



基于以太坊的改进物联网设备访问控制机制研究

张建国, 胡晓辉

(兰州交通大学 电子与信息工程学院, 兰州 730070)

摘要:当前物联网设备节点动态性强且计算能力弱,导致物联网中的传统访问控制机制存在策略判决与策略权限管理效率较低、安全性不足等问题。提出基于以太坊区块链的物联网设备访问控制机制,结合基于角色的访问控制(RBAC)模型设计智能合约。对以太坊相关特性进行分析,建立结合用户组的改进RBAC模型。设计基于以太坊区块链技术的物联网设备访问控制架构及算法,通过编写图灵完备的智能合约实现物联网设备访问控制,融合以太坊区块链MPT树存储结构与星际文件系统对访问控制策略进行存储管理。在以太坊测试链上的实验结果表明,该机制具有较高的策略判决性能与安全性。

关键词:区块链;以太坊;智能合约;基于角色的访问控制模型;物联网设备;访问控制

开放科学(资源服务)标志码(OSID):



中文引用格式:张建国,胡晓辉.基于以太坊的改进物联网设备访问控制机制研究[J].计算机工程,2021,47(4):32-39,47.

英文引用格式:ZHANG Jianguo, HU Xiaohui. Research on improved access control mechanism of internet of things devices based on ethereum[J]. Computer Engineering, 2021, 47(4): 32-39, 47.

Research on Improved Access Control Mechanism of Internet of Things Devices Based on Ethereum

ZHANG Jianguo, HU Xiaohui

(School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China)

[Abstract] The high mobility and weak computation capabilities of Internet of Things(IoT) device nodes lead to some problems in the traditional access control mechanism of IoT, including low security, and inefficient management of policy decision and policy permissions. To address the problems, this paper proposes an access control mechanism for IoT devices based on Ethereum blockchain, and a smart contract designed by using the Role-Based Access Control (RBAC) model. First, this paper expounds the features of Ethereum and proposes an improved RBAC access control model combined with user groups. Then it designs the access control architecture and algorithm for IoT devices based on Ethereum blockchain technology, and writes Turing-complete smart contracts to realize access control for IoT devices. The storage structure of Ethereum blockchain MPT tree and InterPlanetary File System (IPFS) are used to store and manage access control strategies. The test results on the Ethereum test chain verify high security and policy decision performance of the proposed mechanism.

[Key words] blockchain; Ethereum; smart contract; Role-Based Access Control (RBAC) model; Internet of Things (IoT) devices; access control

DOI: 10.19678/j.issn.1000-3428.0057729

0 概述

随着科技水平的不断提高,物联网已经能够在任何时间和地点实现不同角色之间的有效连接,这也使得物联网设备数量大幅增加。大量的物联网设备将会产生海量的隐私数据,这部分数据信息一旦泄漏,会给用户造成巨大损失^[1]。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对特定设备的操

作^[2-3]。具备相应操作权限的用户只有通过访问控制机制才能访问隐私数据,从而保障了数据安全。因此,访问控制机制成为物联网领域的研究热点之一^[2]。在物联网中进行访问控制,可以有效防止用户未经授权就访问系统资源,也能防止已经被授予某些权限的用户通过其他未经授权的方式来访问资源,以及允许用户在被授予相关权限后通过授权方式访问资源。此外,访问控制机制通过阻止某些不良行为以避免可能发生的安全漏洞问题。

基金项目:国家自然科学基金(11461038);甘肃省科技支撑计划项目(144NKCA040)。

作者简介:张建国(1993—),男,硕士研究生,主研方向为分布式计算、区块链技术;胡晓辉(通信作者),教授、博士。

收稿日期:2020-03-16 **修回日期:**2020-04-22 **E-mail:** lzjtuzjg@163.com

访问控制机制需满足完整性、机密性及可用性的安全需求^[4]。传统的物联网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^[5-7]和基于属性的访问控制(Attribute-Based Access Control, ABAC)模型^[8-9]。在RBAC模型中,角色和权限相关联,系统将相应的角色赋予用户以使用户拥有相应的权限,从而保证了物联网环境的跨域访问控制^[5]、可扩展性^[6]及设备的异构性^[7]。但是, RBAC是一种静态机制,不能提前设定{用户, 角色}、{角色, 权限}的对应关系,因此,其不能有效解决物联网节点的动态接入问题。ABAC将属性作为处理访问控制问题的关键,通过实体属性的发现机制得到独立且完备的主体与客体等属性集合,管理者无需手工输入,可以通过自动化的发现机制快速得到{属性, 权限},因此, ABAC是一种动态机制,其能够很好地解决由移动节点和变化的访问数据引起的动态接入问题^[9]。

但在上述访问控制机制中,通常由集中实体对主体的访问权限进行验证,导致极易发生单点故障问题。为此,研究人员提出了基于权能的分布式访问控制(CapBAC)模型机制^[10-11],其由发生请求的物联网对象自身执行访问权限的验证。但是,物联网设备极易受到攻击,它们不完全具备访问权限验证的能力。因此, CapBAC模型机制难以解决存疑物联网环境中的访问控制问题。

近年来,区块链技术^[2]受到各领域研究人员的广泛关注与研究。区块链技术将P2P网络、加密算法、共识机制和智能合约等多种技术方法相结合,以解决去中心化节点间存在的信任问题,建立去中心化、不可篡改、可追溯的信任机制,同时完成价值转移和信息传输^[12-13]。在区块链中,用户身份通过其密钥来证明,节点可以在任意时间和地点连接到区块链网络,只要节点的签名正确就能进行操作。此外,区块链采用了P2P的网络架构,一旦有用户节点请求接入网络,仅需连接到网络中的其他节点即可。由于区块链的P2P网络结构同节点间的地理位置无关,因此节点仅需选择网络中已经存在的区块链节点相连。对于节点移动、频繁接入和退出等问题,区块链利用自身的特性就可以解决,即分布式的区块链架构与分布式的物联网系统和动态访问控制需求相适应^[14]。以太坊区块链具备图灵完备的以太坊虚拟机,能够执行任意复杂算法的智能合约^[3],使用智能合约来实现复杂算法,从而解决传统访问控制机制因物联网设备计算能力较弱导致策略判决效率低的问题。另外,以太坊区块链的不可篡改性也使策略存储得到保障。

本文针对物联网设备的访问控制问题,基于区块链的事务管理和智能合约技术,实现对分布式环境下物联网设备动态、灵活、高效及安全的访问控制。将以太坊区块链技术与改进的RBAC模型相结合,提出一种基于以太坊区块链的物联网设备访问控制机制,通过编写图灵完备的智能合约来实现复杂算法从而进行物联网设备的访问控制。设计一种星际文件系统(IPFS)与以太坊区块链相结合的策略数据存储方案,以提高访问控制数据的安全性。

1 相关工作

1.1 以太坊区块链技术

区块链是一种新型的分布式计算机技术、以加密算法为基础的点对点传输的分布式账本技术以及网络化的去中心共享数据库技术。在区块链中,利用加密算法实现价值的转移,通过时间戳机制和散列链保证数据的可追溯、不可篡改特性,依据共识算法提高节点间区块数据的一致性,使得基于信任的中心化机制所存在的安全性问题得到有效解决。

以太坊^[15]是建立在区块链技术基础上的一个去中心化应用平台,其网络架构完善且具有较高的鲁棒性。以太坊是可编程的区块链,允许用户自定义复杂的操作。以太坊虚拟机(Ethereum Virtual Machine, EVM)是以太坊中智能合约的运行环境,也是以太坊的核心。以太坊是图灵完备的,因此, EVM可执行任意复杂算法的程序编码。此外,以太坊区块链数据库由其网络中的每个节点来进行更新与维护,每个节点均可通过运行以太坊虚拟机来执行相同的指令,从而保证了区块链的一致性。智能合约一旦部署到以太坊的网络中就失去了再被修改的机会,这种设计大幅提高了以太坊平台网络上智能合约的可信性,且在以太坊平台上可以使用多种高级语言来进行智能合约编写。以太坊区块链逻辑架构如图1所示。

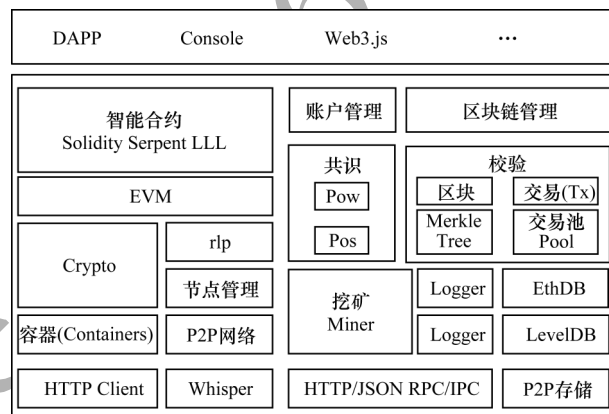


图1 以太坊区块链逻辑架构

Fig.1 Ethereum blockchain logical architecture

1.2 智能合约技术

智能合约^[16-17]是运行在区块链平台上、具有状态机、通过事件驱动并得到多方认可的计算机程序。以太坊区块链的智能合约具备数据透明、不可篡改和永久执行的特性。数据的处理在智能合约中公开透明,部署在区块链上的智能合约代码以及执行结果不可篡改,智能合约的运行节点无需担心其他恶意节点会修改程序及数据,区块链网络由大量的节点组成,部分节点出现故障无法致使智能合约停止运行,因此,在理论上智能合约可靠性稳定且能永久运行。物联网设备的计算能力较低以及资源储存能力受限,导致其不能很好地满足访问控制的需求。以太坊区块链具备图灵完备的以太坊虚拟机,能够执行任意复杂算法的智能合约^[3],因此,使用智能合约来实现复杂算法可以进行物联网

设备的访问控制。

1.3 基于角色的访问控制方法

RBAC模型最初被用来解决大型企业级系统存在的访问控制问题,其通过将角色和一组权限相关联,系统给予用户相关的角色从而促使用户获取对应的权限。随着物联网在多个领域的不断发展, RBAC逐渐被学者引入到物联网的访问控制研究中^[6], RBAC可以支持物联网生态的可扩展性、设备的异构性和跨区域的访问控制等相关特性。

RBAC根据权限的复杂程度又可分为RBAC0、RBAC1、RBAC2和RBAC3。本文通过将RBAC1与用户组相结合,即对角色进行分级并添加用户组,以实现更加细粒度的权限管理。具体如下:

1)角色分级:在RBAC模型中,本文将权限赋予角色再将角色赋予用户。将角色分成若干等级,每个等级的权限不同,使得角色更加细粒度化,如图2所示。

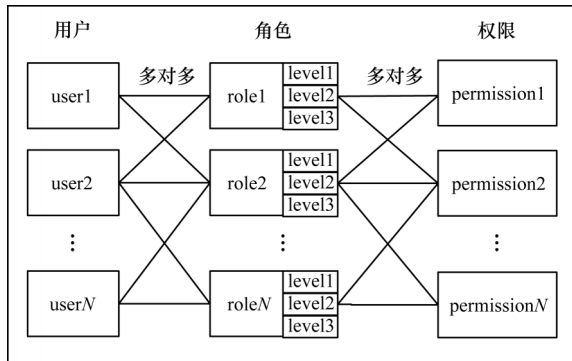


图2 角色分级

Fig.2 Role rating

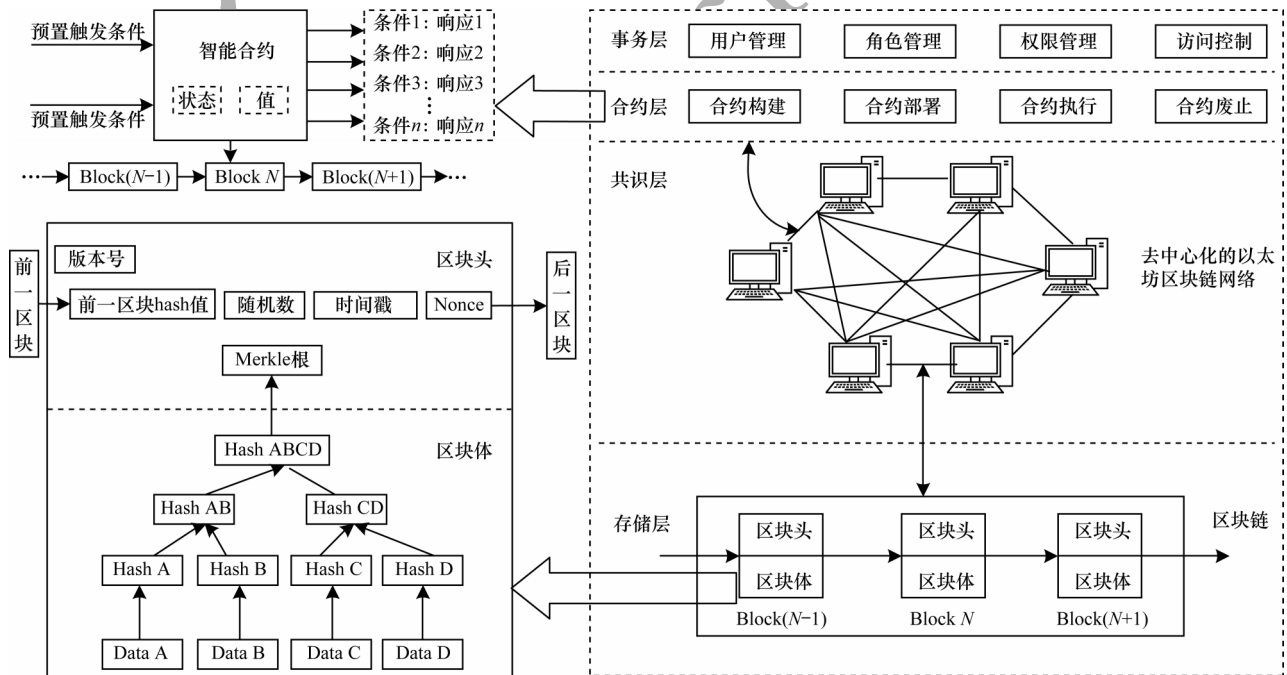


图4 物联网设备访问控制技术架构

Fig.4 Access control technology architecture for IoT devices

2)用户组,如图3所示,本文引入用户组的概念,直接给用户组分配角色,再将用户加入用户组。用户除了自身的权限外,还拥有所属用户组的所有权限。当用户的数量非常大时,系统通过给用户组授权来避免每个用户逐一授权而引起的资源占用问题。

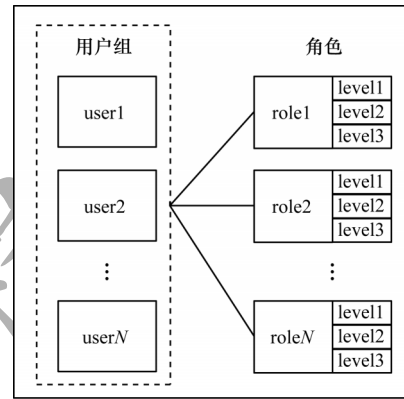


图3 用户组

Fig.3 User groups

2 系统整体架构及设计

2.1 物联网设备访问控制技术架构

基于以太坊区块链技术的物联网设备访问控制包括访问策略事件发布、事件存储和事件的合约验证等。本文物联网设备访问控制架构主要由存储层、共识层、合约层和事务层组成,各层相互协同,共同构成一个完整的物联网设备访问控制架构,如图4所示。

物联网设备访问控制技术架构各层具体如下：

1)存储层:将访问控制策略发送到各节点,并封装在各区块中,区块间以链式结构相连接,实现访问控制策略安全、可追溯及对所有人透明。

2)共识层:封装网络节点的各类共识机制算法。共识机制算法是区块链技术的核心,其决定了记账者,记账者的选择影响整个系统的安全性和可靠性。

3)合约层:智能合约对用户角色进行分配,然后将其发布在区块链上,可提高用户的匿名性同时确保所创建角色及权限的透明性。访问控制合约具有4个功能,一是允许策略管理组织添加用户并向用户发布角色和权限及其他相关信息,二是允许策略管理组织以所有人可见的方式根据需要管理和修改角色信息及权限,三是允许策略管理组织根据需要撤销用户及发布给用户的角色和权限,四是允许策略管理组织根据需求废止合约。

4)事务层:该层位于最上层,通过 ABI 与智能合约进行交互。事务层首先进行用户管理,声明拥有角色的用户;然后实现角色管理,检查与角色有关的信息;接着进行角色-权限管理,声明拥有权限的角色;最后实现访问控制管理,完成权限对用户的响应。

2.2 访问控制合约

2.2.1 合约执行框架及流程

访问控制合约框架基于以太坊区块链技术并将以太坊区块链与改进后的 RBAC 模型相结合,该框架包括用户、角色集、权限集、策略管理、智能合约及资源拥有者,访问控制工作流程可分为准备和执行2个阶段。准备阶段主要进行用户、角色及访问控制策略的管理,包括用户、角色及策略的添加、更新、删除以及对角色及策略查询结果的响应。执行阶段主要对访问请求进行判决、响应及执行。访问控制合约执行框架如图 5 所示。

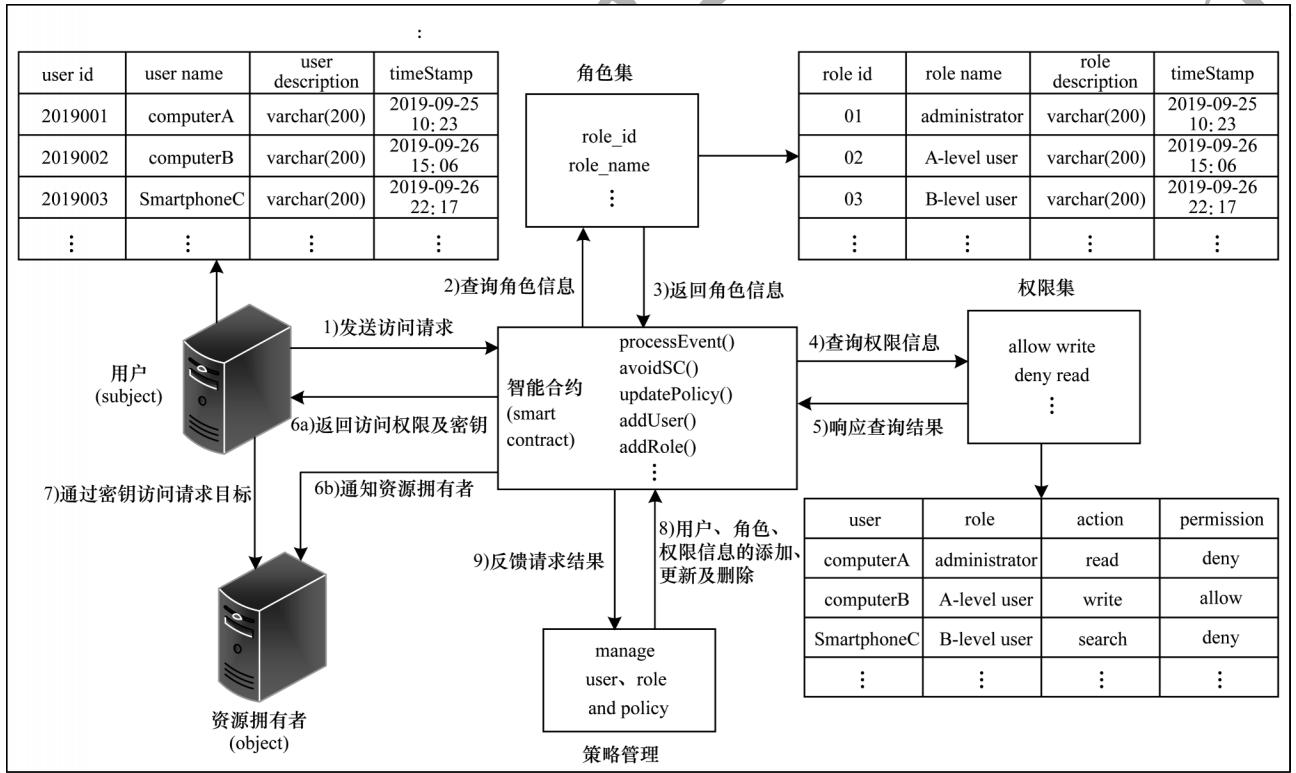


图 5 访问控制合约执行框架

Fig.5 Access control contract execution framework

准备阶段具体如下：

1) 由用户发送访问目标资源拥有者的请求,智能合约通过 ABI 接收用户请求并根据请求内容作出响应。

2) 智能合约通过 processEvent() 方法查询对应的用户-角色信息。

3) 一旦查找完成便返回该用户具备的角色信息到智能合约。

4) 智能合约的 processEvent() 方法通过返回的角色信息访问权限集,查找该角色信息具备的权限

等级。

5) 根据查找到的对应的角色-权限作出响应并返回响应结果到智能合约。

6) 根据策略管理的变动,包括添加新用户、删除已有用户,添加、更新、删除角色信息,添加、更新、删除权限信息,策略管理模块通过 ABI 访问智能合约。

7) 智能合约根据请求内容调用内部相关方法,完成策略管理模块的请求并通过以太坊区块链网络向全网节点广播,最后将响应结果反馈到策略管理模块。

执行阶段具体如下:

1) 智能合约通过 `processEvent()` 方法返回权限及密钥到用户,同时通知资源拥有者以便其根据用户的密钥进行识别。

2) 用户在得到智能合约授予其的相应权限之后立即向资源拥有者发送访问请求,并通过密钥进行身份认证从而访问资源拥有者。

2.2.2 访问控制合约策略判决算法

访问控制的判决结果分为允许访问(allow)和拒绝访问(deny)2种类型。针对访问主体(subject)相应的权限访问请求,遍历用户集(user_set)、角色集(role_set)和权限集(policy_set)中相应的信息,若满足某一访问控制策略中的信息,则判决为允许访问(allow)。如果判决请求不满足策略,则包括2种情况:一是用户集(user_set)、角色集(role_set)和权限集(policy_set)中不具备相应信息,从而无法进行判决,此时使用undefined表示,判决为deny;二是策略集中拒绝访问主体进行相应权限访问,此时判决为deny。访问控制策略判决算法描述如算法1所示。

算法1 访问控制策略判决算法

输入 用户集(user_set),角色集(role_set),权限集(policy_set)

输出 相应权限(allow或deny)

```

1. 部署智能合约并调用 start();
2. 设置 temp_user = null; temp_role = null; temp_policy = null;
3. 设置 allow_result_set = null; deny_result_set = null;
4. if 访问请求主体(subject) from user_set then
5. for i = 1 to role_set.length do
6. if role_set[i] = true then temp_role = role_set[i];
7. for j = 1 to policy_set.length do;
8. if policy_set[j] = true then temp_policy = policy_set[j];
9. if temp_policy = allow then
10. allow_result_set.add (user, temp_role, temp_policy);
11. else if temp_policy = deny then
12. deny_result_set.add (user, temp_role, temp_policy);
13. else if policy_set[j] = undefined then
14. deny_result_set.add (user, temp_role, temp_policy);
15. else if role_set[i] = undefined then
16. deny_result_set.add (user, temp_role, temp_policy);
17. else if 访问请求主体(subject) 不属于用户集(user_set)
then
18. deny_result_set.add (user, temp_role, temp_policy);
19. if allow_result_set != null then
20. return allow;
21. else if deny_result_set != null then
22. return deny;
23. end;
```

访问控制策略判决算法步骤如下:

1) 将访问主体存放于 temp_user,作为临时用户。
2) 遍历系统用户集 user_set,如果访问主体存在于用户集,则进行下一步;否则,返回访问主体为未定义用户(undefined),将访问主体存放于拒绝访问

结果集 deny_result_set 中,判定为无相应访问权限(deny)。

3) 根据主体在用户集中的用户定义,在角色集 role_set 中查询相应的角色。如果该访问主体对应角色存在,则进行下一步;否则,得出访问主体用户未定义角色(undefined),将访问主体存放于拒绝访问结果集 deny_result_set 中,判定为无相应访问权限(deny)。

4) 通过角色信息遍历权限集 policy_set,如果在相应的权限,则将访问主体存放于允许访问结果集 allow_result_set 中,判定为具备相应访问权限(allow);否则,将访问主体存放于拒绝访问结果集 deny_result_set 中,判定为无相应访问权限(deny)。

2.3 访问控制策略存储管理

2.3.1 策略存储方案

本文设计一种 IPFS 和以太坊区块链相结合的策略数据安全存储方案。在该方案中,物联网设备访问控制策略数据以分布式方式通过链下的 IPFS 进行存储,实体可以通过区块链上的地址密钥找到存储地址从而实现对策略数据的访问。策略数据地址哈希由多数区块链矿工控制,防止未授权用户通过地址哈希非法访问存储于 IPFS 中的策略数据。

IPFS 是一种内容可寻址的对等超媒体分发网络传输协议,其目的是实现持久、分布式的文件存储与共享。在 IPFS 网络中,所有节点构成了一个分布式的文件系统,没有节点能够拥有单独的权利。IPFS 采用的索引结构是分布式哈希表(Distributed Hash Table, DHT),采用的数据结构是默克尔有向无环图(Merkle DAG),并用基于内容的地址替代基于域名的地址,无需验证发送者的身份,只需验证内容的哈希。使用内容寻址的方法是 IPFS 与传统存储系统的重要区别,即 IPFS 对文件内容进行哈希运算(Hash),并将 Hash 值用作文件内容的索引地址。存储在 IPFS 中的任何一个数据文件均被分配了一个根据其内容创建的唯一 Hash 值,由于文件的内容不相同,因此哈希值均不同。哈希函数的唯一性和不变性使得用 Hash 代表数据更加合理。

在 IPFS 的整个网络集群中,不允许存在内容相同的文件,且每一个文件都有一个独立的版本管理。根据历史信息均可轻易找到每个文件,因为随着 IPFS 系统中文件的变更,会产生相应的历史记录。当用户对一个文件进行查找时,IPFS 集群节点就会根据查找请求以及 Hash 值来查找文件内容,并且由于 Hash 值唯一,因此文件能够被快速找到。综上,将 IPFS 分布的网络集群系统用于分布式数据安全存储具有合理性。

在以太坊区块链中,使用事务的形式来对 IPFS 哈希进行存储管理。数据存储层将各节点发出的数据封装在以链式结构相连接的各个区块中,结合以太坊区块链去中心化、不可篡改、可追溯的特性,从而满足访问控制策略的安全性要求。MPT 树是以

以太坊区块链中存储区块数据的核心数据结构,是以太坊区块链用来组织管理账户数据及生成交易集合哈希的重要数据结构。MPT树可确保以太坊区

块链中的数据满足不可篡改性,使访问控制策略的安全性得到保证。策略数据存储方案结构如图6所示。

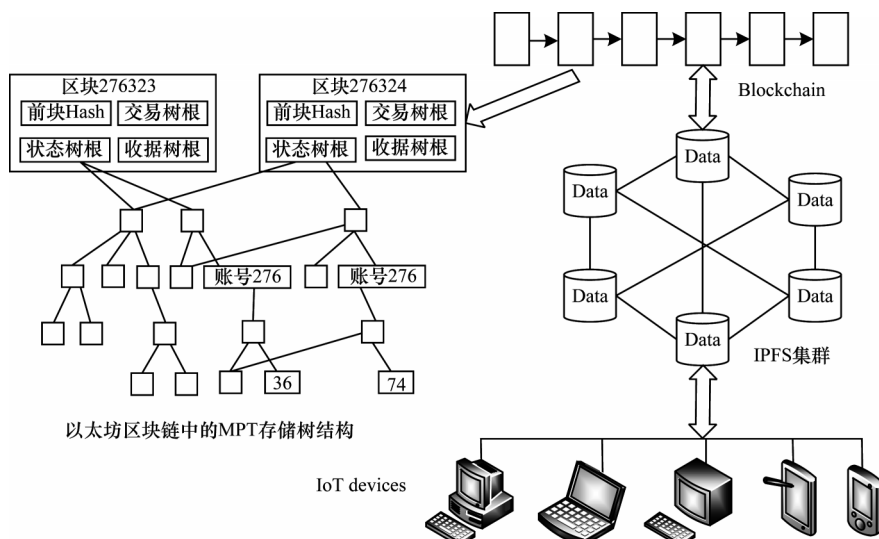


图6 策略数据存储方案架构

Fig.6 Architecture of policy data storage scheme

2.3.2 策略存储算法设计

物联网设备访问控制策略存储后将面临安全问题,为了提高策略管理过程中的安全性,本文设计结合IPFS与以太坊区块链MPT树的策略存储算法,其描述如算法2所示。

算法2 策略存储算法

输入 策略文件(policy_file)

输出 策略哈希地址(hash address)

1.begin

2.if policy_file not exist then

3.while policy_file 请求存储 then

4.create structure data for policy_file;

5.policy_structure_file {id,address,time};

6.while t policy_structure_file = true then

7.将 policy_structure_file 存储于 IPFS;

8.create hash value;

9.while the hash value of policy_structure_file passed then

10.return hash value;

11.Web3.toHex('hash value');//将 hash value 转换为 16 进制字符串存储于以太坊区块链中;

12.return hash address;

13.else

14.policy_file is exist,no need to save;

15.end;

策略存储算法步骤如下:

1)遍历已存储的策略事务数据块,检查待存储策略文件是否已经存储,如果已存储,则退出;否则,进入下一步。

2)创建策略事务数据块 policy{id,address,time}。

3)策略事务数据块创建成功,则将策略事务数

据块存储于IPFS并生成对应的哈希值(hash value),检查哈希值并返回该值。

4)使用 Web3.toHex()方法将哈希值转换为16进制字符串的哈希地址(hash address),将哈希地址以事务形式存放于以太坊区块链中,以便安全访问策略事务数据。

3 实验结果与分析

通过实验对本文所提基于以太坊区块链的物联网设备访问控制机制的有效性及其安全性进行测试。基于XACML提供的标准策略一致性测试包中的属性集和策略集,按照常规方法在PC机上构建拥有3个节点的以太坊区块链测试链仿真环境。实验环境如下:操作系统为Windows 10企业版64位,CPU为Intel® Core™ i7-5960X @ 3 GHz,内存大小为16 GB,Node.js版本为v12.9.1,npm版本为6.10.2。

3.1 有效性分析

为了验证本文访问控制机制的有效性,采用文献[18]中的方法,在不同的策略下对本文结合RBAC模型和智能合约的访问控制策略、RBAC策略、ABAC策略及CapBAC策略的裁决进行有效性测试对比,测试内容为访问控制机制中策略裁决的效率,实验结果如图7所示,实验中5组测试集样本分别对应1 000条、2 000条、3 000条、4 000条和5 000条单一策略。测试集样本面向100个用户标识构建1 000次不同的访问请求,每个标识均具有5个属性值,每个请求有5次随机发送的机会,策略裁决时延根据所有请求平均响应时延计算得到。

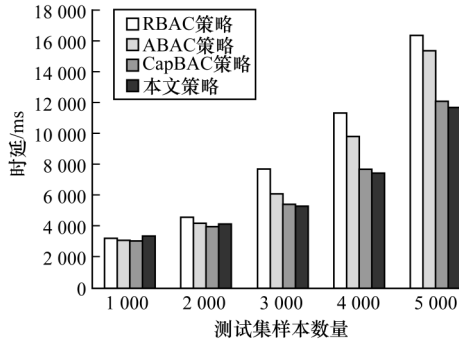


图7 4种策略的判决性能比较

Fig.7 Comparison of decision performance of four strategies

从图7可以看出,所有策略裁决时延随测试集样本的增加而不断增长。当测试集样本数量较少时,本文结合RBAC模型和智能合约的访问控制策略、RBAC策略、ABAC策略及CapBAC策略裁决时延相差不大,原因是当样本较少时,使用上述4种不同策略机制的系统吞吐量(即每秒处理事务请求的数量)均可满足少量样本策略的正常处理条件,不存在时延上的差异。而随着测试集样本数量的不断增加,4种策略的裁决时延逐渐出现差距,当测试集样本增加到较大数量后,CapBAC策略与本文策略的时延相对RBAC策略、ABAC策略增长趋势较慢,同时本文策略裁决时延又较CapBAC策略有所降低,分析原因可知,由于样本数量的不断增加,4种不同策略机制的系统吞吐量均逐渐不能满足同一时间段的较大并发策略数量的裁决请求,导致策略裁决出现排队情况,并且吞吐量的差异使得4种策略性能逐渐拉开差距。但是,本文策略中由于以太坊区块链的P2P网络架构,各个节点均可对策略事务请求做出裁决,并发处理策略请求数更多,且以太坊区块链拥有真正图灵完备的EVM,任何算力需求的智能合约均可在EVM上执行,使用智能合约来实现复杂算法从而快速地对策略做出裁决,此外,本文策略进行角色分级和用户分组的RBAC模型使得策略更加细粒度化,策略裁决更加明确。上述条件均提高了本文策略判决机制的系统吞吐量,降低了策略判决时延。因此,本文策略裁决效率和判决性能更高。

从图8可以看出,随着策略规则的增加,本文策略判决成功率有所下降,这是由于策略集中存在部分冲突策略,针对冲突策略,策略判决合约无法得到一致性的判决结果,但是最终成功率下降趋势逐渐平缓,说明本文访问控制机制具有较好的判决性能。

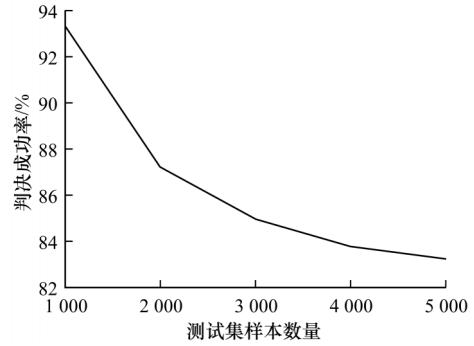


图8 不同样本数量下的策略判决成功率

Fig.8 Decision success rate of strategy with different number of samples

3.2 安全性分析

在以太坊区块链中,攻击者对共识机制进行攻击进而修改区块数据是区块链安全性受到威胁的主要原因。本文采用文献[19-20]提出的攻击模型,通过将研究人员普遍使用的PoW共识机制作为用例,对以太坊区块链的安全性进行分析,用二项随机过程来描述以太坊区块链所面临的信任链与攻击链之间存在的竞争关系。攻击者通过使伪造链长度超过信任链来抵消存在的 z 个区块差距。其中,成功抵消存在的 z 个区块差距的几率问题与赌徒破产问题(Gambler's Ruin Problem, GRP)相似。攻击链攻击成功时的长度不小于信任链长度的概率计算方法如下:

$$q_z = \begin{cases} 1, & p \leq q \\ \left(\frac{q}{p}\right)^z, & p > q \end{cases} \quad (1)$$

其中, p 为信任节点得到下一个区块记账权的概率, q 为攻击节点得到下一个区块记账权的概率, $p+q=1$ 。

为得到攻击链确切的区块进展个数,假设信任链产生一个区块将会耗费平均预期时间,则攻击链的潜在进展可以看作一个泊松分布,分布的期望值用式(2)表示:

$$\lambda = z \cdot \frac{q}{p} \quad (2)$$

为了计算攻击链长度达到信任链长度的概率,将攻击链区块进展数量的泊松分布概率密度与该数量下攻击链长度仍能够达到信任链长度的概率相乘。攻击者成功篡改区块数据的概率 P 用式(3)表示:

$$P = \sum_{k=0}^{\infty} \frac{\lambda^k \cdot e^{-\lambda}}{k!} \cdot \begin{cases} \left(\frac{q}{p}\right)^{(z-k)}, & k \leq z \\ 1, & k > z \end{cases} \quad (3)$$

为避免式(3)发生无限数列求和,将其进一步转化为式(4):

$$P = 1 - \sum_{k=0}^z \frac{\lambda^k \cdot e^{-\lambda}}{k!} \cdot \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \quad (4)$$

本文采用 Matlab 2018b 进行仿真,实验结果如图 9 所示。从图 9 可以看出,攻击者篡改区块数据的成功概率随着区块相差数量 z 的增大呈下降趋势,且当区块数量差距相同时,攻击者篡改区块数据的成功概率随着其得到下一个区块记账权的概率(即算力)的提高而不断上升。因此,当攻击者算力越强时,就越可能篡改区块数据,将自身变为信任链。因此,可以采取增加信任链区块数量从而使其足够长以及增强算力的方式来降低攻击者的攻击效果。由于物联网生态系统中通常设备数量巨大,每个设备均可作为一个以太坊区块链的轻节点,且以太坊区块链具备图灵完备特性,因此本文基于以太坊区块链的物联网设备访问控制机制,符合物联网生态系统对设备访问控制的安全性要求。

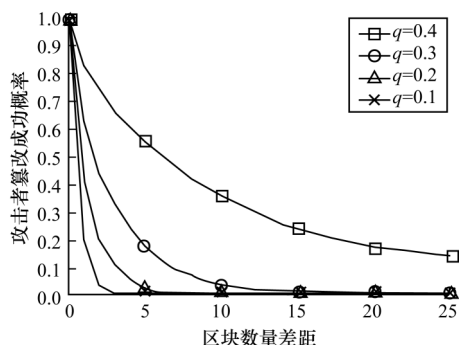


图9 攻击成功概率对比

Fig.9 Comparison of attack success probability

4 结束语

本文提出一种基于以太坊区块链的物联网设备访问控制机制,在以太坊区块链技术中引入 RBAC 相关理论,结合以太坊区块链所具有的去中心化、不可篡改及可追溯等特性,通过以太坊区块链事务管理用户、角色及访问控制策略,实现全程管理及追踪策略的发布、更新以及撤销,从而解决传统权限判决方法非透明与效率低的问题。通过基于 RBAC 模型的智能合约使访问控制策略过程更加灵活且结果更加可信,有效提升物联网设备的安全性及设备间的交互能力。结合 IPFS 与以太坊区块链进行数据存储,能够提高策略存储的安全性。实验结果验证了本文访问控制机制的有效性与安全性。物联网设备的访问控制对时间的要求较高,多数物联网场景需要实现实时的访问控制,在本文基于区块链智能合约的物联网设备访问控制机制中,区块链中的共识速度直接制约着访问控制速度,今后将对共识机制进行研究以提高区块链的共识速度,从而进一步提升访问控制效率。

参考文献

- [1] FANG Liang, YIN Lihua, GUO Yunchuan, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers, 2017, 40(7): 1680-1698. (in Chinese)
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.
- [2] SHI Jinshan, LI Ru. Survey of blockchain access control in Internet of things[J]. Journal of Software, 2019, 30(6): 1632-1648. (in Chinese)
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.
- [3] YUANYU Z, SHOJI K, YULONG S, et al. Smart contract-based access control for the Internet of things[J]. IEEE Internet of Things Journal, 2019, 6(2): 1594-1605.
- [4] NDIBANJE B, LEE H J, LEE S G. Security analysis and improvements of authentication and access control in the Internet of things[J]. Sensors, 2014, 14(8): 14786-14805.
- [5] YAVARI A, PANAH A S, GEORGAKOPOULOS D, et al. Scalable role-based data disclosure control for the Internet of things [C]//Proceedings of 2017 IEEE International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2017: 2226-2233.
- [6] LIU Qiang, ZHANG Hao, WAN Jiafu, 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.
- [7] CRUZ J P, KAJI Y, YANAI N. RBAC-SC: role-based access control using smart contract[J]. IEEE Access, 2018, 6: 12240-12251.
- [8] OUECHTATI H, AZZOUNA N B. Trust-ABAC towards an access control system for the Internet of things[EB/OL]. [2020-01-05]. https://www.researchgate.net/publication/319980251_Trust-ABAC_Towards_an_Access_Control_System_for_the_Internet_of_Things.
- [9] HEMDI M, DETERS R. Using REST based protocol to enable ABAC within IoT systems[C]//Proceedings of 2016 IEEE Annual Information Technology, Electronics and Mobile Communication Conference. Washington D. C., USA: IEEE Press, 2016: 1-7.
- [10] SHEN Haibo, LIU Shaobo. 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. (in Chinese)
沈海波,刘少波. 面向物联网的基于上下文和权能的访问控制架构[J]. 武汉大学学报(理学版), 2014, 60(5): 424-428.
- [11] 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.
- [12] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the Internet of things[J]. IEEE Access, 2016, 4: 2292-2303.

(下转第47页)

(上接第39页)

- [13] China Blockchain Technology and Industry Development Forum. White paper on China's blockchain technology and application development(2016)[EB/OL]. [2020-01-05]. <http://www.cbdforum.cn/bcweb/index/article/rsr-6.html>. (in Chinese)
中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书(2016)[EB/OL]. [2020-01-05]. <http://www.cbdforum.cn/bcweb/index/article/rsr-6.html>.
- [14] FOTIOU N, SIRIS V A, POLYZOS G C. Interacting with the Internet of things using smart contracts and blockchain technologies[EB/OL]. [2020-01-05]. <https://sofie.comnet.aalto.fi/images/4/4c/Spiot.pdf>.
- [15] Ethereum white paper(2013)[EB/OL]. [2020-01-05]. <https://github.com/ethereum/wiki/wiki/White-Paper>.
- [16] GAO Yichen, ZHAO Bin, ZHANG Zhao. Research and implementation of a smart automatic contract generation method for Ethereum[J]. Journal of East China Normal University(Natural Science), 2020(5): 21-32. (in Chinese)
高一琛, 赵斌, 张召. 面向以太坊的智能合约自动生成方法研究与实现[J]. 华东师范大学学报(自然科学版), 2020(5): 21-32.
- [17] RADZIWIŁŁ N. Blockchain revolution; how the technology behind bitcoin is changing money, business, and the world[J]. Quality Management Journal, 2018, 25(1): 64-65.
- [18] LIU Aodi, DU Xuehui, WANG Na, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654. (in Chinese)
刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654.
- [19] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2020-01-05]. <https://bitcoin.org/bitcoin.pdf>.
- [20] DING Wei, WANG Guocheng, XU Aidong, et al. Research on key technologies and information security issues of energy blockchain[J]. Proceedings of the CSEE, 2018, 38(4): 1026-1034, 1279. (in Chinese)
丁伟, 王国成, 许爱东, 等. 能源区块链的关键技术及信息安全问题研究[J]. 中国电机工程学报, 2018, 38(4): 1026-1034, 1279.

编辑 吴云芳