计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20190416
56(10): 2287-2298, 2019

物联网中基于智能合约的访问控制方法

杜瑞忠　刘　妍　田俊峰
(河北大学网络空间安全与计算机学院　河北保定　071002)
(河北省高可信信息系统重点实验室(河北大学)　河北保定　071002)
(drzh@hbu.edu.cn)

An Access Control Method Using Smart Contract for Internet of Things

Du Ruizhong, Liu Yan, and Tian Junfeng
(*School of Cyber Security and Computer, Hebei University, Baoding, Hebei* 071002)
(*Key Laboratory on High Trusted Information System in Hebei Province (Hebei University), Baoding, Hebei* 071002)

Abstract While Internet of things (IoT) technology has been widely recognized as an essential part in our daily life, it also brings new challenges in terms of privacy and security. In view of the limited resources, large number of connections and strong dynamics of the devices in the Internet of things, the traditional centralized access control technology is not fully applicable, and how to achieve secure and efficient access control authorization in the IoT environment has become an urgent problem to be solved. In this regard, a distributed architecture based on hierarchical blockchain for Internet of Things (DAHB) is proposed, which includes device layer, edge layer and the cloud layer. In this architecture, we combine the advantages of blockchain technology to realize flexible, dynamic and automatic access control for IoT devices based on ABAC model in the domain and across the domain by means of smart contract. At the same time, the credit value and honesty are added to the attribute metric to dynamically evaluate the trust relationship between different domains and devices. The theoretical analysis and experimental results show that this scheme is more effective than the existing schemes in solving the requirements of lightweight, flexibility, fine-grained and security in Internet of things (IoT)access control.

Key words Internet of things (IoT); blockchain; access control; trust; smart contract

摘　要　针对物联网中设备资源受限、连接数量大、动态性强等特点,传统的集中式访问控制技术已不完全适用,如何在物联网环境中实现安全高效的访问控制授权成为亟待解决的关键问题.对此,提出一种基于层级区块链的物联网分布式体系架构(distributed architecture based on hierarchical blockchain for Internet of things, DAHB).在该架构中以基于属性的访问控制(attribute-based access control, ABAC)模型为基础,采用智能合约的方式实现对物联网设备基于属性的域内和跨域的灵活、动态、自动化的访问控制.同时,在属性度量中增加信任值与诚实度动态评估不同域间和设备间的信任关系,保证

收稿日期:2019-06-12;**修回日期**:2019-07-30
基金项目:国家自然科学基金项目(61572170,61170254);河北省自然科学基金重点项目(F2019201290);河北省自然科学基金项目(F2018201153);河北大学研究生创新资助项目(hbu2019ss031)
This work was supported by the National Natural Science Foundation of China (61572170, 61170254), the Key Program of the Natural Science Foundation of Hebei Province of China (F2019201290), the Natural Science Foundation of Hebei Province of China (F2018201153), and the Post-graduate's Innovation Fund Project of Hebei University (hbu2019ss031).
通信作者:刘妍(1119250989@qq.com)

实体能够履行合约的信用能力和稳定性.理论分析和实验结果表明:该方案比现有方案更有效解决物联网访问控制中存在的轻量级、灵活性、细粒度和安全性问题.

关键词 物联网;区块链;访问控制;信任度;智能合约

中图法分类号 TP309

随着智能设备和高速网络的快速发展,物联网(Internet of things, IoT)作为资源受限的低功耗网络的主要标准得到了广泛的接受和普及,已经应用到智能城市、车联网、智能医疗等众多领域,使人们进入万物互联时代[1-2].根据市场调研机构 IDC 的预测,到 2020 年将有超过 500 亿的终端与设备联网[3],联网设备数量的急剧增加给物联网系统带来了新的安全风险和挑战.由于物联网设备分布广泛,实施严格的安全控制非常困难,使得设备容易受到恶意节点的各种攻击.同时,物联网设备中往往含有大量和个人隐私相关的敏感数据,如果不对这些数据提供可靠的保护,一旦泄露会给用户带来巨大的损失.因此,研究物联网中访问控制机制,防止未经授权的访问,成为了物联网安全和隐私保护的重要研究内容之一[3-5].

研究者们纷纷提出了各种具有不同目标的访问控制(access control, AC)方法和解决方案.Ferraiolo 等人首次提出基于角色的访问控制(role-based access control, RBAC)模型[6],在访问控制研究中引入角色,将用户映射到角色,使用户拥有角色相对应的权限;文献[7]中提出一种轻量级、高度可伸缩的数据混淆技术以解决物联网中发生未经授权的访问和敏感信息的泄露,将实验设为医疗场景,通过 RBAC 方式管理从传感器获取的人体相关数据,以保证安全性;文献[8]使用区块链解决 RBAC 中跨组织访问控制问题,实现了用户角色的跨组织认证.但 RBAC 模型会出现角色爆炸问题,不适用于需要解释复杂和模糊的物联网场景中安全策略的实现.同时,大量计算和保存用户与角色、角色与权限等信息对物联网设备受限的计算和存储资源带来更大的挑战.

基于权能的访问控制(capability-based access control, CapBAC)在物联网环境中已经实现了轻量级、分布式、动态性和可扩展性,被认为是物联网系统有前途的解决方案.文献[9]中提出了以权能为基础的细粒度的访问控制模型,企业甚至个人都可以使用它来管理自己对服务和信息的访问控制过程;针对物联网环境下动态的网络拓扑结构、受限的上下文环境和资源低功耗设备的弱物理安全特性,文献[10]中提出了一种身份认证和基于权能的物联网访问控制模型,虽然 CapBAC 分布式的设计避免了使用集中式服务器带来的单点故障问题,但其无法解决在不可信环境下的物联网访问控制;因此,文献[11]提出了一种鲁棒的基于身份的权能令牌管理策略,利用智能合约对访问控制进行注册、传播和撤销.提出的 BlendCAC 方案能够在分布式和无信任的物联网网络中高效地实施访问控制授权和验证.

在具有异构性和多样性特征的物联网网络环境下,访问控制技术研究开始向细粒度、分层次的方向发展,考虑用户、资源、操作和运行上下文属性,提出基于属性的访问控制(attribute-based access control, ABAC)[12],将主体和客体的属性作为基本的决策要素,灵活利用请求者所具有的属性集合决定是否赋予其访问权限;文献[13]中提出了属性规则的策略语言及解决策略冲突和冗余的方法,简化了传统 ABAC 的复杂性;文献[14]中基于属性的访问控制机制,验证用户身份,重点研究低功耗物联网设备如何实现数据安全访问;文献[15]中提出了一种基于区块链技术创建、管理和实施访问控制策略的方法,并允许用户之间进行资源访问权的分布式转移.且该方案允许分布式审计,防止一方欺诈地拒绝可执行策略授予的权利.ABAC 模型能够有效地解决动态大规模环境下的细粒度访问控制问题,是新型计算环境中的理想模型,应用前景广阔.

目前研究者结合传统访问控制模型提出的适用于物联网环境的方案中,仍然存在许多不足.如针对医疗数据授权、跨组织角色认证等具体场景的模型存在可扩展性差的问题,在实际应用中具有一定的局限性;甚至有些方案还以降低安全性为代价来提高访问控制的性能.因此,为了在保证安全性的前提下满足物联网时代可扩展性、灵活性和轻量级等诸多需求,本文的主要贡献有 3 个方面:

1) 结合区块链技术的优势,提出一种包括设备链和边缘链的层级分布式物联网访问控制体系结构.边缘链利用网络边缘设备空闲资源执行计算任务,将原有云计算中的部分或全部服务下沉到网络边缘,有效缓解资源受限的物联网设备存储大量数据区块的负担和缩短处理大量访问请求的响应时间.

2) 提出了基于智能合约的访问控制方法,设计智能合约内容实现 ABAC 模型中策略执行点、属性权威、策略决策点部分.按照顺序触发设定的合约内容,实现灵活、可扩展、细粒度的访问控制机制,解决了传统可信网络中面临的访问控制单点化和策略决策中心化的问题.

3) 基于 ABAC 模型,使用实体属性对主体、客体、权限等进行统一描述,在属性中引入信任度量,利用信任值与诚实度反映实体能够履行合约的信用能力和稳定性,作为授权决策的依据.仿真实验中根据信任阈值设定信任等级,该方法能够有效防止恶意节点非法授权访问的发生.

1 相关知识

1.1 区块链技术

区块链是公共分类账本,允许分布式地记录、存储和更新数据[16-17].由于其性质,区块链是一种分散的架构,不依赖于集中的权限.事务被批准并记录在矿工创建的块中,并且块按时间顺序附加到区块链.由于通过网络上的矿工挖矿任务实施的共识机制,用户可以信任全局存储的公共分类账系统,而不是必须与第三方建立和维护信任关系.区块链是确保无信任环境中所有参与者进行分布式事务的理想架构.

区块链自身可以在假定参与者都不是可信的情况下在技术层面迫使所有参与者遵守诚信,而且具有不可篡改性和隐私保护性,使得区块链担任物联网访问控制中可信第三方角色成为可能,为物联网中访问控制提供一个可信的计算环境[18-20].

1.2 智能合约

智能合约本质上是已经在区块链特定地址记录的预定义指令和数据的集合,其通过代码程序来自动执行合约,只要满足合约条款,交易将无需第三方监督自动进行[21].与普通区块链交易一样,节点会首先进行签名验证来确保合约的有效性,验证通过的合约经过共识机制共识后会成功执行.智能合约和区块链网络中生成的所有交易在每个区块中以 Merkle 树结构保存,Merkle 树是一种构建的自下而上的树型数据结构,对所有事务数据进行散列并保存为叶节点,叶到根的连续子节点进行散列直到生成根 Hash 值存储在区块头.

在给定预定义的业务逻辑或合约协议的情况下,由智能合约定义的公共功能或应用程序二进制接口(ABI)允许用户与它们进行交互.通过将操作逻辑封装为字节码并对分布式矿工执行图灵完整计算,智能合约允许用户将更复杂的业务模型转码为区块链网络上新类型的交易.智能合约提供了一种有前途的解决方案,允许在区块链网络上实施更灵活、更细粒度的访问控制模型.

2 基于层级区块链的物联网分布式访问控制系统模型

为了更好地解决设备域内和域间的访问控制问题,考虑物联网设备在能量、存储、计算等方面的局限性,提出一种基于层级区块链的物联网分布式体系架构,该架构在传统的云计算中引入边缘设备,如图 1 所示,构成端-边-云模型.边缘层维护一条区块链,设备层中的每个管理域中各维护一条链,以完成物联网下的安全访问控制.边缘层是利用网络边缘设备空闲资源执行计算任务,将原有云计算中的部分或全部服务下沉到网络边缘,更贴近用户.特别地,对于接入网络数以百万计的设备进行的资源访问请求,能提供高质量、低时延、低能耗的响应服务.

2.1 设备层

如图 1 所示,在设备层中有多个独立的管理域都拥有大量的物联网设备,在每个管理域内根据计算和存储能力大小将众多设备分成 2 类:1)由服务器、存储设备、物联网网关等计算和存储水平较高的设备组成,它们通过区块链网络连接在一起构成设备链,且每个设备都安装遵守区块链协议的客户端并绑定区块链账户;2)域内还存在许多能力较弱的物联网设备(如传感器、摄像头等),其经由物联网网关连接到区块链网络(每个物联网网关通过蓝牙、WiFi、Zigbee 等短程通信技术,将一组物联网设备连接到区块链网络,并作为这些物联网设备的服务代理).

2.2 边缘层

边缘层设备共同参与维护一条边缘链,利用设备空闲的计算、存储和网络资源,实现事务在不同管理域间的资源访问请求,能够显著减少请求的响应时间.设置 Agent 代理设备,该设备绑定了 2 个区块链账户,即连接到本地管理域的区块链账户和连接到边缘层的区块链账户.管理域内的设备只能通过 Agent 代理向另一管理域发起访问请求,或者接收来自另一管理域的请求访问信息.

每个物联网设备隶属于一个唯一的 Agent 代理,每一个 Agent 代理拥有许多不同的物联网设备.

Agent 代理与其所有的下属设备构成一个管理域.设备可以在管理域内或管理域间进行事务请求以实现特定需求,域管理者可以在彼此之间进行事务请求.Agent 代理节点不能是受约束的设备,此类设备需要高性能特性以便满足物联网设备尽可能多的并发请求.

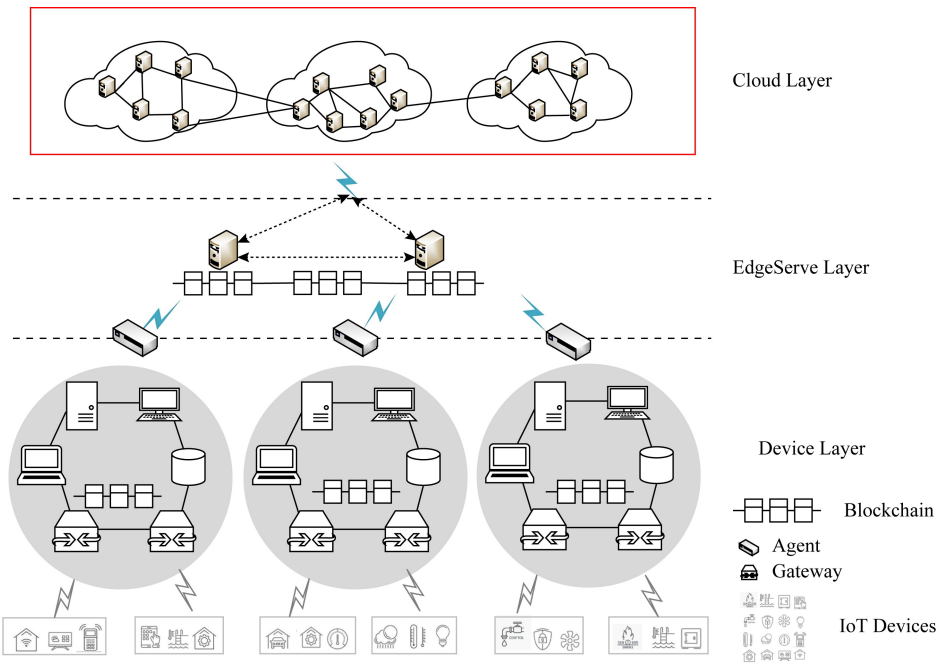

Fig. 1 The system architecture for access control

图 1 访问控制系统架构

3 访问控制工作机制

在 DAHB 系统内主要研究分布式、高动态物联网环境中设备的安全访问控制问题.主要工作是基于传统 ABAC 模型进行改进,利用智能合约与访问控制技术相结合,实现域内与域间的访问控制过程.模型主要包括:策略执行点合约(policy enforcement point by smart contract, SC_PEP)、属性权威合约(attribute authority by smart contract, SC_AA)、策略判定点合约(policy decision point by smart contract, SC_PDP)、策略管理点 PAP(脱链存储)和跨域合约 DAA.在对实体控制流程中,主体通过向合约发送请求事务,调用合约函数,完成特定操作,使用事件监听通知客户端事务的完成状态.为了便于解释主体对客体访问过程,给出一些基本操作的定义:

3.1 预备知识

定义 1. 事务发送.事务主要是指一条外部账户发送到区块链上另一账户的消息的签名数据包.事务处理是一个过程,从账户发起事务请求开始,到包含该交易的区块被共识节点同步为止,完成这一过程才算事务成功完成.事务发送完成后,返回事务的 Hash 地址,可用于查询该事务的发送者地址和接收者地址及其它相关信息.

定义 2. 事件通知.事件是合约与外部实体之间的沟通桥梁.事件可以用来通知外部实体,外部实体通过轻客户端可以方便地查询、访问事件.在真实的环境中,需要发送事务来调用某个智能合约,当事务被发送但未被打包、执行时,将无法立即获取智能合约的返回值.即在合约中定义事件,事件中带有参数,当合约函数内部完成某些操作时,通过触发事件通知交易被打包执行.只有合约将事件写入区块链后,前端才能进行对应的响应.

定义 3. 函数调用.在智能合约中有两类函数调用,即内部函数调用和外部函数调用.内部函数调用是指一个函数在同一个合约中调用另一个函数;外部函数调用是指一个函数调用另一个合约的函数.

定义 4. 属性信息.由管理员向管理域内区块链中发布属性及属性关系信息,由合约 SC_AA 预先收集、整合区块链事务中属性信息,以供 SC_PEP 和 PAP 使用.在访问控制过程中,设备是系统存在的实体,既可以是发起请求的主体,也可以是提供资源的客体.例如,对于主体属性可以有:地址、角色、

信任度等;客体属性包括状态(open,protected)、有效时间(允许访问的时间区间)等.对环境属性通常是访问控制发生时的环境状况,如系统的当前时间、系统的安全级别、IP 地址等;对操作权限来说,其属性为读、写和执行.

定义 5. 信任关系.添加对实体属性的信任度量计算,以有效识别恶意节点,防止其发出异常访问请求.为此,不同的安全域间需要评估与更新信任关系,网络中设备也需要动态更新与其他设备间的信任关系.采用信用值与诚实度对一个实体的可信程度进行描述.其中信用值反映一个特定实体在某时刻被其他实体认定能够履行合约的信用能力.诚实度根据特定实体信用表现稳定性反映期望能提供有效服务的概率.$A(x)$表示域代理节点,$N(x,y)$表示 $A(x)$域内的设备节点,$D(x)$表示管理域.

1) $D(x)$的信用值.不考虑历史信用时标识 $D(x)$受 $D(x')$的信任程度,记为 $T_d(x,m)$.$T_d(x,m)$的信用分值为 $S_d(x,m)$:

$$S_d(x,m)=C_d(x)+\sum_{i=1}^{m-1}\delta(x,i), \tag{1}$$

$$T_d(x,m)=f(S_d(x,m)). \tag{2}$$

一个常数 $C_d(x)$初始确定,$\delta(x,i)\in\{-1,0,1\}$表示域 $D(x')$对 $S_d(x,m)$的调节因子.映射函数 $f(S_d(x,m))=\dfrac{1}{1+a^{-S_d(x,m)}}$,其中$(a>1)$,$m$ 为信任标记序号.

2) $N(x,y)$的信用值.不考虑历史信用时标识 $N(x,y)$受 $N(x',y')$信任程度的值,记为 $T_n(x,y,m)$.$T_n(x,y,m)$的信用分值为 $S_n(x,y,m)$:

$$S_n(x,y,m)=C_n(x,y)+\sum_{\lambda=1}^{m-1}\sum_{i=1}^{\tau(\lambda)}\delta(x,y,i), \tag{3}$$

$$T_n(x,y,m)=f(S_n(x,y,m)), \tag{4}$$

其中,$\tau(\lambda)$表示特定管理域 $D(x_\lambda)$内存在的 $D(x_\lambda,y_\lambda)$向 $A(x_\lambda)$提交的 $D(x,y)$的调节因子的个数.

3) $H_d(x,\hat{m},r)$是对特定实体过去一段信用记录历史的诚实度度量,反映能提供有效服务的概率.$R_d(x,\hat{m},r)$是纳入诚实度考察的实体信用值的标准差,反映主体在与客体的合作过程中因为主体的违约而导致损失的可能性.诚实度值越高,表示在过去一段时间中该实体的信用表现越稳定,意味着在将来的访问请求中该实体出现与其当前的信用值所呈现的信用水平可能性越大.

4) $D(x)$的诚实度.能够衡量 $D(x)$在过去一段信用记录历史中信用表现稳定性反映能提供有效服务的概率.r 表示纳入考虑信用值的个数:

$$R_d(x,\hat{m},r)=\sqrt{\frac{\sum_{m=m-r+1}^{m}[T_d(x,m)-\overline{T_d(\hat{m},r)}]^2}{r-1}}, \tag{5}$$

$$\overline{T_d(\hat{m},r)}=\frac{\sum_{m=m-r+1}^{m}T_d(x,m)}{r}, \tag{6}$$

$$H_d(x,\hat{m},r)=\frac{1}{1+R_d(x,\hat{m},r)}. \tag{7}$$

5) $N(x,y)$的诚实度.能够衡量 $N(x,y)$在过去一段信用记录历史中信用表现稳定性反映能提供有效服务的概率:

$$R_n(x,y,\hat{m},r)=\sqrt{\frac{\sum_{m=m-r+1}^{m}[T_n(x,y,m)-\overline{T_n(\hat{m},r)}]^2}{r-1}}, \tag{8}$$

$$\overline{T_n(\hat{m},r)}=\frac{\sum_{m=m-r+1}^{m}T_n(x,y,m)}{r}, \tag{9}$$

$$H_n(x,y,\hat{m},r)=\frac{1}{1+R_n(x,y,\hat{m},r)}, \tag{10}$$

定义 6. 策略信息.由设备域的管理者向域内的 PAP 设备发布访问控制策略,由 PAP 结合属性信息描述、收集、整合区块链事务中访问控制策略,以供 SC_PDP 进行访问请求判决.一条策略由一个或多个规则组成,而访问控制规则通常用一个逻辑判别式表示,用于判断这个访问请求能否发生,具体格式为 Rule:$access(S,O,E,P)\rightarrow f(attr(S),attr(O),attr(E),attr(P))$其中:$access(S,O,E,P)$表示访问主体 S 在特定环境 E 下能否对客体 O 执行 P 操作,$attr(S)$,$attr(O)$,$attr(E)$,$attr(P)$分别表示主体 S、客体 O、环境 E 及操作 P 的属性集,$f(attr(S),attr(O),attr(E),attr(P))$其返回值为{true,false,not applicable}.当值为 true 时,表示该访问请求能发生;当返回值为 false 时,表示访问请求不能被授权;当返回值为 not applicable 时,表示客体不适用该访问请求.

3.2 基于 DAHB 系统的访问工作流程

本节对基于层级区块链的访问控制工作流程进行详细说明,如图 2 和图 3 所示,分别介绍物联网环境中安全域内和跨域的访问控制工作的实现.

3.2.1 域内访问控制实现

1) 本地域中的主体设备向 SC_PEP 合约发送事务调用 SC_PEP 中的域内访问请求函数,事务中包含参数:客体设备名称及动作.

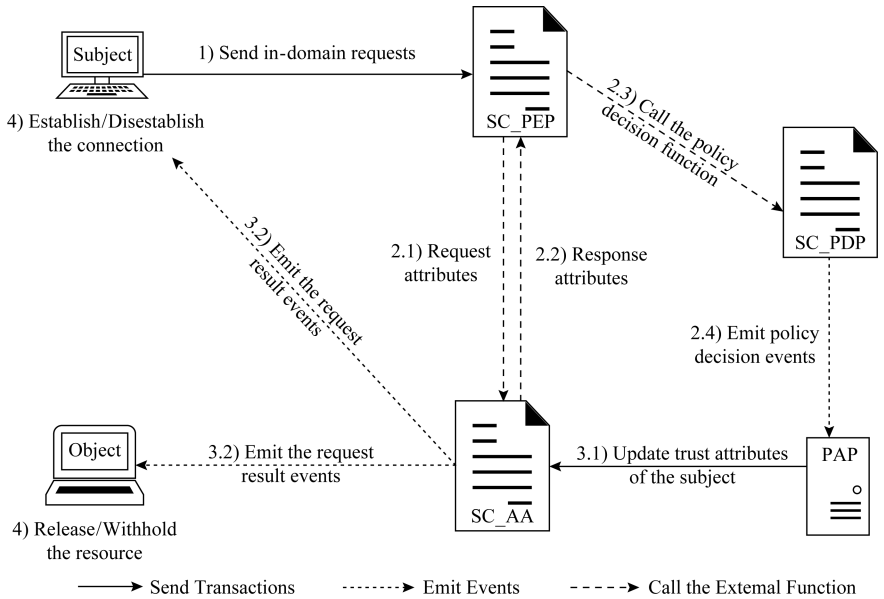

Fig. 2 Access control processes within the domain

图 2 域内访问控制流程

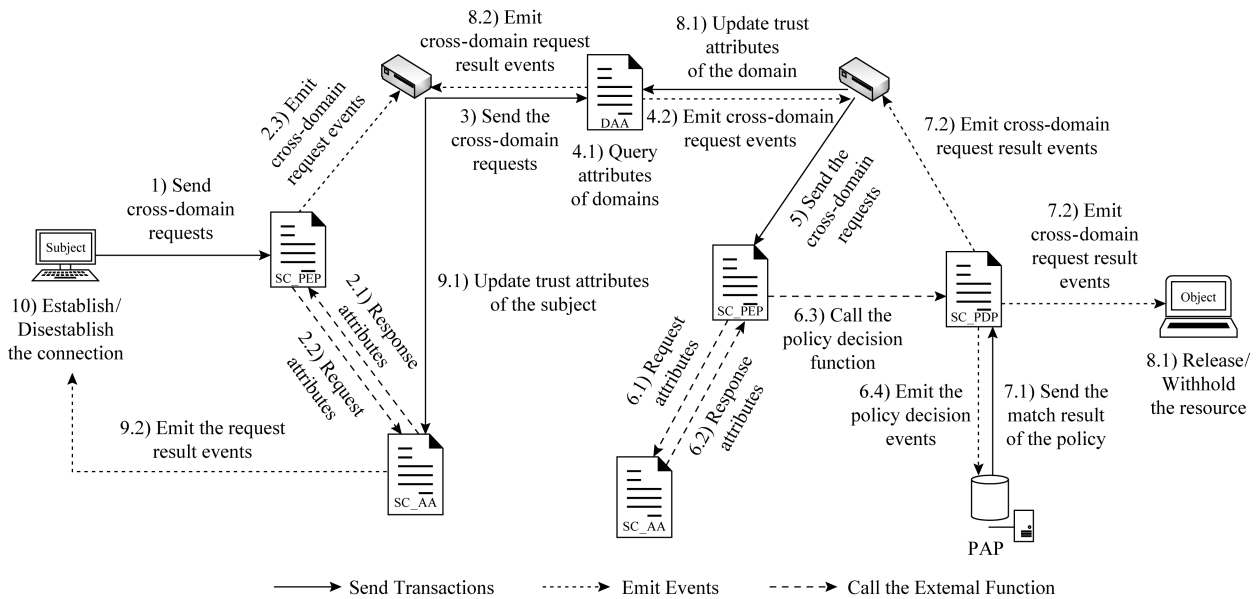

Fig. 3 Access control processes cross the domain

图 3 跨域访问控制流程

2) 该事务被打包执行,SC_PEP 中的域内访问请求函数从本地域中的 SC_AA 中获取主体设备和客体设备的属性信息,然后调用 SC_PDP 中的策略判断函数,触发其中的策略判断事件.

3) 策略执行点 PAP 设备监听策略判断事件,匹配设备中的策略表并进行逻辑推理得到域内访问请求结果.PAP 设备向 SC_AA 合约发送事务调用 SC_AA 内的更新历史记录函数以更新主体的历史访问记录和主体的动态属性,并触发该函数中的访问请求结果事件.

4) 监听到访问请求结果事件的主体设备和客体设备对结果做出响应.

3.2.2 跨域的访问控制实现

1) 本地域中的主体设备向 SC_PEP 合约发送事务来调用 SC_PEP 中的域外访问请求函数,事务中包含参数:目标域、客体设备名称及动作.

2) 该事务被打包执行,SC_PEP 内的域外访问请求函数从本地域的 SC_AA 中获取主体设备属性信息,并触发该函数中的域外请求访问事件,事件中包含参数:目标域域名、主体设备属性信息、客体设

备名称及动作.

3) 来源域中的 Agent 设备监听到来自本地域的域外请求访问事件,并向边缘层中的 DAA 合约发送事务来调用其中的跨域访问请求函数,并发送参数:目标域域名、主体设备属性信息、客体设备名称及动作.

4) 该事务被打包执行,DAA 中的跨域访问请求函数根据传递的参数查询 DAA 合约中域属性表,获得来源域的域名,来源域的属性,目标域 Agent 的区块链账户地址,并触发该函数中的跨域访问请求事件,事件中包含参数:来源域域名、来源域的属性、目标域的 Agent 地址、主体设备属性信息、客体名称及动作.

5) 目标域中 Agent 设备监听到来自边缘层的跨域访问请求事件,并向目标域中的 SC_PEP 合约发送事务来调用其中的域外请求处理函数,并发送该事件传递的参数.

6) 该事务被打包执行,SC_PEP 内的域外请求处理函数会调用目标域中 SC_AA 获取客体设备的属性信息,然后调用 SC_PDP 中策略判断函数,并发送参数:来源域域名、来源域的属性、主体设备和客体设备的地址和属性信息及动作,并触发策略判断事件.

7) 由 PAP 设备监听该事件并匹配设备中的策略表,进行逻辑推理得到 result,并向 SC_PDP 合约发送事务调用其内的域外请求结果函数,返回本次跨域访问的结果并触发该函数中的域外请求结果事件.

8) 目标域中监听到该事件的客体设备对结果做出响应.同时目标域中监听到该事件的 Agent 设备发送事务来调用其中的返回跨域结果函数将结果反馈给边缘层中的 DAA,该函数会计算更新 DAA 合约中来源域的历史记录及信用值和诚实度.并触发该函数中的返回跨域结果事件.

9) 来源域中的 Agent 设备监听来自边缘域的返回跨域结果事件,向来源域中的 SC_AA 发送事务来调用其中的更新历史记录函数来更新主体的历史访问记录和计算并更新主体的动态属性并触发该函数中的更新历史记录事件.

10) 监听到更新历史记录事件的主体设备对结果做出响应.

4 实验分析与验证

4.1 对比分析

目前,将区块链技术与访问控制工作相结合已经是区块链在物联网中的主要应用之一.表 1 是区块链与不同访问控制模型结合的研究,充分体现了本方案的性能优势.表 2 主要说明区块链与 ABAC 模型相结合的主要工作特点.

Table 1 Comparison of Different Access Control Schemes

表 1 不同访问控制方案工作对比

Scheme	Distributed	Lightweight	Flexibility	Dynamics	Fine-grained
RBAC[8]	√		√	√	
CapBAC[11]	√	√	√		√
UCON[24]	√	√	√		
ABAC	√	√	√	√	√

Note: √ means the performance is available in the scheme.

Table 2 Integrating Blockchain into ABAC Access Control Model

表 2 将区块链融入 ABAC 访问控制模型

Scheme	Characteristics
Ref [22]	Using smart contracts to store identity tokens and policies in blockchain, which guarantees the integrity of policy implementation. But the computational cost of encryption is too high to be applied only in the cloud environment.
Ref [15]	The policy and authority exchanges are public on the blockchain, which prevents a party from fraudently denying the rights granted by the policy.
Ref [23]	Using blockchain to record attribute distribution can effectively avoid single point of failure and data tampering.
Ours	Forming the hierarchical blockchain structure to improve the response time of requests, and smart contracts are adopted to implement the ABAC model.

4.2 安全性分析

采用有限状态机(finite state machine, FSM)分析模型的安全性,有限状态机将模型描述为抽象的数学状态,通过证明模型的初始状态和所有状态

的转换函数安全,则整个模型系统安全.构造有限状态机包括4个步骤(以域内访问请求过程为例,跨域访问请求同理可得):

1) 定义相关的状态变量

模型的有限状态机系统定义为一个四元组模型$M=(V,I,X,F)$.其中,V表示系统的有限状态集合,V_0是系统的初始状态;I表示系统的输入集合;X表示系统的输出集合;$F:V\times I\rightarrow V$为状态转换函数,表示在输入的驱动下从某一个状态转换到另一个状态.

根据以上定义的状态变量,访问控制状态的设置如表3所示:

Table 3 Set State of Access Control

表3 访问控制状态设置

State Set V	Input Set I	Output Set X
V_0:Initial state of system	I_0:SC_PEP accepts the request from the subject and initial its instance	X_0:Send transactions and call requests function
V_1:Request attributes	I_1:SC_AA responses the request from SC_PEP	X_1:Get attributes of subject and object
V_2:Get($attr(S)$,$attr(O)$,$attr(E)$)	I_2:Call the policy decision function from SC_PDP	X_2:Emit the policy decision event
V_3:PAP emit events	I_3:Match attributes and the policy	X_3:Emit the request result event
V_4:Access	I_4:Access to object resources normally and update the attributes of the subject	X_4:Send a new access request
V_5:Revoke	I_5:Unsatisfied the access control condition and update the attributes of the subject	X_5:Reject access to the subject
V_6:End state of system	I_6:End the access control of subject	X_6:End the whole process of access control

2) 定义安全状态条件

系统的安全状态是指系统的各个事件在访问控制框架中得到处理,并且在信任关系确立之后根据主体属性$attr(S)$、客体属性$attr(O)$、环境属性$attr(E)$和匹配的策略POL满足访问控制条件CON.由此定义系统的安全状态满足安全条件式即可:

$$safe(v)\leftarrow(\forall SC\_PEP)match(\exists SC\_AA)\wedge(\exists SC\_PDP)\wedge(\exists PAP)\wedge((s\in S)\wedge(o\in O)\wedge(e\in E)\wedge(t\in T)\wedge(pol\in POL)\wedge(con\in CON).$$

3) 定义初始状态并分析其安全性

初始状态没有任何的访问请求,在初始状态下系统没有任何操作,合约只经部署未被调用,属性集为空,能够满足安全条件式的定义,因此初始状态V_0是安全的.

4) 定义状态转换函数并证明其安全性

根据定义的状态变量,定义系统的状态转换函数包括6个子函数.

① $F_1.V_0\times I_0\rightarrow V_1$,该函数表示接受主体的访问请求,调用SC_PEP内的函数$accessInDomain(objectName,action)$.

② $F_2.V_1\times I_1\rightarrow V_2/V_5$,该函数表示调用SC_AA的函数$getSubjcetAttr()$和$getObjcetAttr()$,获得实体属性,或者实体属性获取失败,不能对客体进行访问.

③ $F_3.V_2\times I_2\rightarrow V_3$,该函数表示调用SC_PDP中的函数$policyJundge()$,进行策略请求.

④ $F_4.V_3\times I_3\rightarrow V_4/V_5$,该函数表示对主体的权限进行决策,主体能够获得权限,对客体进行访问;或者主体没有访问权限.

⑤ $F_5.V_4\times I_4\rightarrow V_6$,该函数表示PAP监听事件返回结果,对访问进行信任属性更新,主体对客体的访问结束.

⑥ $F_6.V_5\times I_5\rightarrow V_6$,该函数表示PAP监听事件返回结果,对访问进行信任属性更新,主体对客体的访问结束.

状态转换示意图如图4所示:

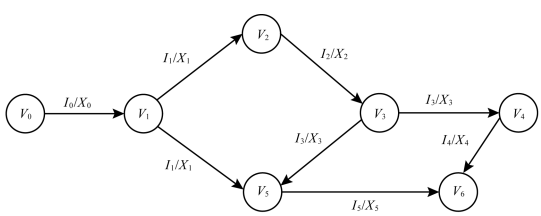

Fig. 4 Transition of state

图4 状态转换示意图

假设主体已经向合约SC_PEP发起安全请求,当前系统状态V_1是安全的.下一个状态需要判断属性获取是否安全,区块链采用带时间戳的链式区块结构存储数据且相连区块间后续区块对前序区块存

在验证关系,因此请求事务是可溯源、防篡改的,状态转换函数 F_2 是安全的,系统状态 V_2 是安全的.接下来需要判断主体是否具有对客体的访问权限,智能合约中执行的所有操作都被记录下来,任何实体都可以审计这些操作,实现了对资源自动化、可信的访问控制操作,完成 V_3,V_4 状态.若所获得的属性信息和策略信息能够满足访问控制条件 CON 时,系统的输出是允许访问,此时系统授予主体访问权限;同时满足之前定义的安全条件式,因此其状态转换函数是安全的.当系统的输出是禁止访问,此时系统所对应的状态不会改变,能够保持系统的安全性,因此状态转换函数是安全的.

根据分析,模型的初始状态 V_0 安全,模型的状态转换函数 F 安全,根据有限状态机对于安全系统的定义可知:满足以上条件,系统就是安全的.

4.3 实验仿真与结果分析

通过仿真实验对提出的访问控制机制的可操作性进行测试,以验证在 DAHB 架构中能够有效解决物联网中设备资源受限的安全控制难题.在实验中利用以太坊技术实现访问控制策略判定过程,实验环境如表 4 所示,其中台式机和笔记本电脑由于具有相对较大的计算能力扮演矿工的角色,树莓派充当轻量级的以太坊节点.在每个设备上安装由 Go 语言编写的 geth 客户端,使用 Remix 集成开发环境编写和编译智能合约,采用 web3.js 通过 HTTP 连接与相应的 geth 客户端交互,用于部署已编译好的合约,并且监视合约状态,即访问控制的结果,使用 PoW 共识机制,完成每笔事务的验证和确认.

Table 4 Specification of Devices

表 4 设备参数说明

Device	CPU	Operating System	Memory Size/GB	Hard Disk Size/GB
Dell OptiPlex 3020	Intel Core i5-4590,3.30 GHz	Windows 10 (64 bit)	12	128+512
Lenovo G480	Intel Core i5-3230,2.6 GHz	Windows 7(64 bit)	12	128+512
Raspberriy Pi 3 Model B	Contex A53,1.2 GHz	Raspbian GNU/Linux 8	1	16

4.3.1 域内访问结果与分析

在实验用例中完成域内私有链的建立和策略执行点合约、属性权威合约和策略判定合约的编译与部署,以实现域内实体间细粒度的访问控制.为了验证域内主体对客体访问的可行性,实施管理域 A 中的主体对客体发起读操作的访问过程,如图 5 所示是客体监听到访问请求结果事件返回为允许的请求结果,并做出释放资源的响应.其中结果显示主体的信用值和诚实度分别为 C 和 B.如图 6 所示,由于该次访问请求成功,并根据式(2)(7)更新主体的信用值和诚实度,主体建立与客体连接,进行资源访问.

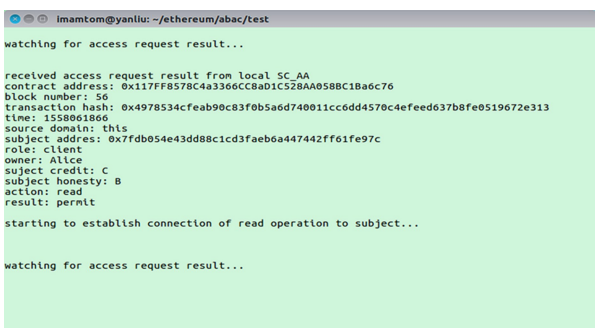

Fig. 5 Results at the Object

图 5 客体返回结果

Fig. 6 Results at the Subject

图 6 主体请求结果

4.3.2 跨域访问结果与分析

在实现实体跨域的访问过程中,考虑物联网设备在能量、存储、计算等方面的局限性,在传统的端-云模型中引入边缘层,在边缘层中利用边缘设备完成边缘链的建立,并编译与部署 DAA 合约,能有效处理数以万计的设备发出的资源访问请求,提供高质量、低时延的响应服务.为了验证主体对客体跨域访问的可行性,实施管理域 A 中的主体对管理域 X 中的客体发起执行操作的访问过程,如图 7 所示的是主体监听到访问请求结果事件返回为拒绝的请求

结果.其中结果显示在发起访问请求前该主体的信用值和诚实度分别为 C 和 B,由于此次访问请求失败,根据式(2)(7)更新主体的信用值和诚实度为 C 和 C,能够实时反映当前环境中主体的信用表现和稳定性,有效阻止恶意节点发起访问请求的发生.如图 8 和图 9 所示,管理域 A 的信用值和诚实度根据式(4)(10)由 A 和 B 更新为 B 和 B,能够在其他实体发起访问时提供判别依据.

Fig. 7 Results at the Subject

图 7 主体请求结果

Fig. 8 Results at the Agent of destination

图 8 目标域中代理结果

4.3.3 区块链网络性能分析

为了验证在 DAHB 架构中方案对恶意节点识别的能力,进行仿真实验,用例 A 是以 1 000 个状态为无访问历史记录的恶意节点进行测试,用例 B 是以 1 000 个状态有正常访问历史记录的恶意节点进行测试.如图 10 所示,由于信任值和诚实度的反馈是根据历史记录得到的,具有正常访问历史记录的恶意节点需要在发送更多数量的访问控制请求事务的延迟确认后才能被检测到.且随着事务数量的增加,该架构中的方案都能将恶意节点检测出来.因此,该方案在分布式物联网网络环境中,在较小的能量和时间消耗情况下,具有良好的恶意节点检测能力.

Fig. 9 Results at the Agent of Request

图 9 来源域中代理结果

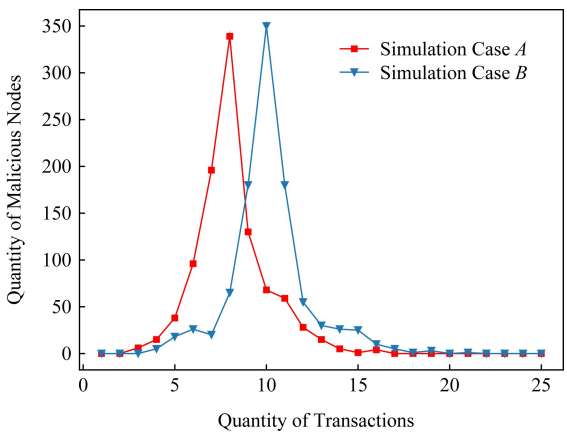

Fig. 10 Malicious node detection results

图 10 恶意节点检测结果

4.3.4 区块链网络性能分析

在实验中,只有当智能合约的相关事务被矿工批准并记录到新区块时,访问控制结果才有效,客体的资源才会做出动作响应即释放或保持.访问控制的效率在事务验证过程不被拥塞的情况下,与块生成时间成比例,块生成时间是指矿工验证新块所消耗的时间.如图 11 显示了矿工数量对区块链网络出块速度的影响.在每个场景中,计算 50 个块附加到区块链的平均块生成时间.随着矿工数量的增加,工作证明所需要的时间缩短,块生成时间减少,最终变得稳定。结果显示,在管理域私有区块链网络中,实现最小块生成时间的最佳矿工数量为 5.

在主体发起访问请求时,总希望快速得到判断

结果,为了验证方案的访问效率,对每秒发出不同访问请求数量时进行实验.如图 12 所示,时间随着访问请求数量的增加而增加,但增长缓慢.因跨域访问请求还需要在边缘层中的边缘链监听事件、调用合约函数以完成进一步操作,完成时间较高于域内的访问请求时间.当每秒请求数量大于 50 时,时间明显延长.

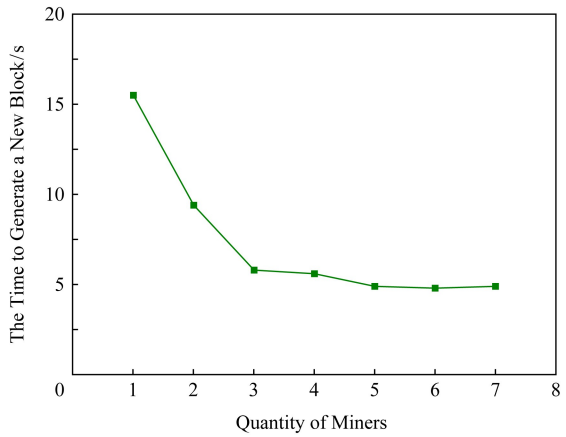

Fig. 11 Time consumption of block generation

图 11 出块速度

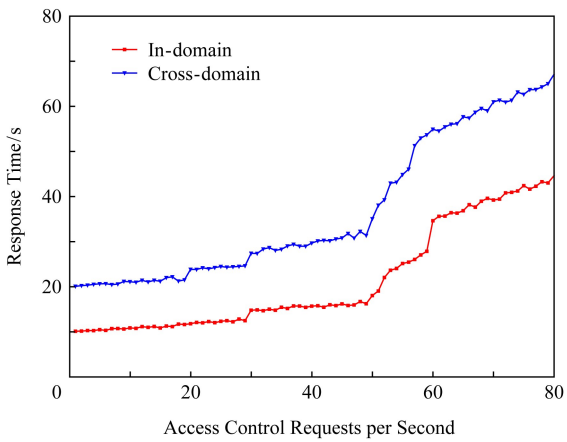

Fig. 12 Response time of access control requests

图 12 访问控制请求响应时间

5 总 结

本文提出一种基于区块链的分布式物联网访问控制方法,在传统端-云模型中引入边缘层,形成分层区块链,充分发挥网络边缘设备优势,实现低时延的访问请求响应.在该框架中以 ABAC 模型为基础,采用智能合约实现灵活、可扩展、细粒度的访问控制过程,按照顺序触发设定的合约内容,完成对设备可信访问控制的自动化操作.引入信任度量动态调整域间和设备间的信任关系,有效避免出现恶意节点的非法授权访问问题.安全性分析表明了系统方案是安全的,并且仿真实验表明该方案在物联网中实施严格和细粒度的访问控制是有效和高效的,但本研究中的属性信息都是以明文形式存储,如何在保证用户数据隐私的情况下,实现灵活、可扩展及细粒度的访问控制是未来需要进行的工作.

参 考 文 献

[1] Ni Jianbing, Lin Xiaodong, Shen Xuemin. Toward edge-assisted Internet of things: From security and efficiency perspectives [J]. IEEE Network, 2019, 33(2): 50-57

[2] Zhang Yuqing, Zhou Wei, Peng Anni, et al. 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)

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

[4] Lin Chao, He Debiao, Huang Xinyi, et al. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0[J]. Journal of Network and Computer Applications, 2018, 116: 42-52

[5] Ourad A Z, Belgacem B, Salah K. Using blockchain for IoT access control and authentication management [C] //Proc of the 3rd Int Conf on Internet of Things. Berlin: Springer, 2018: 150-164

[6] Ferraiolo D, Cugini J, Kuhn D R. Role-based access control (RBAC): Features and motivations [C] //Proc of the 11th Annual Computer Security Application Conf. Los Alamitos, CA: IEEE Computer Society, 1995: 241-48

[7] Yavari A, Panah A S, Georgakopoulos D, et al. Scalable role-based data disclosure control for the Internet of things [C] //Proc of the 37th Int Conf on Distributed Computing Systems. Piscataway, NJ: IEEE, 2017: 2226-2233

[8] Cruz J P, Kaji Y, Yanai N. RBAC-SC: Role-based access control using smart contract [J]. IEEE Access, 2018, 6: 12240-12251

[9] Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of things [J]. Mathematical and Computer Modelling, 2013, 58 (5/6): 1189-1205

[10] Mahalle P N, Anggorojati B, Prasad N R, et al. Identity authentication and capability based access control (IACAC) for the Internet of things [J]. Journal of Cyber Security and Mobility, 2013, 1(4): 309-348

[11] Xu Ronghua, Chen Yu, Blasch E, et al. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the IoT [J]. Computers, 2018, 7(3): Article No.39

[12] 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)

[13] Kaiwen S, Lihua Y. Attribute-role-based hybrid access control in the Internet of things [C] //Proc of the 16th Asia-Pacific Web Conf. Berlin: Springer, 2014: 333-343

[14] Hemdi M, Deters R. Using REST based protocol to enable ABAC within IoT systems [C] //Proc of the 7th Annual Information Technology, Electronics and Mobile Communication Conf. Piscataway, NJ: IEEE, 2016

[15] Maesa D D F, Mori P, Ricci L. Blockchain based access control [C] //Proc of the 17th IFIP Int Conf on Distributed Applications and Interoperable Systems. Berlin: Springer, 2017: 206-220

[16] Angin P, Mert M B, Mete O, et al. A blockchain-based decentralized security architecture for IoT [C] //Proc of the 11th Int Conf on Internet of Things. Berlin: Springer, 2018: 3-18

[17] Liu Aodi, Du Xuehui, Wang Na, et al. Research progress of blockchain technology and its application in information security [J]. Journal of Software, 2018, 29(7): 2092-2115 (in Chinese)
(刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7): 2092-2115)

[18] Ouaddah A, Elkalam A A, Ouahman A A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT [M] //Proc of Europe and MENA Cooperation Advances in Information and Communication Technologies. Berlin: Springer, 2017: 523-533

[19] Pahl C, El Ioini N, Helmer S. A decision framework for blockchain platforms for IoT and edge computing [C] //Proc of the 3rd Int Conf on Internet of Things, Big Data and Security. Lisbon, Portugal: Science and Technology Publications, 2018: 105-113

[20] Ren Yanbing, Li Xinghua, Liu Hai, et al. Blockchain based trust management framework for distributed Internet of things [J]. Journal of Computer Research and Development, 2018, 55(7): 108-124 (in Chinese)
(任彦冰, 李兴华, 刘海, 等. 基于区块链的分布式物联网信任管理方法研究[J]. 计算机研究与发展, 2018, 55(7): 108-124)

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

[22] Alansari S, Paci F, Sassone V. A distributed access control system for cloud federations [C] //Proc of the 37th Int Conf on Distributed Computing Systems. Piscataway, NJ: IEEE, 2017: 2131-2136

[23] Ding Sheng, Cao Jin, Li Chen, et al. A novel attribute-based access control scheme using blockchain for IoT [J]. IEEE Access, 2019, 7: 38431-38441

[24] Stihler M, Santin A O, Marcon A L. Managing distributed UCONabc policies with authorization assertions and policy templates [C] //Proc of 2015 IEEE Symp on Computers and Communication. Piscataway, NJ: IEEE, 2015: 619-624

Du Ruizhong, born in 1975. PhD, professor. Senior member of CCF. His main research interests include network security, trusted computing and network technology.

Liu Yan, born in 1993. Master candidate. Student member of CCF. Her main research interests include network security, IoT security and edge computing.

Tian Junfeng, born in 1964. PhD, professor, PhD supervisor. Senior member of CCF. His main research interests include distributed computing, network security, network technology.