基于区块链的智能家居认证与访问控制方案*

张利华[a], 张赣哲[b†], 曹 宇[b], 刘 季[a], 陈世宏[b]
(华东交通大学 a. 软件学院; b. 电气与自动化工程学院, 南昌 330013)

摘 要: 智能家居运用物联网技术为用户提供自动化的智能服务,但传统的集中式架构存在机密性和完整性等安全性问题,而现有的分布式架构又存在重复认证、高延迟等问题。针对这些问题,基于区块链和椭圆曲线集成加密技术提出了一种智能家居认证与访问控制方案,同时还引入了边缘计算,降低系统的延迟。并将基于权能的访问控制与区块链相结合,在区块链上存储权能令牌并设计了相应的智能合约以实现安全的访问控制。安全性分析表明,该方案具有去中心化、不可窜改、机密性、完整性和可扩展性等安全特性。在以太坊区块链上进行仿真,并根据计算开销、通信开销和响应时间等指标对方案进行了性能评估。评估结果表明,相比其他方案,该方案计算开销和通信开销更小,响应时间更短,具有明显的优势。

关键词: 智能家居; 认证; 访问控制; 区块链; 椭圆曲线; 边缘计算
中图分类号: TP309.2 **文献标志码**: A **文章编号**: 1001-3695(2022)03-038-0863-05
doi:10.19734/j.issn.1001-3695.2021.08.0321

Authentication and access control scheme for smart home based on blockchain

Zhang Lihua[a], Zhang Ganzhe[b†], Cao Yu[b], Liu Ji[a], Chen Shihong[b]
(*a. School of Software, b. School of Electrical & Automation Engineering, East China Jiaotong University, Nanchang* 330013, *China*)

Abstract: Smart home uses Internet of Things technology to provide users with automatic intelligent services, but the traditional centralized architectures have security problems such as confidentiality and integrity, while the existing distributed architectures have problems such as repeated authentication and high latency. To solve these problems, based on blockchain and elliptic curve integrated encryption technology, this paper proposed a smart home authentication and access control scheme. At the same time, it introduced edge computing to reduce the delay of the system. It also combined the capability based access control with the blockchain, stored the capability token on the blockchain, and designed the corresponding smart contract to achieve secure access control. Security analysis showed that the scheme had the security characteristics of decentralization, tamper proof, confidentiality, integrity and scalability. Simulated experiment was carried out on Ethereum blockchain, and the performance of the scheme was evaluated according to computing overhead, communication overhead and response time. The evaluation results show that compared with other schemes, this scheme has less computational and communication overhead and shorter response time, has obvious advantages.

Key words: smart home; authentication; access control; blockchain; elliptic curve; edge computing

0 引言

智能家居是物联网应用的一个典型实例,它将住宅作为主要平台,可以给家庭用户创造便利和舒适的环境。智能家居环境中的设备通过物联网技术连接起来,提供环境监测、危险预警、安全监控等多种智能化家庭服务[1]。智能家居系统主要由终端设备、移动 APP、物联网云端、通信网络四部分组成。随着智能家居系统的日益普及,其存在的安全问题引起了人们的广泛关注。在智能家居系统中,用户身份认证的主要目的是验证设备使用者的身份,防范非法用户对终端设备进行操控。多个用户希望能够访问共享设备提供的服务,需要避免重复认证问题。而访问控制机制决定了移动 APP 如何访问敏感资源,良好的访问控制机制能够有效地保护设备敏感资源[2]。因此,为了消除智能家居系统中的安全威胁,设计一种可靠、高效的认证与访问控制机制是很有必要的。

近年来,在智能家居安全研究领域,已经有相当多的研究成果。为了智能家居环境中的设备安全,Kang 等人[3]提出了一个增强的安全框架,该安全框架利用自签名和访问控制技术提供完整的系统,以防止数据修改、泄漏和代码伪造等安全威胁,针对完整性、可用性和身份验证都有相应的解决方法,缺点在于没有考虑智能家居设备是轻量级,计算能力普遍不强。Zhang 等人[4]设计了一种新的基于近邻的物联网设备认证机制 move2auth,以增强物联网设备的安全性,在 move2auth 中,要求用户手持智能手机,在智能家居设备附近完成移动或旋转操作,实现了手机与设备间的相互认证,该方案能够有效抵御攻击者的主动模拟攻击,但只考虑手机与设备之间的认证,未考虑手机与平台之间的认证。Jia 等人[5]提出了一个基于上下文的权限系统 ContexIoT,它为应用物联网平台提供上下文完整性,支持对敏感操作进行细粒度上下文识别,并提供丰富的上下文信息提示以帮助用户执行有效的访问控制,但由于太专业化而不容易让用户理解。Han 等人[6]提出了一个基于上下文的设备配对方案,使用固定时间内传感器测量信息作为密钥协商协议的秘密,实现了智能家居场景下不同设备的自动配对。Rahmati 等人[7]设计了一个基于风险的权限访问控制,它将设备操作按其风险相似度分组,并以组为单位授予相应的访问权限。

收稿日期: 2021-08-30; **修回日期**: 2021-09-30 **基金项目**: 国家自然科学基金资助项目(61563016);江西省教育厅科技项目基金资助项目(GJJ14371)

作者简介:张利华(1972-),男,副教授,博士,主要研究方向为信息安全、区块链技术;张赣哲(1996-),男(通信作者),硕士研究生,主要研究方向为区块链技术及其应用(2714218025@qq.com);曹宇(1996-),男,硕士研究生,主要研究方向为区块链技术;刘季(1996-),男,硕士研究生,主要研究方向为区块链技术;陈世宏(1996-),男,硕士研究生,主要研究方向为区块链技术.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

上述方案都采用的是集中式架构,存在单点故障问题。为了解决这些问题,引入了一种新兴的分布式技术,即区块链,其是一种按时间顺序将数据区块以顺序相连的方式组合而成的一种链式数据结构,并以密码学方式保证的不可窜改和不可伪造的分布式账本[8],具有去中心化、不可窜改、可追溯、匿名性和透明性五大特征,为系统提供了完整性和可用性。许多研究者将区块链技术引入到智能家居中,来解决隐私和安全问题。为了工业 4.0 应用建立具有细粒度访问控制的安全远程用户认证,Lin 等人[9]提出了基于区块链的框架 BSeIn,利用区块链的基本特性以及一些加密机制来实现分散、隐私保护和可审计功能,但是在该方案中用户无法得到有效的监管,没有一种有效的机制来跟踪执行恶意请求的用户。Hammi 等人[10]提出了一种独创的物联网身份验证系统,称之为 bubbles of trust,依赖区块链提供的安全优势,创建相互认同和信任的虚拟区域,可以弥补集中式认证系统的不足,实验证明该方案能够显著降低安全风险。Lee 等人[11]提出了一种基于区块链的智能家居网关网络,网络由设备层、网关层和云层三层组成,网关层采用区块链技术,以区块链的形式存储和交换数据,支持分散化,克服了传统集中式架构的安全问题,不足之处在于云端传输数据过程中数据可能会泄露,计算开销会加大。Li 等人[12]设计了一个有效的基于身份签名的增强消息认证隐私(IMAEP)方案,可以提供无条件隐私和全密钥暴露攻击下的增强隐私,在自适应选择消息和身份攻击下也能提供不可伪造性。针对轻量级的物联网设备,Tu 等人[13]提出基于 RFID 的轻量级相互认证协议,提供所需的安全性和隐私。文献[12,13]都未能考虑具体的应用实例,不适用于智能家居系统中。

虽然在智能家居系统中引入区块链技术可以解决一些安全隐私问题,但云计算产生的较大计算开销和通信开销成为了新的问题。与现有的研究不同,本文旨在提供一种安全、可扩展且轻量级的方案。因此,为了让用户对智能家居设备拥有更安全的认证机制,通过结合区块链和椭圆曲线集成加密技术,针对智能家居设备计算能力弱且轻量级的问题,采用基于权能的访问控制来实现,保证用户对设备的安全访问和控制,并且引入边缘计算确保比较小的计算开销和通信开销,因为使用边缘端比云端网络延时更低,可用性更强,数据在传输过程中也不会受到攻击。

1 预备知识

1.1 椭圆曲线集成加密

椭圆曲线集成加密方案(elliptic curve integrated encryption scheme,ECIES)是一种提供认证加密、数字签名、密钥交换以及对称加密密钥的公钥机制[14]。它加入一个基于对称密钥的非对称椭圆曲线密码体制,提供基于椭圆曲线私钥的数据加密和相应的椭圆曲线公钥的解密。椭圆曲线密码(elliptic curve cryptograph,ECC)拥有较小的密钥长度,只需 256 bit 的加密算法就能提供与 3 072 bit RSA 算法相当的安全性。因此,安全的身份验证、密钥生成、密钥交换以及通过云服务器在网络上传输所需的带宽较少。ECIES 的工作方式是从发送方的公钥生成一个对称密钥,与一般的密钥交换方法不同,在这种方法中,相同的密钥将被生成到接收方。使用基于 ECC 的密码体制的主要优点是密钥长度短,处理速度快,计算量较小,存储空间占用少,安全性高,可以抵挡选择明文攻击和选择密文攻击,非常适合在计算能力有限的设备上使用。

1.2 区块链

2008 年,Nakamoto 引入了区块链的概念,即比特币的底层技术。具体来说,区块链是一种分布式账本,它可以验证和存储交易,而无须依赖任何中央可信机构(与传统银行系统不同)[15]。它将焦点从集中的权威机构转移到网络中的每个节点,同时增强每个节点的自治性,而不是任意的第三方或中央服务器。在区块链网络中,所有参与者需要就交易数据状态达成共识,以获得信任。区块链具有透明性、隐私性和可追溯等安全特性,而它之所以具备以上特性,是因为区块链通过数据区块和链式结构来存储数据,如图 1 所示。每个数据区块包括区块头和区块体两部分,都有唯一的哈希值作为区块地址与之对应,当前区块通过存储前一区块哈希值与前一区块相连,从而形成链式结构。区块头中封装了前一区块链的哈希值、时间戳、Merkle 树根值等信息。区块体存储交易信息,即由区块链记录的数据信息,每笔交易都由交易方对其进行数字签名,从而确保数据未被伪造且不可窜改,每一笔已完成的交易都被永久性地记录在区块体中,供全体用户查询。

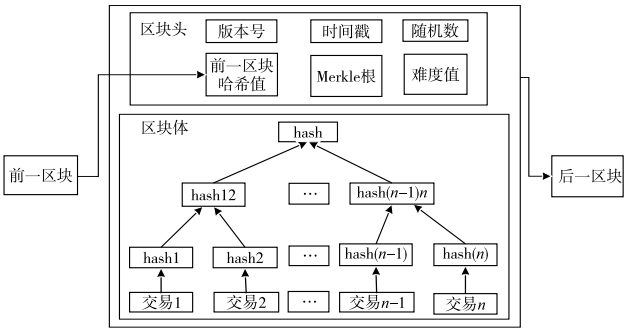


图 1 区块结构

Fig. 1 Block structure

区块链还通过智能合约提供计算基础设施,智能合约是在区块链网络上部署和执行的用户预定义程序。部署后,智能合约可以自动触发,以启用复杂的业务逻辑。

1.3 边缘计算

传统的云计算已不能适用于智能家居系统,而边缘计算是组建智能家居系统的最优平台。边缘计算是指一种新型的在网络边缘执行分布式计算的模型[16]。在该模型中,网络边缘设备已经具有足够的计算能力来实现源数据的本地处理,并将结果发送给云计算中心。边缘计算可以降低中心服务器的计算负载,减缓网络带宽的压力,提高计算的实时性和万物互联时代数据处理的效率;同时能较好地保护隐私数据,降低终端敏感数据隐私泄露的风险[17]。它将计算和通信资源从云转移到网络的边缘节点上,从而为边缘的用户提供更快的服务与计算响应,减少中间不必要的通信延迟和网络拥塞。

1.4 基于权能的访问控制

经典的访问控制方案有基于角色的访问控制(role based access control,RBAC)、基于属性的访问控制(attribute based access control,ABAC)和基于权能的访问控制(capability based access control,CapBAC)。RBAC 是主体对特定设备/数据/服务的访问,由主体在 RBAC 系统中的角色决定[18]。ABAC 定义了一组由不同属性(如用户属性、资源属性、环境属性)组成的访问策略,以确定特定访问权限的授予[19]。与其他方案相比,CapBAC 相对更轻量级,因为它只需要描述主体的访问权限,并通过令牌(token)授予权能[20]。然而,这些模型都依赖于集中式体系结构,这可能会引发严重的问题,因此需要更具可扩展性和分布式的设计来提供安全的访问控制管理。所以本文在传统 CapBAC 模型的基础上融合了区块链技术,提供安全可靠的环境。

2 系统模型

图 2 所示是本文构造的系统模型,由用户、移动 APP、终端设备、网关、边缘服务器(edge sever,ES)组成,其中用户指智能

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

家居的家庭成员,移动 APP 是用户用来与区块链网络进行交互的设备,终端设备如智能灯泡、智能电表(smart meter,SM)、智能监控、传感器等,是一些轻量级设备,可以充当区块链网络的轻节点。这些传感器和设备通过智能家居中配置的各种异构物联网收集和监控智能家居网络环境中的数据。网关和边缘服务器都是能力设备,它是指具有足够的计算、存储和通信资源的设备,作为区块链网络的全节点,可以进行交易的创建、验证以及查询等操作。网关存储设备层生成的数据,并根据需要提供给用户。边缘服务器充当边缘云,可以处理大量运算。

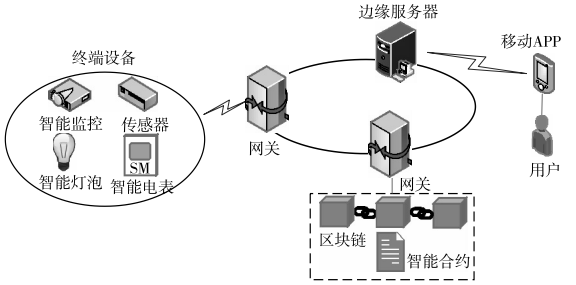


图 2　系统模型

Fig. 2　System model

首先,系统应该进行初始化,由边缘服务器执行,产生系统所需的公共参数以实现相应的加密函数。其次,用户和各类终端设备可以使用自己的身份 ID 向网络注册自身,其中设备还需要在区块链网络上为自己创建权能令牌。然后,用户需要登录认证,通过认证之后才可以进行访问请求。最后,用户先请求相应设备的权能令牌,再向网关请求设备服务访问,访问请求通过后可以对设备进行操作,这一阶段通过调用区块链上的智能合约来完成,智能合约中定义了与特权和服务相关的策略和约束。

3　方案设计

本章对所提方案进行详细的描述,基于系统模型,提出了在智能家居场景下基于区块链的认证与访问控制方案。该方案分为系统初始化、注册、认证和授权访问四个阶段。

3.1　系统初始化

此阶段由边缘服务器 ES 执行,ES 选择一条椭圆曲线 E,E 是定义在有限域 F_p 上的椭圆曲线,满足

$$y^2 = x^3 + ax + b(\mathrm{mod}\ p) \tag{1}$$

其中:p 是一个大于 3 的素数;$a,b \in F_p$,取其上一点 G。

使用椭圆曲线集成加密来确定通信所需的共享密钥,还使用 SHA256 哈希算法来进行加密确保传输数据的完整性。

3.2　注册

每个设备都有自己的标识 ID,需要先将设备的标识 ID 注册,生成设备唯一标识 DUID,再存储到区块链上,具体过程如图 3 所示。

a)网关先生成一个随机数 r_j,公钥 $PK_j = r_j \cdot G$,将公钥 PK_j 发送给终端设备。

b)终端设备将生成一个随机数 d_j,并计算 $R_j = d_j \cdot G$ 以及 $S_j = d_j \cdot PK_j$,将 R_j 发送给网关。

c)网关能够确定共享密钥 S_j,其中

$$S_j = d_j \cdot PK_j = d_j \cdot (r_j \cdot G) = r_j \cdot (d_j \cdot G) = r_j \cdot R_j \tag{2}$$

d)终端设备使用自己标识 ID_j,先用哈希函数 SHA256 计算 $H(ID_j)$,再用共享密钥 S_j 加密 $H(ID_j)$,得到 Enc(S_j,$H(ID_j)$),发送给网关。

e)网关收到加密消息,用共享密钥 S_j 解密 Dec(S_j,$H(ID_j)$),查询设备 ID_j 是否在设备列表中。

f)如果存在,则为其生成设备唯一标识 $DUID_j$,并存储到区块链上。如果不存在,则表明该设备是不合法的,断开连接。

类似地,为了确保用户的合法性,用户必须在 ES 上进行注册,具体过程如图 4 所示。

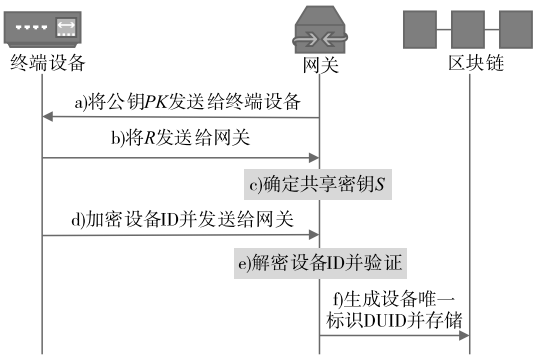


图 3　设备注册

Fig. 3　Device register

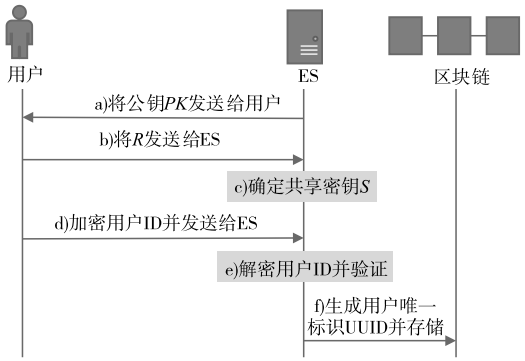


图 4　用户注册

Fig. 4　User register

a)ES 生成一个随机数 r_i,公钥 $PK_i = r_i \cdot G$,将公钥 PK_i 发送给用户。

b)用户通过移动设备生成一个随机数 d_i,并计算 $R_i = d_i \cdot G$ 以及 $S_i = d_i \cdot PK_i$,将 R_i 发送给 ES。

c)ES 能够确定共享密钥 S_i,其中

$$S_i = d_i \cdot PK_i = d_i \cdot (r_i \cdot G) = r_i \cdot (d_i \cdot G) = r_i \cdot R_i \tag{3}$$

d)用户选择一个身份 ID_i,并用哈希函数 SHA256 计算 $H(ID_i)$,用共享密钥 S_i 加密 $H(ID_i)$,得到 Enc(S_i,$H(ID_i)$),发送给 ES。

e)ES 收到加密消息,用共享密钥 S_i 解密 Dec(S_i,$H(ID_i)$),查询用户 ID_i 是否在智能家居的成员列表中。

f)如果存在,则为其生成用户唯一标识 $UUID_i$,并存储到区块链上。如果不存在,则表明该用户是非法用户,断开连接。

设备和用户完成本地注册之后,终端设备需要在区块链上为自己创建权能令牌,权能令牌如式(4)所示。

$$token_{cap} \rightarrow \{UUID, DUID, right, T\} \tag{4}$$

其中:$UUID$ 为用户注册的唯一标识;$DUID$ 为设备注册的唯一标识;$right$ 为特定设备服务的访问权限;T 为该设备令牌有效时间段。在注册阶段,利用随机数、hash 算法和椭圆曲线集成加密算法对终端设备和用户信息进行加密与解密,并将其存储在去中心化且不可窜改的区块链网络中。

3.3　认证

如果用户需要寻求某些特定的设备服务,在进行访问服务之前,用户必须通过认证,详细的认证过程如下:

a)用户通过移动设备输入他/她的 ID_i,然后移动设备连接到边缘服务器,进入区块链网络。

b)边缘服务器通过解码函数 $f(UUID_i) = ID_i$ 验证 ID_i 是否有其对应的 $UUID_i$,如果有,用户通过认证,否则,此会话结束。

c)因此,在设备和用户之间建立初始信任关系,以便进一

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

步交互。

d)用户认证过程被记录在区块链中,无法被窜改。

通过认证阶段的实现过程,用户进行了身份验证。由于用户 ID 与用户唯一标识 UUID 是一一映射的关系,避免了恶意用户的非法连接,同时能够有效地避免无线网络中常见的网络攻击,如中间人攻击等。

3.4 授权访问

授权访问过程如图 5 所示,用户通过认证之后,要想进行访问,需要有设备的权能令牌,设备的权能令牌存储在网关中。用户需要检查设备 DUID 以获取他/她应该连接到哪个网关,并联系该网关,向网关请求相应设备的权能令牌,这一过程需要调用区块链上的智能合约(获取令牌算法,即算法 1)用以获取设备权能令牌,验证通过后,该网关会将设备权能令牌发送给用户。用户再向网关请求设备服务访问,再次调用区块链上的智能合约(验证令牌服务算法,即算法 2),验证令牌以检查存储在相应的链上凭证中被授予的访问控制权限,返回验证结果,网关根据验证结果将所需的设备服务 API 和手册转发给用户,为用户提供设备服务访问,用户此时可以对终端设备进行访问操作。

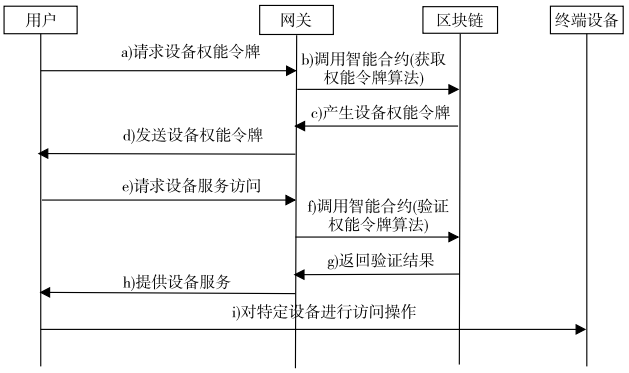


图 5 授权访问

Fig. 5 Authorized access

算法 1 为向通过认证的用户发送设备的权能令牌。算法 2 为验证用户是否有对设备的访问控制权限。

算法 1 获取令牌算法

a)从网关中获取服务列表
b)接受服务名称作为输入,并确定相应的服务 ID
c)传递服务 ID 和设备 ID 给“/fetchToken”路径去请求一个令牌
  如果响应为否定
    打印错误消息并退出
  否则
    转到步骤 d)
d)获取数据
  如果响应是“无效令牌”
    从服务器请求新令牌并转到步骤 e)
  否则
    打印收到的数据并返回到菜单
e)获取数据
  如果响应是“无效令牌”
    打印错误消息并退出

算法 2 验证令牌服务算法

a)如果请求设备没有被注册
    返回错误
  否则
    转到步骤 b)
b)如果服务不受支持
    返回错误
  否则
    转到步骤 c)
c)查询具有设备 ID 和服务 ID 的智能合约的访问权限
  如果设备不允许访问所请求的服务
    返回错误
  否则
    转到步骤 d)
d)如果所请求的服务存在已缓存的令牌
    转到步骤 e)
  否则
    转到步骤 f)
f)如果缓存的令牌已过期
    从身份验证服务器获取新令牌,缓存并返回
  否则
    返回缓存的令牌
g)从身份验证服务器获取新令牌,缓存并返回

系统中的每个参与者(即用户和物联网设备)被一个唯一的 UID 识别,并且特定设备服务的访问控制权限由权能令牌确定。与其他方案相比,基于权能的访问控制相对更轻量,因为它只需要描述主体的访问权限,并通过令牌授予权限。

对于未获得相应权限的设备,每次处理访问请求时被访问设备都会创建访问交易记录。如果全节点发现该设备存在超出可接受阈值的异常行为时,会将该设备从设备列表中清除,同时从区块链中查询所有该设备的权能令牌,调用各个令牌管理合约的令牌撤销接口冻结该异常节点的所有访问令牌。

4 性能分析

4.1 安全性分析

假设智能家居中的网关和边缘服务器都是诚实可信的。

引理 假设方案中所使用的椭圆曲线是密码学安全的,单向安全性是指在不知道私钥的情况下,由密文不能获得相应的明文,即敌手 A 成功地对加密算法 Enc 求逆的概率是可忽略的。

$$Succ_A = \Pr[(PK,SK)\leftarrow KG(\lambda);A(PK,Enc(PK,m))=m] \quad (5)$$

证明 当攻击者在传输信道中截获了公钥 PK 和 R,他想要通过 PK 和 R 分别求解出 r 和 d,等同于求解椭圆曲线离散对数问题。例如,已知 r 计算 $r \cdot G = PK$ 很容易,但通过 PK 计算相应的 r 非常困难,已有研究证明求解概率极低,可忽略不计。当敌手无法求出 r,那么他就不知道共享密钥 S,此时敌手成功从密文 $Enc(S,H(ID))$ 恢复出明文 $H(ID)$ 的概率 P_A 为

$$P_A = \Pr[(PK,S)\leftarrow KG(G);A(PK,Enc(PK,H(ID)))=H(ID)] \quad (6)$$

由引理可知 P_A 是可以忽略的,所以该方案可以实现单向安全性,证毕。除了单向安全性,该方案还具有防窜改等安全特性,同时能抵抗多种攻击。

a)防窜改。如果攻击者没有权能令牌,则无法通过访问请求进而访问数据。而且,权能令牌存储在区块链上,可以防止被攻击者窜改。

b)机密性。由于在整个访问控制过程中用户和设备都进行了认证,实体的每一个有效行为都会记录在区块链上,所以它比当前使用的一般身份认证方案更加安全。

c)完整性。当在每个实体之间发送和接收数据时,数据的传输过程不得出现伪造。哈希函数降低了这些数据被伪造的可能性,并允许精确跟踪和检查记录的数据。

d)抗假冒攻击。在该系统中,任何合法成员都可以访问授权设备,通过用户唯一标志符来防止冒名顶替行为。

e)抗重放攻击。网关或边缘服务器在每次会话请求中会生成一个新的密钥对,该密钥对用于加密响应信息和计算消息,由于生成的密钥对是最新的,所以可以抵抗任何重放攻击。

f)抗分布式拒绝服务(distributed denial of service,DDoS)攻击。区块链是基于点对点的分布式网络架构,如果一个节点出现故障,与故障节点连接的用户将无法进入到系统中,不会影响其他节点正常工作,能有效抵抗 DDoS 攻击。

表 1 将本文方案与当前其他研究成果进行了安全性对比。其中,“√”表示该方案具有这种特性,“×”表示不具有这种特性。可以看出,本文方案具有一定的优势。

4.2 实验分析

提出系统架构采用以太坊来构建,并以此作为测试和评估

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

的平台。在实验中,以太坊的节点分为全节点和轻节点。高性能设备成为全节点,如边缘服务器、网关。而性能一般的设备成为轻节点,如传感器。通过在 Linux 服务器上托管的独立虚拟机中运行 SDN 控制器来实现网关。Raspberry Pi 配置为 Raspbian 2019-09-26,用做边缘服务器。智能合约使用 Solidity v.0.4.20 以稳定的格式编写,分散的应用程序是使用 Truffle 开发套件部署和编译的,实验环境如表 2 所示。

表 1　各个方案对比

Tab.1　Comparison of various schemes

特性	文献[7]	文献[10]	文献[11]	本文方案
防窜改	×	√	√	√
机密性	√	√	×	√
完整性	√	√	√	√
去中心化	×	√	√	√
可扩展性	×	×	×	√

表 2　实验环境

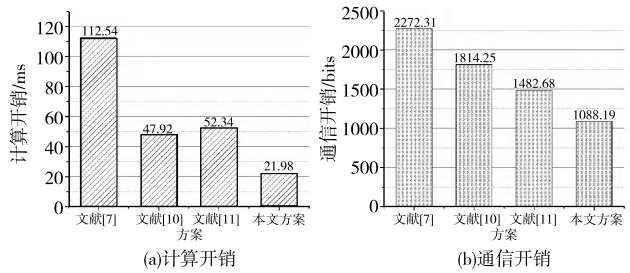
Tab.2　Experimental environment

软件/硬件	参数	软件/硬件	参数
操作系统	Ubuntu Linux 18.04 LTS	内存	8 GB
CPU	Intel Core 8565U 1.8 GHz	Raspberry Pi	3 B +
编写语言	Solidity		

以太坊智能合约不是直接运行在节点上,而是运行于以太坊虚拟机中。合约存储在以太坊的区块链上,并被编译为以太坊虚拟机字节码,通过虚拟机来运行。在终端打开 ethereum 文件夹,在终端命令行输入 node compile.js 命令,编译 Solidity 语言编写的智能合约,自动生成 build 文件夹,其中为编译过的智能合约;然后同样在终端,在 ethereum 文件夹下运行 node deploy.js 命令,通过 truffle-hdwallet-provider 编译过智能合约的 bytecode 提交到 Rinkeby 测试网。

在评估中,将所提网络架构与其他方案中网络架构的性能进行了比较。为了对方案进行分析,考虑了计算开销、通信开销和响应时间三个评价指标。对比方案为文献[7]的基于风险的访问控制方案,文献[10]基于区块链的身份验证方案和文献[11]结合云计算和区块链的智能家居访问控制方案。

首先,测试本文方案的计算开销,计算开销主要包括注册和认证阶段所涉及到的 ECIES 加解密算法、SHA256 算法和解码函数。实验中使用发起一次注册和认证请求所用的总时间作为计算开销,实验结果为 10 次测试的平均值。通过与文献[7,10,11]进行比较,如图 6(a)所示。可以看出,本文方案所花费的时间最少,这是因为采用的 ECC 密码密钥长度更短,计算速度更快。然后,还测试了通信开销,以发起一次访问请求所用的传输带宽作为本实验的通信开销,实验结果也为 10 次测试的平均值。同样进行对比,如图 6(b)所示。由于本文引入边缘计算,使用了边缘服务器来进行数据处理和传输,传输带宽更低,所以通信开销也就最低。



(a)计算开销　　(b)通信开销

图 6　各方案计算开销与通信开销的对比

Fig.6　Comparison of calculation and communication cost of each scheme

最后,测试了方案所用的响应时间,响应时间为发出访问请求到访问请求通过所用的时间。为了准确地模拟真实情况,将访问请求的数量分别设置为 5/10/15/20/25/30 个。同样与其他方案进行对比,如图 7 所示,可以看出本文方案所用响应时间最少,没有太多延迟。文献[7]采用的是集中式网络架构,开始时响应时间较少,但随着请求数量的增加,集中式的架构不足以处理越来越多的访问请求。文献[10,11]都采用的是分布式网络架构,并结合区块链,但访问请求是在云端进行处理。而本文方案是在边缘端进行处理,所以比起其他方案有更少的响应时间。

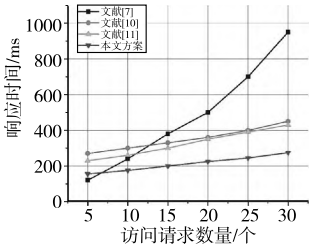


图 7　各方案响应时间的对比

Fig.7　Comparison of response time of each scheme

5　结束语

智能家居给人们带来了舒适便捷的生活环境,但网络通信传输安全问题不容乐观,人们的隐私安全正在遭受威胁。本文提出了基于区块链的智能家居认证与访问控制方案,该方案结合区块链与密码学技术,保护用户身份和设备信息,同时引入边缘计算保证高效的访问控制。用户和设备都有自己的唯一标志符,不需要额外的身份注册。因此,本文方案可以解决用户身份管理困难的问题。安全性分析表明本文方案具有数据防窜改、机密性、完整性和可扩展性等特点。实验结果表明,本文方案与传统方案相比具有更快的响应时间,能够提供服务的可用性。由于智能家居系统本身还有许多难题需要解决,所以本文方案具体实施还需要一段时间,可以为以后的智能家居研究作参考。

参考文献:

[1] Guhr N, Werth O, Blacha P P H, *et al*. Privacy concerns in the smart home context[J]. SN Applied Sciences,2020,2(2):1-12.

[2] 王基策,李意莲,贾岩,等.智能家居安全综述[J].计算机研究与发展,2018,55(10):2111-2124.(Wang Jice, Li Yilian, JiaYan, *et al*. Survey of smart home security[J]. Journal of Computer Research and Development,2018,55(10):2111-2124.)

[3] Kang W M, Moon S Y, Park J H. An enhanced security framework for home appliances in smart home[J]. Human-Centric Computing and Information Sciences,2017,7(1):1-12.

[4] Zhang Jiansong, Wang Zeyu, Yang Zhice, *et al*. Proximity based IoT device authentication[C]//Proc of IEEE Conference on Computer Communications. Piscataway,NJ:IEEE Press,2017:1-9.

[5] Jia Yunhan, Chen Q A, Wang Shiqi, *et al*. ContexIoT: towards providing contextual integrity to applified IoT platforms[EB/OL]. [2021-07-24]. http://dx.doi.org/10.14722/ndss.2017.23051.

[6] Han Jun, Chung A J, Sinha M K, *et al*. Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types[C]//Proc of the 39th IEEE Symposium on Security and Privacy. Piscataway,NJ:IEEE Press,2018:836-852.

[7] Rahmati A, Fernandes E, Eykholt K, *et al*. Tyche:risk-based permissions for smart home platforms[EB/OL]. [2021-07-24]. https://arxiv.org/pdf/1801.04609.pdf.

[8] 蔡晓晴,邓尧,张亮,等.区块链原理及其核心技术[J].计算机学报,2021,44(1):84-131.(Cai Xiaoqing, Deng Yao, Zhang Liang, *et al*. The principle and core technology of blockchain[J]. Chinese Journal of Computers,2021,44(1):84-131.)

[9] 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.

(下转第 873 页)

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

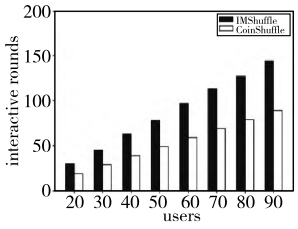


图 9　混币机制交互轮次对比
Fig. 9　Interactive round comparison of mixcoin mechanisms

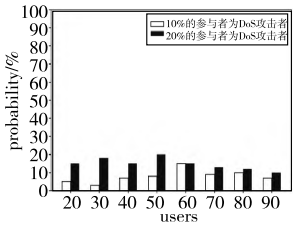


图 10　中间人为 DoS 攻击者的概率
Fig. 10 Probability that Intermediator is a DoS attacker

4　结束语

本文提出了一种基于中间人的混币机制(IMShuffle)。为了完善现有去中心化混币机制 CoinJoin、CoinShuffle 等存在的计算量大、效率低下、容易遭受拒绝服务攻击等问题,通过采用随机分组和选取中间人的方式实现输出地址的高效传递,保障了混币交易参与者的隐私,缩短了混币交易运行时间,提升了混币交易的效率,同时降低了遭受拒绝服务攻击的风险。经过实验分析可知,IMShuffle 机制相较于 CoinShuffle 机制来说在效率、安全等方面有着显著的优势。虽然该方案提升了混币交易的效率,保障了混币交易参与者的隐私安全,但是也存在一些缺点。例如,在混淆阶段每个小组的最后节点以及需要重新加密传递输出地址的部分参与者承担了比其他参与者更繁琐的任务,可能会导致这些参与者进行混币交易的积极性降低,在后续工作中将考虑引入激励方案以提高他们的积极性。

参考文献:

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2008-11-01)[2021-08-11]. http://bitcoin.org/bitcoin.pdf.

[2] Bartoletti M, Pompianu L. An empirical analysis of smart contracts: platforms, applications, and design patterns[C]//Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2017: 494-509.

[3] Androulaki E, Karame G O, Roeschlin M, *et al*. Evaluating user privacy in Bitcoin[C]//Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2013: 34-51.

[4] Rivest R L, Shamir A, Tauman Y. How to leak a secret? [C]// Proc of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 552-565.

[5] Gentry C. Fully homomorphic encryption using ideal lattices[C]// Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[6] Khalilov M C K, Levi A. A survey on anonymity and privacy in Bitcoin-like digital cash systems[J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 2543-2585.

[7] Philip K, Diana K, Patrick D M. An analysis of anonymity in Bitcoin using P2P network traffic[C]//Proc of International Conference on Financial Cryptography and Data Security-18th International Conference, Berlin: Springer, 2014: 469-485.

[8] Feng Qi, He Debiao, Zeadally S, *et al*. A survey on privacy protection in block chain system[J]. Journal of Network and Computer Application, 2019, 126(1): 46-58.

[9] Bonneau J, Narayanan A, Miller A, *et al*. Mixcoin: anonymity for Bitcoin with accountable mixes[C]//Proc of the 18th International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 486-504.

[10] Valenta L, Rowan B. Blindcoin: blinded, accountable mixes for Bitcoin[C]//Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 112-126.

[11] 张奥,白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报, 2020, 31(5): 1406-1434. (Zhang Ao, Bai Xiaoying. Survey of research and practices on blockchain privacy protection[J]. Journal of Software, 2020, 31(5): 1406-1434.)

[12] Maxwell G. CoinJoin: Bitcoin privacy for the real world[EB/OL]. (2013)[2021-08-11]. https://bitcointalk.org/index.php? topic = 279249.0.

[13] Ruffing T, Moreno S P, Kate A. CoinShuffle: practical decentralized coin mixing for Bitcoin[C]//Proc of European Symposium on Research in Computer Security. Berlin: Springer, 2014: 345-364.

[14] 李旭东,牛玉坤,魏凌波,等. 比特币隐私保护综述[J]. 密码学报, 2019, 6(2): 133-149. (Li Xudong, Niu Yukun, Wei Lingbo, *et al*. Overview on privacy protection in Bitcoin[J]. Journal of Cryptologic Research, 2019, 6(2): 133-149.)

[15] Maxwell G. CoinSwap: transaction graph disjoint trustless trading [EB/OL]. (2013)[2021-08-11]. https://bitcointalk.org/index.php? topic = 321228.0.

[16] Heilman E, Alshenibr L, Baldimtsi F, *et al*. TumbleBit: an untrusted Bitcoin-compatible anonymous payment hub[C]//Proc of the 24th Annual Network and Distributed System Security Symposium. 2017.

[17] Ziegeldorf J H, Grossmann F, Henze M, *et al*. CoinParty: secure multi-party mixing of Bitcoins[C]//Proc of the 5th ACM Conference on Data and Application Security and Privacy. New York: ACM Press, 2015: 75-86.

[18] 程其玲,金瑜. TTShuffle:一种区块链中基于两层洗牌的隐私保护机制[J]. 计算机应用研究, 2021, 38(2): 363-366, 371. (Cheng Qiling, Jin Yu. TTShuffle: privacy protection mechanism based on two-tier shuffling in blockchain[J]. Application Research of Computers, 2021, 38(2): 363-366, 371.)

(上接第 867 页)

[10] Hammi M T, Hammi B, Bellot P, *et al*. Bubbles of trust: a decentralized blockchain-based authentication system for IoT[J]. Computers & Security, 2018, 78: 126-142.

[11] Lee Y, Rathore S, Park J H, *et al*. A blockchain-based smart home gateway architecture for preventing data forgery[J]. Human-Centric Computing and Information Sciences, 2020, 10: article No. 9.

[12] Li Jian, Zhang Zhenjiang, Hui Lin, *et al*. A novel message authentication scheme with absolute privacy for the Internet of Things networks [J]. IEEE Access, 2020, 8: 39689-39699.

[13] Tu Y J, Kapoor G, Piramuthu S. Security of lightweight mutual authentication protocols[J]. The Journal of Supercomputing, 2021, 77(5): 4565-4581.

[14] Velmurugadass P, Dhanasekaran S, Shasi A S, *et al*. Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm[J]. Materials Today: Proceedings, 2020, 37: 2653-2659.

[15] Berdik D, Otoum S, Schmidt N, *et al*. A survey on blockchain for information systems management and security[J]. Information Processing and Management, 2020, 58(1): 102397.

[16] 黄倩怡,李志洋,谢文涛,等. 智能家居中的边缘计算[J]. 计算机研究与发展, 2020, 57(9): 1800-1809. (Huang Qianyi, Li Zhiyang, Xie Wentao, *et al*. Edge computing in smart homes[J]. Journal of Computer Research and Development, 2020, 57(9): 1800-1809.)

[17] Batalla J M, Gonciarz F. Deployment of smart home management system at the edge: mechanisms and protocols[J]. Neural Computing and Applications, 2019, 31(5): 1301-1315.

[18] Rao K, Nayak A, Ray I, *et al*. Role recommender-RBAC: optimizing user-role assignments in RBAC[J]. Computer Communications, 2021, 166: 140-153.

[19] 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.

[20] Liu Yue, Lu Qinghua, Chen Shiping, *et al*. Capability-based IoT access control using blockchain[J]. Digital Communications and Networks, 2021, 7(4): 463-469.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net