信的,如式 4。资源所有者构建设备注册交易,并记录到访问控制链。

$$\{true, false\} = Verify(Hash(devId, type, role, loc, oper), sign_{acc\_reg}, PK_{acc}) \quad (4)$$

步骤 3:访问者提出访问请求,使用哈希函数计算访问请求字段的数字摘要并数字签名,如式 5。

$$sign_{acc\_req} = Sign(Hash(IPFShash, devId, type, role, loc, oper), SK_{acc}) \quad (5)$$

步骤 4:资源所有者收到访问请求消息,根据访问者的身份标识(区块链账户地址)在访问控制链中找到对应的设备注册交易,使用式 3 对访问请求中的静态属性进行哈希计算得到 D_{static},若 D_{static} 和 staicToken 相同则表明访问请求中静态属性的真实性,如式 6,避免逐一验证频繁的访问请求。

$$\{true, false\} = Equal(D_{static}, staticToken) \quad (6)$$

步骤 5:资源所有者根据访问请求中资源链接找到访问控制策略,以算法 1 提出的访问控制策略为例对访问请求的评估过程进行说明。

首先说明算法中策略的数据结构,比较了访问控制表、逻辑表达式和访问树的表达方式后,选择在访问树中引入多项式函数的策略表达方法。多项式函数最高指数为非叶子节点阈值减 1,其他自变量前的系数为随机数,常数项为节点值。根据父节点的多项式,得到孩子节点的值。将策略中的静态属性要求构建为左子树,动态属性要求构建成右子树。接下来,将以图 5 中的访问树为例进行说明。

如果访问请求中的静态属性满足策略中静态属性需求,则返回左子树阈值个数的节点键值对(叶子节点索引,叶子节点值),随后通过式 7 计算,得到左子树根节点值。同理,获得右子树根节点值,最终得到根节点值,则表明访问请求中的操作被授权。资源所有者将资源的解密密钥和对应操作权限打开,并发送给访问者。

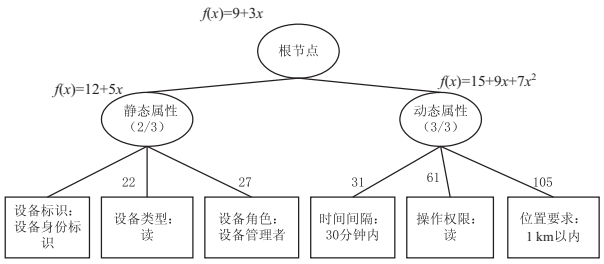


图 5 访问树示例

$$F(x) = \sum_{i=1}^{n} y_i \left(\prod_{j \neq i}^{1 \leqslant j \leqslant n} \frac{(x - x_j)}{(x_i - x_j)} \right) \quad (7)$$

算法 1:访问请求评估算法

输入:IPFShash, devId, type, role, loc, oper, devOwner, staticToken

输出:访问权限 allowed/deney/errorMsg

```
1:for(i=0;i<devOwner.devices.length;i++)
2: if(devOwner.devices[i].devId ===devId)
3:  devInfo = devOwner.devices[i] //找到设备注册信息
4:for(i=0;i<resources.length;i++)
5: if(resources[i].IPFShash ===IPFShash)
6:  py = resources[i].policy //资源策略信息
7:if(py.shouldReg)//策略要求设备需注册
8:   if(staticToken) //静态令牌存在
9:    flag=Equal(staticToken,Hash(devId,type,role))
10:    if(flag)
11:   Get(staticRootIndex,staticRootSecret)
12:    else
13:   return erroMsg //静态属性令牌不正确
14:  else  //静态令牌不存在,逐一比较
15:staticNum = getTrueNumber(devInfo.devId===devId,
devInfo.type===type,devInfo.role ===role)
16: if(staticNum >= staticThreshold) //检查静态属性
17:  Get(staticRootIndex,staticRootSecret)
18: else
19:   return errorMsg
20:dynamicNum=getTrueNumber(py.loc===loc,py.oper=
==oper, py.time < timestamp)
21: if(dynamicNum >= dynamicThreshold)//检查动态属性
22:   Get(dynamicIndex, dynamicRootSecret)
23: else
24:   return errorMsg
25:if(staticRootSecret && dynamicRootSecret)
26:   Get(rootSecret)
27:   return allowed
28: else
29:   return deny
```

访问控制链的其他参与节点可以以同样的方式对访问请求中的属性进行验证。也可以信任其他节点验证得到的(叶子节点索引,叶子节点值)利用式 7 计算根节点的值,从而与其他节点达成一致。

3　安全性分析和仿真实验

分析方案抵抗密文和共谋攻击的能力,基于以太坊平台进行了相应的实验来证明方案的可行性,并对属性划分提高访问控制效率进行性能分析。

3.1　安全攻击

密文攻击,是未授权用户获得了密文之后,在区块链中查找不到其对资源的访问请求交易,无法获得相应的访问权限,便无法得到所需的解密密钥。

共谋攻击,指不同用户之间试图通过属性组合实现最终授权。首先,设备的静态属性都是默认在很长一段时间内不会改变,一般不会有设备为了满足某一个访问控制策略而捏造其静态属性,且区块链中的设备注册信息难以篡改。其次,动态属性的获取是通过设备传感器实时上传的,上传过程不会被更改。因此设备的属性一定是真实的,且同属于一个设备。设备注册交易中的签名若无法使用设备所有者的公钥验证,则表明注册信息是虚假的、无法验证的。

3.2　仿真实验和模拟

建立以太坊私有链网络,模拟真实应用环境。实验目的是设计资源访问控制智能合约实现物联网设备的注册、资源访问控制策略的发布、资源的访问请求。其中,react 技术开发用户前端界面,truffle 框架部署和测试智能合约。合约部署成功如图 6。

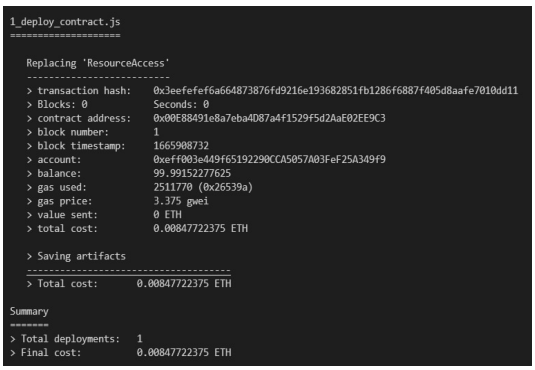


图 6　访问控制智能合约部署情况

设备注册的目的是保证物联网设备属性信息的真实性,如图 7。设备注册消息的签名和时间戳由系统自动生成。访问控制策略发布,目的是为资源制定访问控制策略,前端界面与图 7 类似。

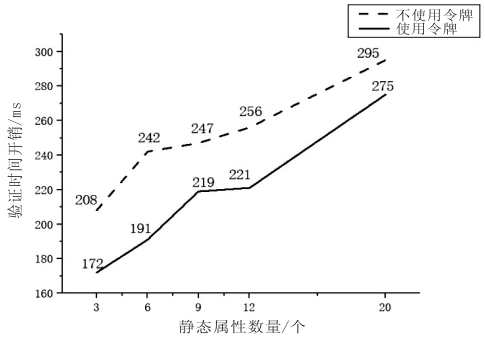
图 7　注册物联网设备

访问请求,目的是对物联网设备的属性真实性进行验证,评估属性与策略的匹配程度,并得到权限。以请求成功为例,如图 8。

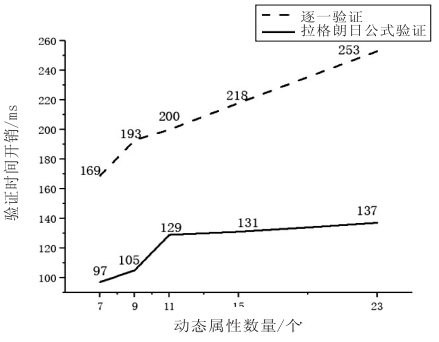
图 8　访问请求成功的情况

3.3　性能分析

策略中属性的个数会影响访问控制的效率,根据属性的划分带来的静态属性令牌和访问树的方法。从两个角度切入进行了性能分析:第一,固定动态属性的个数和访问数的验证方法,探讨随静态属性个数的增长,静态属性令牌对效率的影响。从图 9(a)可以发现静态属性令牌减少逐一验证,减少策略评估和权限验证的时间开销。第二,固定静态属性令牌验证方法,探讨随动态属性个数的增长,访问树的验证方法和拉格朗日函数直接验证方法对效率的影响。从图 9(b)可以发现其他节点使用第二种验证方法的时间开销较少。



(a)验证静态令牌功能



(b)验证拉格朗日函数功能

图 9　影响访问请求验证时间开销的因素

实验中所有的数值都是程序的执行时长,该时长通常与执行环境有关,同样的程序在不同时间段执行会存在 10 ms 左右的误差,进行了近 20 次的实验,最终采用 20 次实验执行时长的平均值。

上述实验验证了方案的可行性和正确性,确保了访问控制过程的透明可信,有效地防止资源的未授权访问和滥用,提高了访问请求评估速度和权限验证速度。实验是在本地测试网络中进行,正式应用需要根据真实网络环境做相应的调整。

4 结束语

该文提出一种基于区块链的物联网资源访问控制方案,充分利用区块链技术、IPFS 和 ABAC 的技术特征以保证资源的安全存储和可信管理。通过交易管理用户、属性、策略和访问行为,管理和追踪策略的发布、评估和权限验证,有利于以资源所有者为中心管理资源的存储和使用。通过属性划分的方法,研究访问请求全过程的评估和验证方法,以提高访问控制评估和权限验证的速度。仿真实验证明了方案的可信性和正确性,今后会从共识机制的角度,研究访问控制效率提升的方法。

参考文献:

[1] ZHANG W, YAN H. A blockchain-based access control scheme for smart home[J]. Journal of Physics: Conference Series, 2021, 1971(1): 012049.

[2] KASHANI M H, MADANIPOUR M, NIKRAVAN M, et al. A systematic review of IoT in healthcare: applications, techniques, and trends[J]. Journal of Network and Computer Applications, 2021, 192: 103164.

[3] GÜRFIDAN R, ERSOY M. A new approach with blockchain based for safe communication in IoT ecosystem[J]. Journal of Data, Information and Management, 2022, 4(1): 49-56.

[4] 张建国. 基于区块链智能合约的物联网设备访问控制研究[D]. 兰州: 兰州交通大学, 2020.

[5] RIABI I, AYED H K B, SAIDANE L A. A survey on Blockchain based access control for Internet of Things[C]//2019 15th international wireless communications & mobile computing conference (IWCMC). Tangier: IEEE, 2019: 502-507.

[6] FERRAG M A, SHU L. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: a tutorial[J]. IEEE Internet of Things Journal, 2021, 8(24): 17236-17260.

[7] QIN X, HUANG Y, YANG Z, et al. An access control scheme with fine-grained time constrained attributes based on smart contract and trapdoor[C]//2019 26th international conference on telecommunications (ICT). Hanoi: IEEE, 2019: 249-253.

[8] SHEN H, LIU S. A context-aware capability-based access control framework for the Internet of things[J]. Journal of Wuhan University (Natural Science Edition), 2014, 60(5): 424-428.

[9] 沈苏彬, 毛燕琴, 李 莉. 一种面向非数字货币的区块链通用应用方案[J]. 南京邮电大学学报: 自然科学版, 2019, 39(1): 1-11.

[10] BUTERIN V. Ethereum Yellow Paper[EB/OL]. [2022-10-24]. https://ethereum.github.io/yellowpaper.

[11] 李 铭, 沈苏彬. 一种基于区块链的自媒体版权管理方案[J]. 计算机技术与发展, 2023, 33(1): 206-213.

[12] KSHETRI N. Can blockchain strengthen the internet of things?[J]. IT Professional, 2017, 19(4): 68-72.

[13] HU B, CHEN Y, YU H, et al. Blockchain enabled data sharing scheme for consumer IoT applications[J]. IEEE Consumer Electronics Magazine, 2021, 11(2): 77-87.

[14] 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.

[15] DI FRANCESCO MAESA D, MORI P, RICCI L. Blockchain based access control[C]//Distributed applications and interoperable systems: 17th IFIP WG 6.1 international conference, DAIS 2017, held as part of the 12th international federated conference on distributed computing techniques, DisCoTec 2017. Neuchâtel: Springer, 2017: 206-220.

[16] 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.

[17] XU R, CHEN Y, BLASCH E, et al. Blendcac: a smart contract enabled decentralized capability-based access control mechanism for the iot[J]. Computers, 2018, 7(3): 39-66.

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

[19] XU Q, SONG Z, GOH R S M, et al. Building an ethereum and ipfs-based decentralized social network system[C]//2018 IEEE 24th international conference on parallel and distributed systems (ICPADS). Singapore: IEEE, 2018: 1-6.

[20] DANIEL E, TSCHORSCH F. IPFS and friends: a qualitative comparison of next generation peer-to-peer data networks[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 31-52.

[21] 田志宏, 赵金东. 面向物联网的区块链共识机制综述[J]. 计算机应用, 2021, 41(4): 917-929.