计算机科学与探索
Journal of Frontiers of Computer Science and Technology
1673-9418/2023/17(03)-0733-15
doi: 10.3778/j.issn.1673-9418.2206011

边缘计算与区块多链下的安全可信认证模型

黄敏敏[1],袁凌云[1,2+],潘　雪[1],张　杰[1]
1. 云南师范大学 信息学院,昆明 650500
2. 云南师范大学 民族教育信息化教育部重点实验室,昆明 650500
+ 通信作者 E-mail: blues520@sina.com

摘　要:边缘计算模式引发的数据安全和隐私保护等问题是制约边缘计算发展的基础性问题,而区块链因自身扩展性瓶颈,在解决边缘计算中的安全问题时受到了限制。为了解决边缘侧的信任管理及区块链的扩展性问题,促进边缘计算与区块链协同发展,基于边缘计算与主从多链提出了分布式安全可信认证模型。首先,基于传统单链设计了主从多链结构,并集成边缘计算部署了三层体系架构;针对边缘侧的安全性问题,基于椭圆曲线加密算法(ECC)集成区块链加密技术设计了签名认证方案。其次,基于角色的访问控制模型(RBAC)结合智能合约对用户权限进行了细粒度划分,构建了域间访问控制模型(ID-RBAC),并给出了域内、域间详细的访问认证流程设计。实验结果表明,该模型安全可信,与传统部署方式的单链架构相比,该方案存储开销平均下降50%,时延也有明显的降低。与现有方案相比,该方案在吞吐量方面有更大的优越性,发送速率与吞吐量之比达到1∶1,能满足大规模物联网实际应用需求,具有高扩展性、高安全性。

关键词:边缘计算;区块多链;跨域;身份认证;信任管理
文献标志码:A　　**中图分类号:**TP309;TN929.5

Secure and Trusted Authentication Model Under Edge Computing and Multi-blockchain

HUANG Minmin[1], YUAN Lingyun[1,2+], PAN Xue[1], ZHANG Jie[1]
1. College of Information Science and Technology, Yunnan Normal University, Kunming 650500, China
2. Key Laboratory of Educational Information for Nationalities, Ministry of Education, Yunnan Normal University, Kunming 650500, China

Abstract: Issues such as data security and privacy protection caused by the edge computing model are fundamental problems that restrict the development of edge computing, while blockchain is limited in solving security problems in edge computing due to its own scalability bottleneck. In order to solve the trust management at the edge side and the scalability of blockchain, and promote the synergistic development of edge computing and blockchain, this paper proposes a distributed secure and trusted authentication model based on edge computing with master-slave multiple chains. Firstly, a master-slave multi-chain structure is designed based on traditional single chain and a three-tier architecture is deployed by integrating edge computing. A signature authentication scheme for edge computing security based on elliptic curve cryptography (ECC) integrated with blockchain cryptography is also proposed. Secondly, an inter domain-role-based access control (ID-RBAC) is constructed based on role-based access control

基金项目:国家自然科学基金(62262073);云南省应用基础研究计划项目(202101AT070098);云南省万人计划青年拔尖人才项目。
This work was supported by the National Natural Science Foundation of China (62262073), the Applied Basic Research Program of Yunnan Province (202101AT070098), and the Ten-Thousand Talents Program of Yunnan Province.
收稿日期:2022-06-02　　**修回日期:**2022-08-29

(RBAC) combined with smart contracts for fine-grained division of user privileges, and a detailed access authentication process within and between domains is given. Experimental results show that the model is secure and trustworthy, and the storage overhead of this scheme is reduced by about 50% on average and the latency is significantly reduced, compared with the single-chain architecture of traditional deployment methods. Compared with existing methods, the proposed scheme in this paper has greater superiority in throughput, with the ratio of sending rate to throughput reaching 1:1, which can meet the demand of large-scale IoT practical applications with high scalability and high security.

Key words: edge computing; multi-blockchain; cross-domain; authentication; trust management

物联网(Internet of things,IoT)即“万物相连的互联网”,是指将各种传感设备与网络结合起来形成的一个大型网络。现该网络数据的增长速度已远超集中式处理模式网络带宽的负载限制,已不能满足IoT多维、实时的服务请求。边缘计算作为新型计算范式被提出[1],为IoT异构设备间的实时通信、协作和存储提供了理想场景。欧洲电信标准化协会(European Telecommunication Standard Institute, ETSI)将边缘计算定义为在移动网络、近无线接入网络(radio access network,RAN)和移动用户的边缘侧提供互联网服务环境和云计算功能[2]。即提供服务的边缘节点是大面积分散、多样化及不确定的,故边缘节点是置于不可信环境中的。当恶意节点接入后,可协助相应的恶意应用服务跳过相关的安全认证机制,并提供攻击其他边缘设备以窃取用户隐私的机会,数据的安全性受到了严峻的挑战。为了促进边缘计算在IoT应用中的发展,其数据的安全访问问题亟需解决。

区块链作为一项新型信息处理技术,已成为满足IoT网络安全需求最有前途的技术之一,在安全、访问控制方面存在天然的优势[3],为学术界解决边缘计算模式下的数据安全和隐私保护等问题提供了新思路。2020年,中国移动5G联合创新中心发布的《区块链+边缘计算技术白皮书》明确了边缘计算与区块链技术的结合是相互促进、协同发展的。但是区块链1.0即比特币(bitcoin,BTC)和区块链2.0即以太坊(ethereum,ETH)为追求去中心化而牺牲了扩展性[4]。且随着交易量的日益增加,系统整体性能受单个节点性能上限的限制越发明显,导致了中央服务器的成本和性能瓶颈[5]。此外,区块链网络的安全性是基于每个节点在链上存储所有事务以进行验证得以保证的,故需要高扩展性以支持其高安全性。这些问题阻碍其在边缘计算安全问题上发挥最大的作用,不符合边缘计算大带宽、低延时的服务宗旨。

针对区块链性能瓶颈问题,有研究提出了链上、链下扩容方案,而扩容方案应用过程中的安全性与性能之间又是互相制约的关系[6],特别体现在跨链交互问题上。故基于扩容方案部署边缘计算网络架构,需考虑区块链所构成的边缘信任域之间的安全交互问题。且域间设备安全交互过程中还存在身份认证难、访问控制难及隐私保护难等[7]问题。现有构建域间信任的方式,一般是在域内设置中心管理机构来管理和验证身份。因是中心化的认证方式,其节点设备间无法进行身份的相互验证,缺乏跨域身份信任,导致不同信任域的IoT设备无法便捷地互相访问,同时数据也无法安全共享[8]。

针对上述边缘计算与区块链网络架构中的数据安全、跨域身份认证难题,本文设计了主从多链结构,并集成边缘计算提出了一种支持跨域访问控制的高扩展性分布式可信认证模型。本文的主要贡献包括四方面:

(1)针对区块链扩展性瓶颈,采用链下扩容方法设计了可无限伸缩的主从多链结构。将大量的跨域工作转移到主链上,减轻了从链的交易负担。而从链无需向主链提交所有的交易数据便可提供数据可用性证明。

(2)基于链上扩容方案的实现思路,将主从多链集合到边缘计算上,部署了三层体系架构。并基于椭圆曲线加密算法(elliptic curve cryptography,ECC)设计了边缘节点的安全接入流程。通过主从链赋予边缘可信,提高了网络架构的安全性与计算有效性。

(3)基于RBAC(role-based access control)提出了域间访问控制模型(inter domain-role-based access control,ID-RBAC)。并结合智能合约与角色权限设计了细粒度的访问控制策略。

(4)基于ID-RBAC模型设计了域内、域间访问控制机制,包括具体的身份认证流程、跨域数据管理方法。

1 相关工作

边缘网络架构在异构边缘节点的相互作用和跨边缘节点的服务迁移下，数据的安全性风险增加。依托区块链技术的分布式存储、共识机制、加密不可篡改等特点，许多研究基于区块链赋予边缘网络安全可靠的访问与控制。Ma等人[9]提出了一种基于区块链的可信数据管理方案，是满足可配置的边缘区块链安全系统。Pan等人[10]定义了边缘链，提出了一种基于区块链和智能合约的边缘物联网系统。程冠杰等人[11]提出一种基于区块链与边缘计算的物联网数据管理架构。这些方法中，区块链技术的加持维护了数据的安全性，但因目前区块链扩展能力的有限性，一定程度上限制了其支持边缘计算中频繁事务的访问处理能力。虽然边缘计算将区块链从受限的设备中卸载了出来，但并未真正解决区块链扩展性问题，整体性能上缺少优势。可见，目前区块链的存储和计算能力还不足以应对两者集成后分散管理的性能挑战。

吞吐量低、数据存储困难和可扩展性差等引起的性能问题极大地限制了区块链的发展[12]。鉴于此，众多研究学者对区块链扩容技术展开了研究。区块链扩容技术包括链上、链下两种方法。其中链上扩容[13-14]方案通过改变基本协议来提升区块链整体性能，但存在节点故障导致数据丢失等问题。不改变基本协议而对应用层进行改变以提升扩展性的链下扩容[15-17]方案，将各服务压力转移到链下处理，以减轻主链的负担，但不可避免地加剧了系统的中心化程度。同时，系统中因多条链的存在，势必涉及链之间的安全交互问题，且其交互过程中会产生大量的密码数据，节点因此受到繁重的计算、验证负担。许多研究在扩容技术的基础上集成了边缘计算，致力于促进区块链扩容技术的发展，以强化其与边缘计算集成的协同作用。Li等人[18]通过边缘计算来构建区块链系统，利用边缘计算富余的算力解决复杂的密码学计算问题。Chuang等人[19]提出了分层区块链，并通过边缘计算来减轻区块链系统运行带来的存储和计算负担。这些方案在扩容的基础上集成边缘计算，形成安全的分布式处理模式，两者协同发展提高了系统的整体服务能力。但该模式下的信息系统与数据是分域管理的，信息系统呈现域内互联、域间孤立的特征，若不能关注到该特征，域间的设备和数据容易出现明显的“孤岛”现象。

为了解决各应用域间的安全性、共享性问题，许多学者对跨域共享展开了研究。传统的跨域共享机制采用集中式的身份认证方法，如基于证书的公钥基础设施（public key infrastructure，PKI）[20]和基于身份的密码体制（identity-based cryptography，IBC）[21]。这种集中式处理方法的认证资源极易耗尽，认证效率不稳定，特别不适用于多设备的服务场景，这与要求实时、高效地处理多并发事务边缘计算发展模式不匹配。而在大规模跨域场景应用中，陈彦冰等人[22]通过引入区块链和无证书认证技术，提出一种基于医疗联盟链安全高效的跨域认证方案。赵平等人[23]设计了主从区块链身份认证结构和匹配使用的分层拜占庭容错算法，实现了双向异构跨域身份认证，其身份认证较繁琐复杂，产生大量的计算开销。基于区块链扩容技术，Jiang等人[13]基于图结构的IOTA（Internet of things application）即Tangle平台设计了跨链框架，区块链的扩展性得到了提高，但该方法涉及到的用户隐私数据问题并未解决。Zhang等人[24]提出了一种完全跨域的方法。Guo等人[25]设计了一种支持分布式跨域身份验证的主从区块链体系结构，解决了一定的用户隐私问题，但其对隐私数据的访问权限划分不明确，不能做到数据的细粒度访问控制，存在隐私数据过度访问等问题。

上述各模型的安全方案对区块链技术的依赖，致使这些方案在实现数据安全保护的同时，还要考虑区块链性能受限的问题。而要兼顾高性能与高安全性要求，区块链需要更具可扩展性和分布式的设计。故本文重点关注边缘计算和区块链扩容技术的协同作用，以高性能、低功耗以及高扩展性的方式在边缘侧部署访问控制模型。兼顾区块链的安全与性能，设计更加完善且有效的安全方案，以进一步解决边缘计算场景下应用服务的跨域身份认证与数据安全共享等问题。

2 主从链下的分布式可信认证模型

2.1 主从多链设计

为突破传统单链性能瓶颈，设计了主从多链结构，如图1所示（图中，Node0为通信节点，其余为普通节点）。该主从多链结构包括一条主链（main chain，MC）和多条从链（slave chain，SC）。SC作为域内的可信平台，对域内访问操作进行管理，并定义了普通节点和通信节点，普通节点负责数据存储，通信节点是网络交互的枢纽，连接到MC。MC是从链间交互的桥梁，用于解析跨链请求，实现可信身份认证。

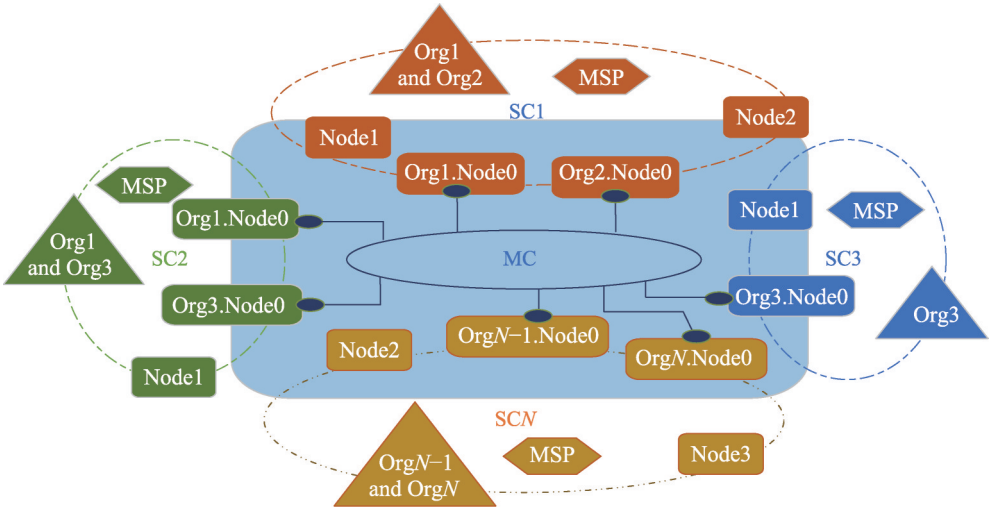


图1 主从多链结构

Fig.1 Master-slave multi-chain structure

MC定义了通信节点和缓存节点，通信节点与SC网络进行交互，实现链之间的互联、互通，缓存节点通过CouchDB状态数据库缓存跨域数据。通信节点构成MC与SC的索引，将多个SC衔接起来构成一个无限扩展的主从多链，具有很好的灵活性和扩展性。成员关系服务提供者（membership service provider，MSP）是证书管理服务器，参与本地区块链账本的维护，为加入区块链的节点进行身份审核和证书发放。

主从链结构的优点在于其可伸缩性强，可通过动态扩展从链，使得整个系统的性能不会受限于某个链，打破其可扩展性瓶颈。而主链作为可信认证平台，保存其交易的哈希时间锁，维护了从链间交易的原子性。

2.2 基于主从多链的分布式安全架构

在主从多链下集成边缘计算设计了三层分布式安全架构，如图2所示，包括设备层、从链网络及主链网络，三层自下向上服务。设备层为上层提供可信计算服务，该层中的边缘设备通过身份注册流程后，接入从链网络，组成从链网络的“矿工”——边缘节点（edge node，En）。*En*将数据预处理后存储于SC节点中，SC为当前所在域的设备提供安全的数据存储环境及域内访问控制；SC与MC中的通信节点共同维护可靠的通信，为跨域访问控制提供服务。主链网络支持跨不同SC域之间进行访问。该三层架构覆盖了区块链和边缘计算的核心功能，从存储、网络和计算不同层面提供了分布式安全服务。架构中的从链、边缘节点可根据需求进行开发，是一个无限扩展的联盟。

（1）下层为设备层，该层设两个功能模块：感知模块、设备管理模块。其中设备管理模块设计了基于密码学的安全接入流程，设备需经过该流程的验证才可成为合法的*En*。

（2）中间层为从链网络，该层包含了数据处理和域内访问控制两个功能模块。在数据处理模块中，*En*对设备层采集到的数据进行预处理，并统一格式后打包成块，存储于SC帐本；域内访问控制模块是中间层的核心功能模块，实现物联网域内访问管理。

（3）上层为主链网络，该层作为域间的可信共享平台，是数据跨域管理的控制器。该层设置了缓存模块、域间访问控制模块，域间访问控制模块联合SC共同管理跨域访问行为，缓存模块对跨域数据及相关信息进行缓存。

2.3 基于RBAC的域间访问控制模型

2.3.1 ID-RBAC模型

在物联网访问控制方案中，常见的访问控制模型有属性集、权限集等，这些方法的集合保护措施不够安全，且设计成本较高[26]。在边缘计算和区块多链架构下，多设备、多节点的接入，加剧了访问与权限的复杂关系，使得授权管理变得繁琐。同时频繁申请、授权与访问操作更是加大了权限管理成本。基于角色的访问控制模型可以解耦用户与权限的关系，并支持层次化的权限分级和权限继承，极大简化了权限的管理。但因其是根据角色划分用户权限，导致实现细粒度的访问控制变得困难，通常需要创建更具体的角色版本或设计其他机制[27]。

智能合约具有高准确性和智能性，不需人为参与

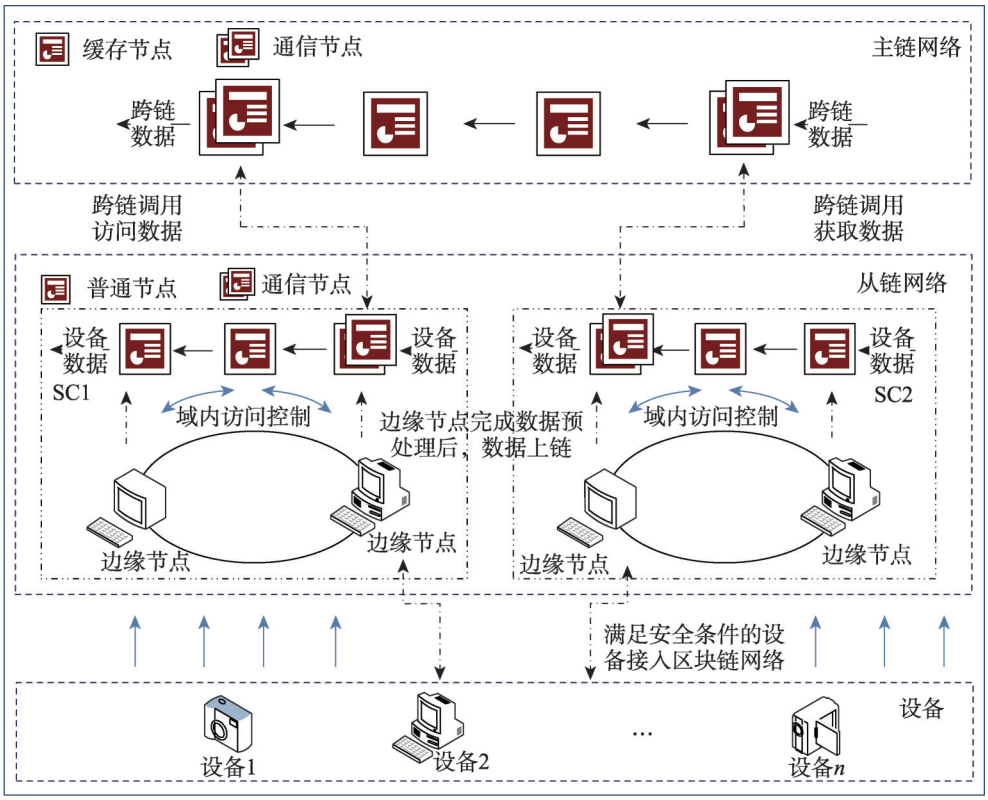


图2　分布式安全架构

Fig.2　Distributed security architecture

便可自动执行。通过智能合约为访问用户分配与他们身份信息相符的角色，使接受角色与用户的关系转变要比角色对应权限的转变更频繁[28]，即可降低授权的复杂性，并减少组织的管理成本。因此本文以RBAC模型为基础，利用智能合约来进行用户、角色与权限的逻辑划分，提出域间访问控制模型ID-RBAC。

在ID-RBAC模型下，设计了动态授权机制，该机制可以动态调整用户在不同状态下的权限。授权规则如角色A持有权限Ⅰ，在域内访问流程中满足授权策略，权限Ⅰ被授权。而在域间访问流程中，该权限不能满足所跨域的授权策略时，权限Ⅰ被限制授权。即同一个角色对于同一个访问内容，应具有相同的权限，而在ID-RBAC中，在域内和域间访问过程中权限却可能不同，这是因为采用了细粒度划分的合约机制。针对不同域中复杂的授权状态，ID-RBAC模型是灵活可用的。当系统中需增加角色时，可将其写入到合约机制中，进行权限动态授权。ID-RBAC较传统RBAC的扩展性、灵活性更优。

2.3.2　ID-RBAC的合约设计

角色的分配及访问控制过程通过智能合约实现，基于ID-RBAC设计了五个合约，分别实现数据存储的管理、隐私数据的访问控制、用户角色的管理、数据跨域访问控制及跨域数据的缓存转发。

（1）数据管理合约（data management contract，DMC）{地址，资源，属性}，DMC用于管理上链的数据，通过DMC合约对数据进行分域与分类管理。地址指明某数据资源所处的IoT域，属性说明数据资源的数据类型。

（2）隐私数据合约（private data contract，PDC）{DMC属性，策略Policy，时间}，通过DMC合约的数据属性构建隐私数据集合（privacy dataset，PDS），并将PDS存储于私有数据库（Private-DB），PDS是系统特定成员（Member）所私有，其算法如下：

算法1　PDC

输入：数据属性，策略 *Policy*，时间，数据 K。

输出：隐私数据集合 *PDS*。

1. *name*=*build Name*(*PDS*)

2. *Policy*=OR(*Org*$_1$*MSP.member*, *Org*$_2$*MSP.member*, …, *Org*$_x$*MSP.member*) /*定义集合访问策略*/

3. if *member*　*OnlyRead* =True /*共识*/

4. push *PDS* to *blockchain* /*背书通过则将所创建的PDS集合写入合约*/

5. else

6. return False

7. PDS ToLive=100000 /*定义集合的有效时间*/

8. return *PDS*

(3)角色管理合约(role management contract, RMC){用户属性, 用户地址, *PDC*-*Policy*结果, 用户, {角色1,角色2,…,角色*N*},{权限1,权限2,…,权限*N*}}。当新用户加入网络时,RMC根据其属性、所在域进行身份匹配,一个用户可同时拥有多个角色。

根据用户处于不同物联网域,可分同域和异域用户,一个从链维护一个域,故每个域都有相对应的账本,因此域间权限的划分主要针对该域所维护的账本。域所对应的权限如表1。

表1 域权限的划分

Table 1 Division of domain authority

角色	权限
IoT1-member	可进入IoT1对应的SC1账本
IoT2-member	可进入IoT2对应的SC2账本
IoT3-member	可进入IoT3对应的SC3账本

为了实现细粒度的访问控制,本文对每个账本内的数据进行了分类,并设计了不同的访问“门槛”。根据RMC合约对域内用户划分了Ⅰ级、Ⅱ级、Ⅲ级及Ⅳ级,各等级对应的权限如表2。

表2 角色等级与权限的关系

Table 2 Relationship between role level and authority

用户	角色	权限
用户A	Ⅳ级	可访问账本的Public-DB数据
用户B	Ⅲ级	可访问账本中的Public-DB数据、Private-DB1数据
用户C	Ⅱ级	可访问账本中的Public-DB数据、Private-DB2数据
用户D	Ⅰ级	可增删改查账本中的Public-DB、Private-DB1、Private-DB2数据

(4)跨域合约(cross domain contract,CrossD){访问属性,RMC结果},根据请求操作解析访问属性,并结合RMC获取相应权限后跨域调用。

(5)缓存合约(cache contract,cacheC){CrossD结果,属性},通过CrossD的结果执行CacheC,并根据数据属性进行分类缓存。

跨域访问及缓存算法如下:

算法2 跨域缓存

输入:$Sig_{SK_{SC1}}(PK_C,Sig_{SK_C}(Ar)),PK_{SC1}$ /* *Ar* 所打包的访问请求信息*/

输出:PK_{SC2} and *Datablock* or *Error*(*message*)。

1. *func*(*t***AccessChaincode*) /*初始化访问请求*/

2. *Init*(*stub shim.ChaincodeStubInterface*) /*初始化跨域接口*/

3. use PK_{SC1} parse the message. *M* /*解析跨域访问请求的消息*M*/

4. *verifyRes* = *DMC*(*shim.Success*)&*PDC*(*shim.Success*)&*RMC*(*shim.Success*) /*调用合约验证*/

5. if *Ar* is invalid /*打包好的 *Ar* 是否有效*/
return False

6. else if $Sig_{SK_C}(M)$ is illegal /*如果跨域访问消息不合法*/

7. return *Error* ($Sig_{SK_C}(M)$ is illegal) /*返回错误消息*/

8. else

9. signature $Sig_{SK_{MC}}(PK_D,Sig_{SK_D}(M))$ /*MC进行数字签名*/

10. forward with PK_{MC} and $Sig_{SK_{MC}}(PK_D,Sig_{SK_D}(M))$ to *SC*2

11. execution RMC /*调用RMC合约*/

12. use RMC role authorization

13. if $Sig_{SK_{SC2}}(Ar)$ not meet authorization

14. return *Error* ($Sig_{SK_{SC2}}(Ar)$ is illegal)

15. else if $C \notin Policy_{SC2}$ /*如果跨域用户所申请的访问内容不满足访问策略*/

16. return *Error* ($C \notin Policy_{SC2}$) /*返回错误消息*/

17. else

18. generate $Cert_C$ /*生成跨域访问证书*/

19. forward with $Cert_C$ to SC1-C /*返回跨域访问证书给用户 *C* */

20. use *Ar* and $Cert_C$ to get the *Ac* /*获取访问数据信息*/

21. generate *Datablock* = $Sig_{SK_{SC2}}\{Ac(stub.PutState(data_i))\}$ /*缓存数据*/

22. return PK_{SC2} and *Datablock*

3 访问控制流程设计

3.1 边缘初始化

为了确保提供计算服务的边缘节点安全性,设计了如图3的安全接入流程,包括初值设定、注册及身份认证流程。其中初值设定的初始化由 *En* 执行,通过ECC生成公私钥对,作为系统所需的公共参数。结合设备MAC(media access control)地址值获取其身份信息 *Enc* ,并将其打包存储到区块链上,以向区块链网络注册自身。当设备A向设备B发起访问请求

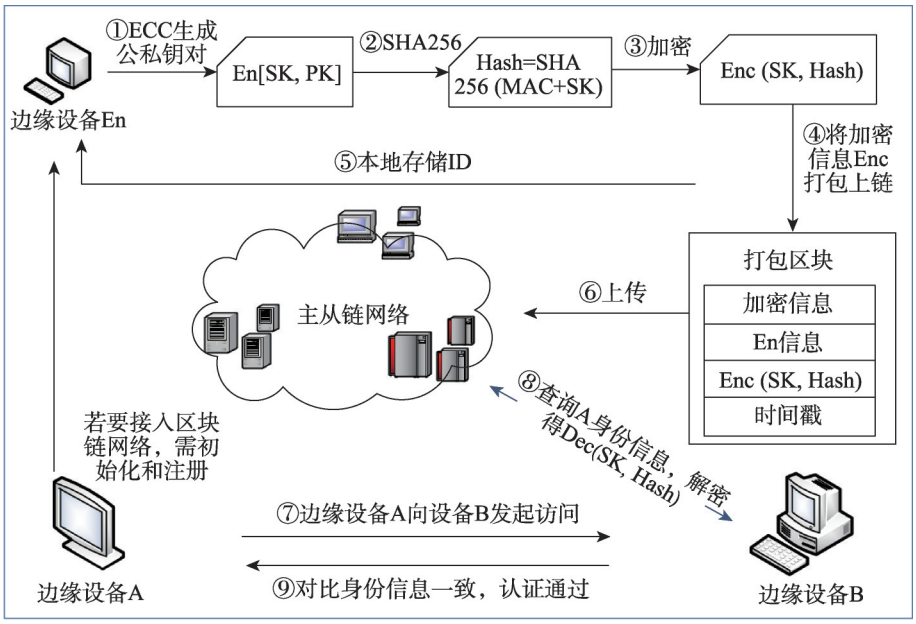


图3 认证流程

Fig.3 Certification process

时，设备B通过区块链网络验证A的身份信息。

其边缘节点认证具体流程如下：

(1)初值设定

加入区块链网络的 En 采用ECC计算公钥和私钥。当 Q 在有限域 Fp 上满足大于3的素数时，整数对 p 取模，有方程 E：

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

其中，$a,b \in Fp, Ep(a,b)$，取任意数 K 得到私钥 SK。取椭圆曲线上基点 Q，生成公钥 $PK=Q*SK$，并将公钥进行全网广播。

(2)注册

将 En 的 MAC 地址和 SK 值输入式(2)，计算得到 $Hash$。通过SK对其进行加密得到 $Enc(SK,Hash)$，并将 Enc 存储在本地及区块链上，完成注册。

$$Hash = SHA256(MAC + SK) \tag{2}$$

(3)身份认证

En 成为矿工前需得到一致性认可，即全网节点对其身份进行验证。当节点 A 向节点 B 发起访问等行为时，节点 B 查询区块链上是否存在 A 的身份信息。①存在，则通过 A 发布的 PK 对 $Enc(SK,Hash)$ 进行解密，得到 $Dec(SK,Hash)$，并与 $Enc(SK,Hash)$ 进行对比，对比结果一致则证明该节点是合法的，认证通过。否则该节点已被污染，或是恶意节点伪造。②不存在，该节点不合法，断开连接。身份认证避免了节点的伪造冒充，阻止将数据交付到恶意节点中。至此 En 与数据账本建立了初始信任关系。

3.2 域初始化

颁发、校验证书的MSP为加入主从链网络的各物联网域及各实体生成公钥、私钥，并将域及用户发布到主从链网络中。

(1)发布域 $(Hash_X(pk_{MSPx}), Sign_X, Hash_X)$，其中 $Hash_X(pk_{MSPx})$ 是 pk_{MSPx} 的哈希值，$Sign_X$ 与 $Hash_X$ 分别表示域 X 进行的数字签名及哈希运算。

(2)发布用户 $(Hash_X(pk_{UAi}), Hash_X(pk_{MSPx}), State)$，其中 pk_{UAi} 表示域 X 中 Uxi 用户的公钥，$State$ 表示用户身份信息是否可用。

(3)验证 $(pk_{UAi}, Sign_X(sk_{UAi}, N), N, Hash_X(pk_{MSPx}))$，$N$ 是进行哈希计算的随机数。

(4)将验证结果存储到主从链账本中。

(5)区块链网络验证通过，开始响应发布域 $(Hash_X(pk_{MSPx}), Sign_X, Hash_X, Sta_{BC})$ 与发布用户 $(Hash_X(pk_{UAi}), Hash_X(pk_{MSPx}), State)$ 请求。Sta_{BC} 表示维护该新发布域的区块链网络信息。

3.3 访问授权

3.3.1 隐私数据访问管理

PDC和RMC对隐私数据进行了分层保护。PDC为每个域的隐私数据定义了隐私数据集合(privacy data set，PDS)，RMC通过PDS里定义的访问策略 $Policy_N$ 访问管理。

定义1 隐私数据访问策略：$Policy_N$（隐私数据属

性 $Type$，所在域 $Domain$，访问权限 P）。

具体表示为：

$$Policy_N=\left\{\begin{array}{l}(Type1,IoT1,Level-\mathrm{Ⅳ})\\ \left(Type2,IoT2,\left\{\begin{array}{l}Level-\mathrm{Ⅳ},\\ Level-\mathrm{Ⅲ}\end{array}\right\}\right)\cdots\\ \left(Typei,IoTi,\left\{\begin{array}{l}Level-\mathrm{Ⅳ},\\ Level-\mathrm{I},\cdots\end{array}\right\}\right)\end{array}\right\}$$

隐私数据访问管理流程如图4所示。设Org1有三个属性的数据{*Public-DB*1(属性1,属性2),*Private-DB*1(属性3)}。属性3划分在隐私数据集合中,存储于私有数据库中。同一个链上的组织成员可共享 *Public-DB*1 中的数据,而 *Private-DB*1 中的数据为Org1私有,隐私数据策略 $Policy_1$ 表示为：

$$Policy_1=\{Type3,IoT1,Level_{\mathrm{Ⅳ}}-Org1\}$$

3.3.2 域内访问

域内访问指访问行为发生在同一个边缘物联网域下的不同IoT系统。如图5所示,设SC1所管理的域中有用户 A、用户 B,用户 A 在SC1中向用户 B 发布访问行为。

(1)IoT1-A向MSP发送一个状态为身份注册的请求,MSP验证通过后向其返回身份证书 $Cert_A$,$Time$ 表示 $Cert_A$ 的有效时间。

$$A\rightarrow MSP:\left\{pk_{UA},Status,Sig_{sk_{IoT1}}\left(\begin{array}{l}sk_{UA},\\ Hash_A(pk_{UA})\end{array}\right)\right\}$$

$$MSP\rightarrow A:Cert_A\left\{sig_{MSP_{pk}}(States:True,Time)\right\}$$

(2) A 将其 $Cert_A$、自身信息及访问内容 Ac 三者打包成访问请求 Ar。Ar 打包成功后会被写入到帐本中,区块高度增加1。$Packaged_{A_{Ar}}$ 为当前 Ar 打包的状态,状态有两种标识:Success OR failure。

$$A:Ar\left\{\left(\begin{array}{l}Cert_A,Owner,\\ Ac(where,Dt)\end{array}\right),Packaged_{A_{Ar}}\right\}\rightarrow block++$$

将 Ar 发送到SC1以进行解析验证。其中 Dt 表示 A 所访问的数据集合。SC1是维护 A 所在域的从链网络,且作为该域内访问可信认证平台,访问流程中的各记录会存储在SC1上,供历史溯源。此外,域内细粒度的访问控制策略依靠SC1上的智能合约实现。

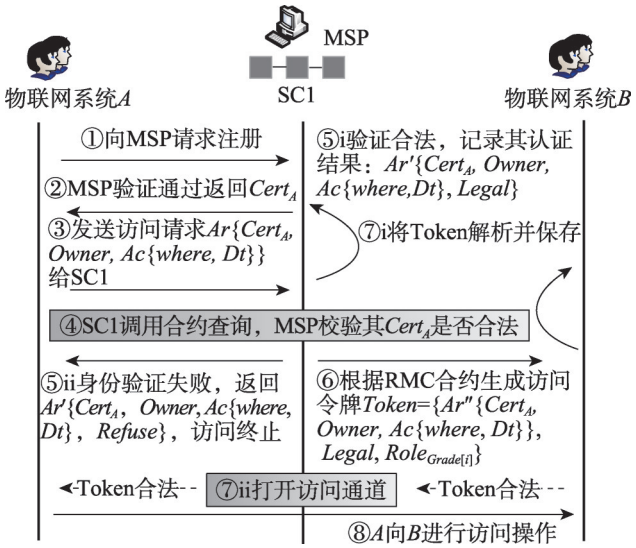


图5 域内访问流程

Fig.5 Intra-domain access process

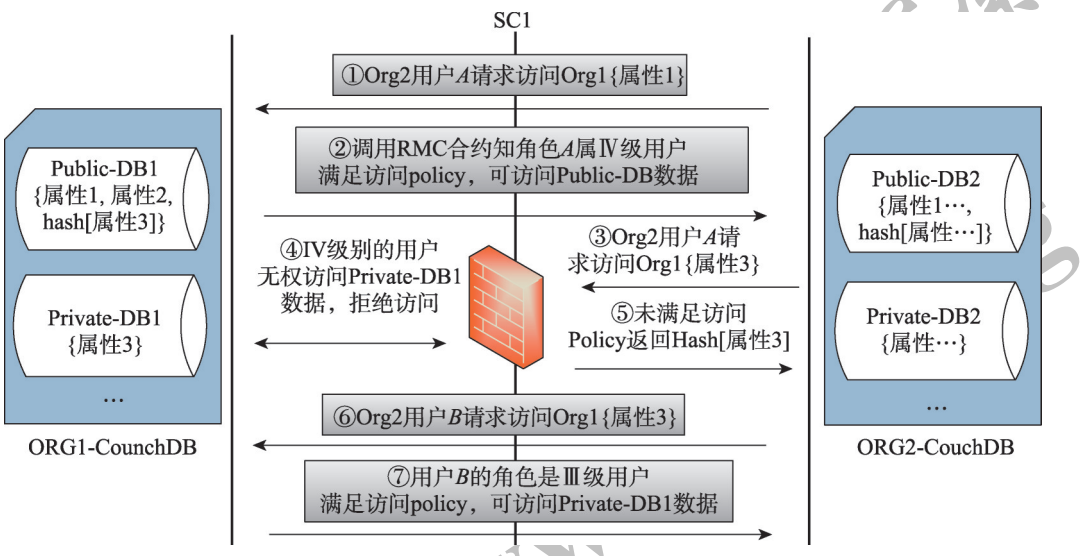


图4 隐私数据访问管理流程

Fig.4 Privacy data access management process

$$A \rightarrow SC1:\left\{pk_{UA}, Sig_{sk_{UA}}\left(Ar\begin{pmatrix}Cert_A, Owner,\\ Ac(where, Dt)\end{pmatrix}\right), T_1\right\}$$

（3）SC1将收到的Ar进行解析，确认当前行为是域内访问，随后通过MSP进行身份认证。

① $Cert_A$有效认证合法，则记录其认证结果，并修改A在SC1账本中的状态信息。

$$SC1 \leftarrow \left\{Sig_{PK_{SC1}}\left(Ar'\begin{pmatrix}Cert_A, Owner,\\ Ac(where, Dt)\end{pmatrix}, Legal\right), T_2\right\}$$

②$Cert_A$无效验证失败，则向A返回拒绝信息，表明A是不合法用户，或是不属于本域用户，访问终止。

$$SC1 \rightarrow A:\left\{Sig_{PK_{SC1}}\left(Ar'\begin{pmatrix}Cert_A, Owner,\\ Ac(where, Dt)\end{pmatrix}, Refuse\right), T_2\right\}$$

（4）通过身份验证后，SC1调用RMC合约并根据Dt为A自动匹配角色，随后根据角色权限生成访问令牌$Token$，发送给A所访问的IoT1-B，$Deadline$是访问令牌的有效期。若访问无法在令牌$Deadline$期内完成，出于安全性考虑，用户需重新进行身份验证以生成新的Token′。

$$SC1 \rightarrow B:Token\left\{\begin{Bmatrix}Sig_{PK_{SC1}}\left(Ar''\begin{pmatrix}Cert_A, Owner,\\ Ac(where, Dt)\end{pmatrix}, \\ Legal, Role_{Grade[i]}\end{Bmatrix}, \\ T_3, Deadline\end{Bmatrix}\right\}$$

（5）IoT1-B将$Token$解析后保存，并打开访问通道。

3.3.3 域间访问

域间访问是指发生在不同边缘物联网域下的访问行为，如图6所示，IoT1-C与IoT2-D之间的访问操作，其中SC2做出访问应答，MC起调度作用。

（1）IoT1-C向MSP发送一个状态为身份注册的请求，MSP验证通过后向其返回身份证书$Cert_C$，$Time$表示$Cert_C$的有效时间。

$$A \rightarrow MSP:\left\{pk_{UC}, Status, Sig_{sk_{IOT1}}\begin{pmatrix}sk_{UC},\\ Hash_C(pk_{UC})\end{pmatrix}\right\}$$

$$MSP \rightarrow A:Cert_C\left\{sig_{MSPpk}(States:Ture, Time)\right\}$$

（2）IoT-C拿到$Cert_C$后向MC发出跨域身份验证请求，并提交访问请求内容。

$$C \rightarrow MC:\left\{pk_{UCi}, Sig_{sk_{UC}}\left(Ar\begin{pmatrix}Cert_C, Owner,\\ Ac(where, Dt)\end{pmatrix}\right), T_1\right\}$$

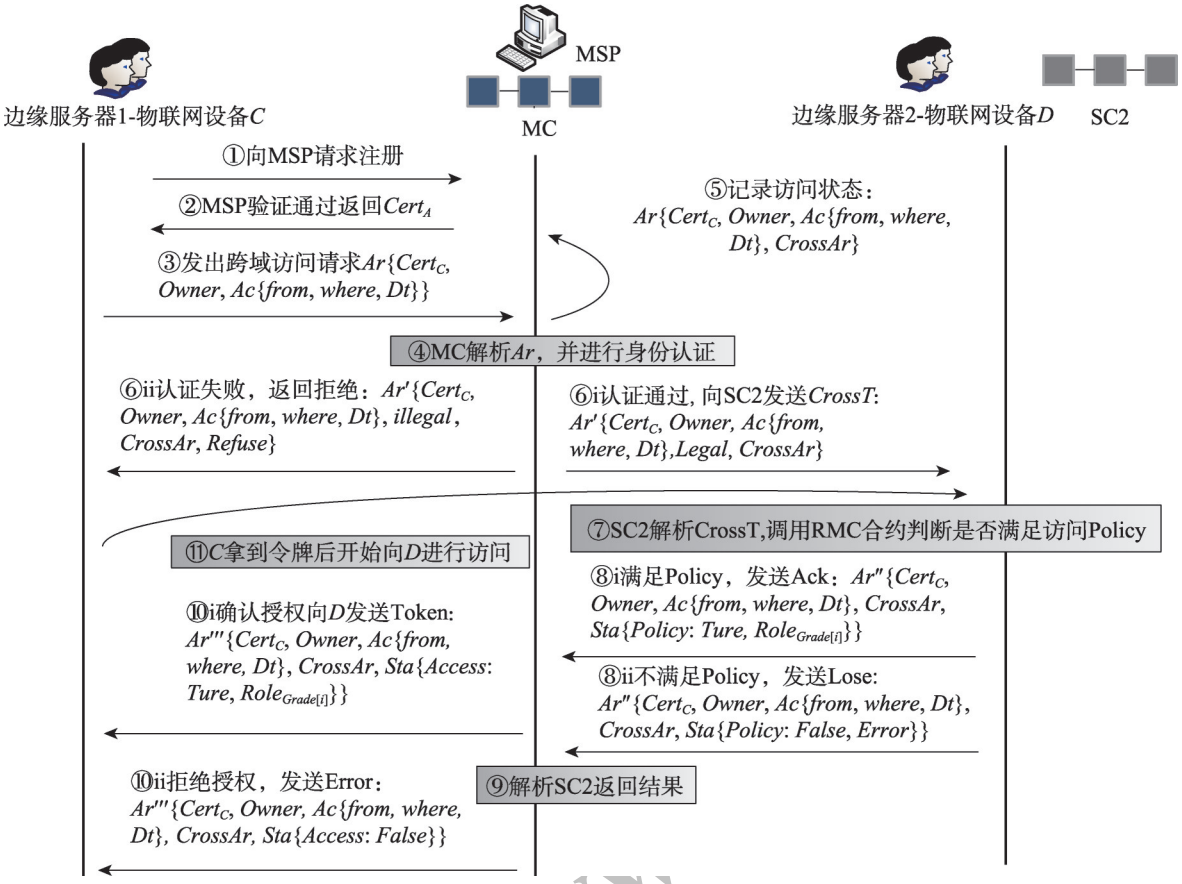


图6 域间访问控制流程

Fig.6 Inter-domain access control process

(3)主链MC将收到的 Ar 进行解析,并将此访问状态标记为跨域。随后对访问用户进行身份认证。

$$MC \leftarrow \left\{ Sig_{sk_{MC}} \left(Ar \left(\begin{matrix} Cert_C, Owner, \\ Ac \begin{pmatrix} from, \\ where, Dt \end{pmatrix}, CrossAr \end{matrix} \right) \right), T_2 \right\}$$

① $Cert_C$ 合法验证通过,将验证结果 $CrossT$ 发送给SC2。

$$MC \rightarrow SC2{:}CrossT \left\{ Sig_{sk_{MC}} \left(\begin{matrix} Ar' \begin{pmatrix} Cert_C, Owner, \\ Ac \begin{pmatrix} from, \\ where, Dt \end{pmatrix} \end{pmatrix}, \\ Legal, CrossAr \end{matrix} \right), T_3 \right\}$$

② $Cert_C$ 不合法,验证未通过,该用户无权访问,返回拒绝信息,跨域访问进程结束。

$$MC \rightarrow C{:} \left\{ Sig_{sk_{MC}} \left(\begin{matrix} Ar' \begin{pmatrix} Cert_C, Owner, \\ Ac(from, where, Dt) \end{pmatrix}, \\ illegal, CrossAr, Refuse \end{matrix} \right), T_3 \right\}$$

(4)SC2将 $CrossT$ 进行解析,并调用RMC合约查询 C 的角色,判断 C 当前角色是否满足 $Policy$ 。

①满足 $Policy$,则向MC发送确认信息。

$$SC2 \rightarrow MC{:}Ack \left\{ \begin{matrix} Sig_{sk_{SC2}} \left(\begin{matrix} Ar'' \begin{pmatrix} Cert_C, Owner, \\ Ac(from, where, Dt) \end{pmatrix}, \\ CrossAr, Sta \begin{pmatrix} Policy{:}Ture, \\ Role_{Grade[i]} \end{pmatrix} \end{matrix} \right), \\ T_4, Deadline \end{matrix} \right\}$$

②不满足 $Policy$,返回错误信息。

$$SC2 \rightarrow MC{:}Lose \left\{ Sig_{sk_{SC2}} \left(\begin{matrix} Ar'' \begin{pmatrix} Cert_C, Owner, \\ Ac(from, where, Dt) \end{pmatrix}, \\ CrossAr, \\ Sta(Policy{:}False, Error) \end{matrix} \right), T_4 \right\}$$

(5)MC解析SC2返回的授权信息。

①解析结果为确认授权,调用CrossD、CacheC合约获取并缓存数据。打开 C 对 D 的访问通道,并向IoT-C发送访问令牌。

$$MC \rightarrow C{:}Token \left\{ \begin{matrix} Sig_{PK_{MC}} \left(\begin{matrix} Ar''' \begin{pmatrix} Cert_C, Owner, \\ Ac(Where, Dt) \end{pmatrix}, \\ CrossAr, \\ Sta \begin{pmatrix} Access{:}Ture, \\ Role_{Grade[i]} \end{pmatrix} \end{matrix} \right), \\ T_5, Deadline \end{matrix} \right\}$$

②解析结果拒绝授权,则 MC 向 C 发送错误信息,表明该数据集合不对该用户开放。

$$MC \rightarrow C{:}Error \left\{ Sig_{PK_{MC}} \left(\begin{matrix} Ar''' \begin{pmatrix} Cert_C, Owner, \\ Ac(where, Dt) \end{pmatrix}, \\ CrossAr, \\ Sta(Access{:}False) \end{matrix} \right) T_5 \right\}$$

如该数据属于PDS集合的数据,对已通过身份认证但未满足所访问域中PDS集合访问策略中的用户,其权限未授权被“激活”,该类用户均无权对其访问,故 C 无法访问当前所申请访问的内容。若继续向该域继续访问,可重新选择所要访问的集合,返回(2)修改 Ac 中的访问内容信息,选择其他的访问集合,重新打包 Ar 以发起新一轮的访问流程。

$$Ac \rightarrow Ac'{:}\{Ac(where, Dt'), T_5'\}$$

(6) C 拿到令牌后开始向 D 进行访问。

3.4 安全性分析

3.4.1 不可伪造性证明

攻击者需获取合法节点的 SK 才能伪造合法节点,而基于密码学的ECC是以求解椭圆曲线离散对数问题(elliptic curve discrete logarithm problem,ECDLP)的困难性为安全基础的公钥密码系统。在已知 PK 和 Q ,逆向寻找 SK 过程的困难就是ECDLP。本文通过穷举搜索法试图求解ECDLP,验证逆向寻找 SK 几乎不可能成功。

定理1 已知 $Q=q$ 和 $P=PK$,P 的阶为 N。 $E \in (Fp)$,当 L 满足 $Q=LP$ 时求得 SK,其中 L 满足 $(0 \leqslant L \leqslant N-1)$ 。如果ECDLP成立,则该方法不可行。

证明 计算 $E \in (Fp)$ 的点序列 $P, 2P, 3P, \cdots, nP$,直到 $nP=Q$,则 $n=L$ 。考虑最坏情况下,需要计算 N 步才能找到满足 $nP=Q$ 的答案,平均需要 $N/2$ 步才能解决ECDLP。因此,该计算的时间复杂度是指数级的 $O(N)$ 。而当 N 足够大时,该求解方法在计算时间上变得不可行,该方法的有效性无法保证,ECDLP难度成立。此时式(3)中的 $SK(PK,P)$ 无穷小,那么攻击者 A 成功伪造合法节点的成功概率 $SuccA$ 几乎为0。

$$SuccA = \frac{ECDLP\{SK(PK,Q)\}}{A\{PK,Q,Enc(SK,Hash)\}} \tag{3}$$

可证得在本文方案下,边缘节点是不可能被成功伪造和篡改的,满足不可伪造性。

3.4.2 正确性测试

在ID-RBAC模型下并发事务107 936次,成功执行107 934次,未成功执行2次,成功率达到了99.99%,而0.01%的失败率是可忽略的。

在ID-RBAC模型中,身份认证信息的上传、访问、失效都以带有时间戳的链结构进行记录,其访问记录可被追溯但不可篡改。即使攻击者截获相应的身份认证信息,也无法重放此消息躲避身份验证机制。因此,在访问响应测试中,基于ID-RBAC模型模拟恶意节点发生访问行为,验证该模型身份认证与

数据访问策略的正确性。表3预设了四种场景，包括物联网应用下主要可能出现的访问攻击类型。测试结果表明ID-RBAC模型具有正确性，可正确实现对用户的身份认证并进行有效的访问控制。

表3 响应测试说明

Table 3 Response test description

访问场景	预设结果	实验组数	验证通过组数	验证失败组数
有权或合法用户对消息进行签名，并发起验证请求	$Cert_i' = Cert_i$ 验证通过	100	100	0
无权或恶意节点对消息进行签名，并发起验证请求	$Cert_i' \neq Cert_i$ 验证不通过	100	0	100
不符合访问Policy的用户对数据进行访问	$Cert_i' = Cert_i$ 但不满足Policy无法获取明文	100	0	100
合法且满足数据访问Policy的用户对数据进行访问	$Cert_i' = Cert_i$ 且满足Policy可获取明文数据	100	100	0

4 实验验证与分析

本章围绕吞吐量、时延和资源消耗三个性能指标展开实验验证与分析，且通过改变边缘节点数进行分组测试。为了评估模型扩展性及优越性，围绕上述三个性能指标与文献[13]、文献[24]进行对比。

4.1 实验设置

基于Hyper Ledger Fabric开源框架和Docker容器技术搭建了区块链开发平台，并以此作为测试与评估平台。在实验中，本文设定网络中的所有合法节点都为背书(endorser)节点和提交(committing)节点，锚(anchor)节点在域初始化时指定，主(leafer)节点在域初始化时选举，且通过高鲁棒拜占庭容错算法(robust Byzantine tolerance，RBFT)达成一致。智能合约使用Go语言编写。在Ubuntu 20.04 OS上运行边缘计算平台，该平台由3个边缘设备Edge1、Edge2和Edge3组成。同时这些边缘设备作为区块链网络的“矿工”，为其提供存储能力与计算能力。表4为实验详细设置。

表4 实验设置

Table 4 Experimental setup

软/硬件	资源使用
CPU	Intel® Core™ i7-10700，2.90 GHz
开发平台	Hyperledger Fabric 2.0.0，Docker 20.10.7
边缘设备	OS，Ubuntu20.4 Desktop；内存，4 GB；内核，4 GB
编程语言	Go语言

4.2 吞吐量

吞吐量(throughput)是衡量并发处理能力的重要指标。根据不同边缘节点数进行了3组实验，测量周期内域内与域间发生的所有事务流量：事务提交量(successfully committed transactions，Succ)和吞吐量，结果如图7所示。从实验可观察到吞吐量、事务量总体上随边缘节点 *En* 的数量增加呈现稳定增长趋势。当 *En* 的数量不超过2时，吞吐量增长到350 TPS左右后便处于滞停状态，是因为随并发事务的增加系统处理能力出现不足，导致此时的吞吐量不再增加甚至出现下降情况。而 *En* 数为3时，*En* 富余的算力提升了系统的计算能力，起到了负载均衡的作用。由3个 *En* 的线性拟合预测线知，吞吐量随事务量的增加是呈线性增长的。在负载条件、交易时间一致的情况下，1个 *En* 提交的最大事务数是63 588，吞吐量是354.5 TPS，而3个 *En* 时的最大事务数为104 648，此时吞吐量达到583.4 TPS，事务数及吞吐量约是1个 *En* 的1.7倍。可见集成边缘计算的区块链网络可极大提升其性能。特别地，在多并发访问的场景中，可通过增加 *En* 数来保证跨域认证效率与吞吐量。

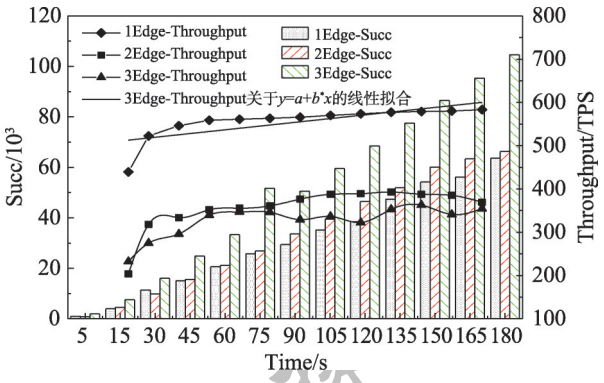


图7 吞吐量与Succ随时间的变化关系

Fig.7 Throughput versus Succ over time

4.3 时延

通过已发布事务的完成时间，加上各节点对事务达成共识的时间来计算时延。在180 s内持续发起事务，得到不同Edge数下域内和域间执行事务的最大时延(max latency)。以域内、域间的最大时延总和计算出其平均值，结果如图8所示。结果显示，不同 *En* 数下的时延差距较大，*En* 数为3时的时延最低且保持稳定。1个 *En* 时，处理事务过程中的最大时延为2.19 s，平均时延为0.69 s。而 *En* 数为3时的最大时延和平均时延分别是0.10 s、0.05 s，相比 *En* 数为1时，最大时延降低了95.43%，平均时延降低了92.75%。

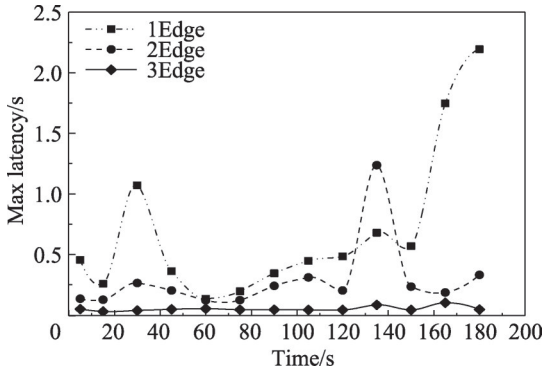


图8 不同Edge数的最大时延情况

Fig.8 Maximum latency for different number of edge

可见集成边缘计算的区块链网络继承了边缘计算实时性的优点，可根据网络规模扩展边缘节点数以满足实际应用的实时性需求。

4.4 资源开销

在交易时间txDuration为180 s时，修改测试并发交易数txNumber分别为1 000、2 000、5 000，测试工作节点Node1在主从链、单链环境下的CPU占用情况与内存使用情况，如表5所示。可观察到主从链工作过程中Node1的CPU占有率较低，内存使用较小，整体上其资源开销较单链环境降低了50%左右。可见主从链环境下的资源复用情况良好，CPU利用率较高。原因是主链节点Node0分担了工作节点Node1的部分资源压力，提高了事务处理的效率，释放了一定的系统资源。因此，同一时间下，Node1的CPU占比较低。

表5 单链与主从链存储开销对比

Table 5 Single chain versus master-slave chain storage overhead

组数	环境	CPU占比/%	Memory/MB
①	单链	32.59	176.00
	主从链	14.05	86.88
②	单链	50.46	177.50
	主从链	19.17	87.39
③	单链	81.88	228.60
	主从链	44.10	115.32

工作节点在不同边缘节点数下的CPU占用、内存使用情况如图9所示。3个*En*下CPU利用率稳定在27%左右，需要的平均内存为55 MB，相比1个*En*时有大幅度的降低。即使同一时间内3个*En*处理的事务是1个*En*的两倍，但其CPU占用、内存使用情况是1个*En*的50%。其原因是3个边缘节点较1个边缘节点可提供更多的系统资源，且分担了更多的存储压力，有效地均衡工作节点的负载。此外，同一时间下，多节点环境会释放更多的系统资源，提升了系统资源复用率。因此，基于多边缘节点部署的主从链环境可实现较高的资源利用率，总体可扩展性更强。

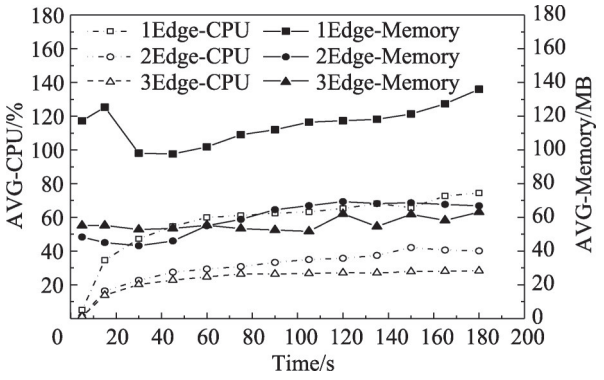


图9 不同Edge数下的CPU及内存占用情况

Fig.9 CPU and memory usage under different number of edge

4.5 对比分析

Jiang等人[13]基于公证机制提出了交互式的跨域框架以管理数据。针对隐私保护问题提出了一种数据访问控制模型，并设计了一种特定的事务类型，以提供对不同链和节点的数据的细粒度访问控制。该方案的隐私访问控制方案只能保证物联网数据的隐私保护，未考虑到交易中涉及的用户信息的隐私保护，且适用于资源较少的物联网应用场景。本文方案将模型部署在大规模的物联网场景下，且考虑交易过程中的隐私保护，将其进行比较，在应用扩展及隐私保护上有重要意义。Zhang等人[24]为了解决底层密码学基础导致的“不完全跨域”问题，提出了一种“彻底”的跨域认证方案，以供来自不同域、不同设置的参与域使用。其有效解决了跨域通信中的实体认证问题，且给出了域内、域间认证流程。与其对比时延、TPS等性能指标，在相同仿真环境下，本文方案虽增加了隐私数据集合、ECC等复杂的认证流程，但其性能指标未有明显下降。它们代表了区块链在数据隐私保护、可信跨域研究的两个重要方向，本文与之进行比较，有较强的可参考性。

4.5.1 与其他方案的吞吐量对比

文献[13]测试了不同内存条件时的跨链吞吐量。在4 GB内存、4 GHz内核及交易数txNumber为6 000时，对跨域访问行为进行仿真，与本文TPS对比结果如图10所示。当其发送速率（sending rate）到达

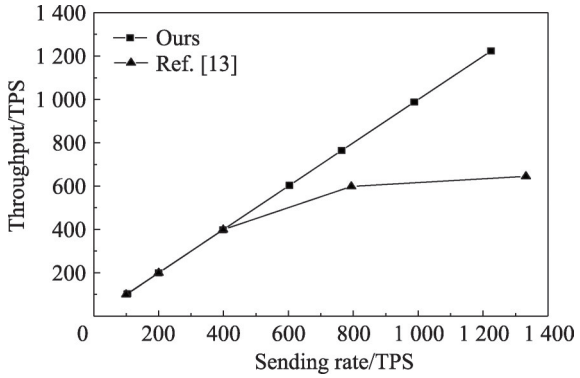
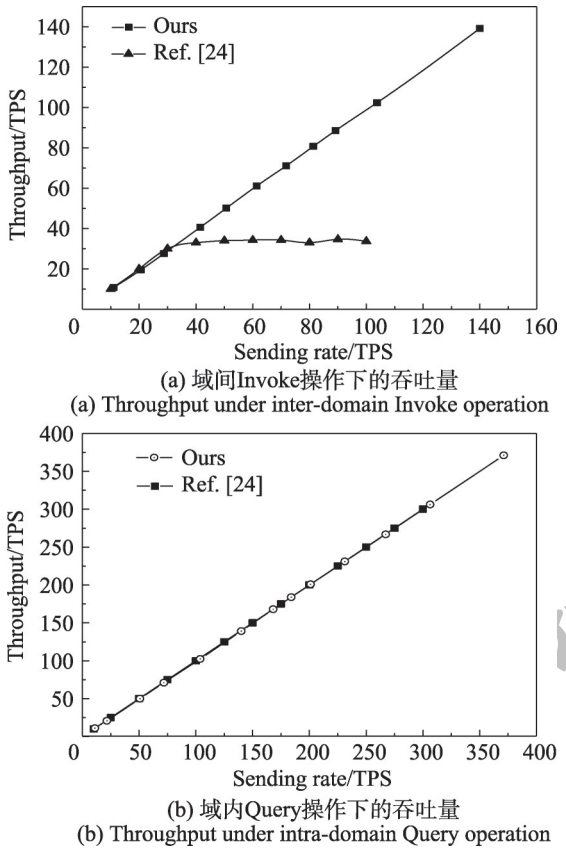


图10　本文方案与文献[13]的吞吐量对比

Fig.10　Throughput comparison of our scheme and ref. [13]

500 TPS左右后，吞吐量开始跟不上发送速率。而发送速率为1 332 TPS时，吞吐量只有645 TPS，发送速率与吞吐量的比值约为2∶1。而本文方案中吞吐量随发送速率的增加呈线性增长，且在测试范围内发送速率与吞吐量的比值始终为1∶1。较文献[13]而言，可获得更高的吞吐量。

在6个peer下进行跨域查询Invoke和域内查询Query操作，与文献[24]进行比较，结果如图11所示。在域间Invoke操作时，文献[24]发送速率不超过30 TPS，吞吐量呈线性增加，发送速率继续增加超过30 TPS后，吞吐量开始表现出瓶颈，到达最大值34 TPS左右后趋于稳定。此时，系统性能已不足以处理更多的事务。当发送速率为100 TPS时，与吞吐量的比值为3∶1。其域内Query操作吞吐量与发送速率的比值是1∶1，呈线性关系。对比本文方案，Invoke、Query操作的吞吐量始终随发送速率增加呈线性增长，发送速率与吞吐量均接近1∶1。对比文献[24]，本文方案在跨域工作上处理事务的效率更高，整体性能更占优势。



(a) 域间Invoke操作下的吞吐量

(a) Throughput under inter-domain Invoke operation

(b) 域内Query操作下的吞吐量

(b) Throughput under intra-domain Query operation

图11　本文方案与文献[24]的吞吐量对比

Fig.11　Throughput comparison of our scheme and ref. [24]

本文在Jiang等人[13]、Zhang等人[24]方案的基础上实现了高效交互式的跨域访问控制。且较两者有更稳定的发送速率与吞吐量，结果符合预期目标。

4.5.2　与其他方案的时延对比

一定发送速率下各方案的时延情况如表6所示。可观察到不管域内或是域间，本文方案下的时延均是三者中最小。即使是在通信复杂的跨域场景，本文获得毫秒级别的时延，相对文献[13]、文献[24]的方案，有较明显的优势，更适用于对时延敏感的物联网应用。

表6　一定发送率下的各方案时延对比

Table 6　Comparison of delay of each scheme at certain transmission rate

测试	发送速率/TPS	平均时延/s
文献[13]跨域	794.0	3.75
本文跨域	828.0	0.05
文献[24]域内	300.0	0.05
本文域内	300.1	0
文献[24]域间	100.0	10.90
本文域间	103.8	0.02

4.5.3　与其他方案的资源开销对比

在4 GB内存和4 GHz内核配置下，评估各方案的资源开销情况。在交易测试时间txDuration为180 s、并发交易数txNumber为6 000时，对各方案进行仿真得到工作节点CPU平均占用值与内存平均使用值，如表7所示。从资源复用情况来看，Jiang等人[13]、

表7　资源开销情况对比

Table 7　Comparison of resource overhead

测试	CPU占比/%	内存/MB
文献[13]域内	50.90	203.90
文献[13]域间	61.00	264.30
文献[24]域内	45.88	176.00
文献[24]域间	69.90	234.00
本文域内	29.00	76.68
本文域间	44.10	136.00

Zhang等人[24]方案不宜在资源有限的物联网设备中部署,而本文基于主从链结构部署的方案,在并发交易量较大时,其CPU占比及内存使用情况良好,可在大型物联网应用场景中部署。

5 结束语

区块链作为安全技术代表有望打开制约边缘计算发展的束缚,但因计算效率低、共识能耗高等扩展性瓶颈,使得其不能在解决边缘计算安全问题时发挥最大作用。因此本文设计了主从多链结构,并集成边缘计算构建了分布式安全的可信认证模型,即域间访问控制模型(ID-RBAC),有效解决了数据孤岛的问题。同时细粒度的访问控制方法避免了越权访问数据、过度授权等情况。最后通过实验对模型的安全性、稳定性做出了评估,并证明了边缘计算与区块链的结合有互补性。即边缘计算为区块链提供存储、计算能力,区块链为边缘计算提供安全的审计功能。相比现有方法,本文方案具有更好的扩展性,性能更优,符合现下环境的服务需求。

对于未来工作,考虑扩大实验规模并优化区块链的共识算法,为区块链网络创造一个较现有方案更高性能、更低延时及更高带宽的电信级服务环境。同时为进一步提高访问控制效率,可以尝试与隐私计算等技术结合起来,优化跨域访问控制模型。

参考文献:

[1] 施巍松, 孙辉, 曹杰, 等. 边缘计算: 万物互联时代新型计算模型[J]. 计算机研究与发展, 2017, 54(5): 907-924.
SHI W S, SUN H, CAO J, et al. Edge computing—an emerging computing model for the Internet of everything era[J]. Journal of Computer Research and Development, 2017, 54(5): 907-924.

[2] YU Y. Mobile edge computing towards 5G: vision, recent progress, and open challenges[J]. China Communications, 2016, 13(S2): 89-99.

[3] HERBADJI A, GOUMIDI H, HARBI Y, et al. Blockchain for Internet of vehicles security[M]//Blockchain for Cybersecurity and Privacy. Boca Raton: CRC Press, 2020: 159-197.

[4] 喻辉, 张宗洋, 刘建伟. 比特币区块链扩容技术研究[J]. 计算机研究与发展, 2017, 54(10): 2390-2403.
YU H, ZHANG Z Y, LIU J W. Research on scaling technology of bitcoin blockchain[J]. Journal of Computer Research and Development, 2017, 54(10): 2390-2403.

[5] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//Proceedings of the 2017 IEEE International Congress on Big Data, Honolulu, Jun 25-30, 2017. Washington: IEEE Computer Society, 2017: 557-564.

[6] 王慧, 王励成, 柏雪, 等. 区块链隐私保护和扩容关键技术研究[J]. 西安电子科技大学学报(自然科学版), 2020, 47(5): 28-39.
WANG H, WANG L C, BAI X, et al. Research on key technology of blockchain privacy protection and scalability[J]. Journal of Xidian University (Natural Science), 2020, 47(5): 28-39.

[7] 谢英英, 石洞, 黄硕康, 等. 面向5G的命名数据网络物联网研究综述[J]. 计算机科学, 2020, 47(4): 217-225.
XIE Y Y, SHI J, HUANG S K, et al. Survey on Internet of things based on named data networking facing 5G[J]. Computer Science, 2020, 47(4): 217-225.

[8] LOU J, ZHANG Q, QI Z, et al. A blockchain-based key management scheme for named data networking[C]//Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking, Shenzhen, Aug 15-17, 2018. Piscataway: IEEE, 2018: 141-146.

[9] MA Z F, WANG X C, JAIN D K, et al. A blockchain-based trusted data management scheme in edge computing [J]. IEEE Transactions on Industrial Informatics, 2019, 16(3): 2013-2021.

[10] PAN J, WANG J, HESTER A, et al. EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts[J]. IEEE Internet of Things Journal, 2018, 6(3): 4719-4732.

[11] 程冠杰, 黄诤杰, 邓水光. 基于区块链与边缘计算的物联网数据管理[J]. 物联网学报, 2020, 4(2): 1-9.
CHENG G J, HUANG Z J, DENG S G. Data management based on blockchain and edge computing for Internet of things[J]. Chinese Journal on Internet of Things, 2020, 4(2): 1-9.

[12] 曹雪莲, 张建辉, 刘波. 区块链安全、隐私与性能问题研究综述[J]. 计算机集成制造系统, 2021, 27(7): 2078-2094.
CAO X L, ZHANG J H, LIU B. Review on security, privacy, and performance issues of blockchain[J]. Computer Integrated Manufacturing Systems, 2021, 27(7): 2078-2094.

[13] JIANG Y M, WANG C X, WANG Y W. A cross-chain solution to integrating multiple blockchains for IoT data management[J]. Sensors, 2019, 19(9): 2042-2053.

[14] PYOUNG C K, BAEK S J. Blockchain of finite-lifetime blocks with applications to edge-based IoT[J]. IEEE Internet of Things Journal, 2019, 7(3): 2102-2116.

[15] CUI Z, XUE F, ZHANG S, et al. A hybrid blockchain-based identity authentication scheme for multi-WSN[J]. IEEE Tran-

sactions on Services Computing, 2020, 13(2): 241-251.
[16] 毕娅, 张曙红, 冷凯君, 等. 基于双链区块链的制造服务集成平台框架[J]. 计算机集成制造系统, 2022, 28(4): 1177-1187.
BI Y, ZHANG S H, LENG K J, et al. Framework of manufacturing service integration platform based on double-chain blockchain[J]. Computational Integrated Manufacturing Systems, 2022, 28(4): 1177-1187.
[17] ZHOU H, XU W, CHEN J, et al. Evolutionary V2X technologies toward the Internet of vehicles: challenges and opportunities[J]. Proceedings of the IEEE, 2020, 108(2): 308-323.
[18] LI G, REN X, WU J, et al. Blockchain-based mobile edge computing system[J]. Information Sciences, 2021, 561: 70-80.
[19] CHUANG I H, HUANG S H, CHAO W C, et al. TIDES: a trust-aware IoT data economic system with blockchain-enabled multi-access edge computing[J]. IEEE Access, 2020, 8: 85839-85855.
[20] 张明德. PKI/CA 与数字证书技术大全[M]. 北京: 电子工业出版社, 2015.
ZHANG M D. The complete guide to PKI/CA and digital certificate technology[M]. Beijing: Electronic Industry Press, 2015.
[21] ISLAM S H, BISWAS G P. A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication[J]. Journal of King Saud University-Computer and Information Sciences, 2017, 29(1): 63-73.
[22] 陈彦冰, 钟超然, 周超然, 等. 基于医疗联盟链的跨域认证方案设计[J]. 计算机科学, 2022, 49(S1): 537-543.
CHEN Y B, ZHONG C R, ZHOU C R, et al. Design of cross-domain authentication scheme based on medical consortium chain[J]. Computer Science, 2022, 49(S1): 537-543.
[23] 赵平, 王赜, 李芳, 等. 主从区块链容错异构跨域身份认证方案[J]. 计算机工程与应用, 2022, 58(22): 79-88.
ZHAO P, WANG Z, LI F, et al. Master-slave blockchain fault-tolerant heterogeneous cross-domain identity authentication scheme[J]. Computer Engineering and Applications, 2022, 58(22): 79-88.
[24] ZHANG H, CHEN X, LAN X, et al. BTCAS: a blockchain-based thoroughly cross-domain authentication scheme[J]. Journal of Information Security and Applications, 2020, 55: 102538.
[25] GUO S, WANG F, ZHANG N, et al. Master-slave chain based trusted cross-domain authentication mechanism in IoT[J]. Journal of Network and Computer Applications, 2020, 172: 102812.
[26] 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.
SHI J S, LI R. Survey of blockchain access control in Internet of things[J]. Journal of Software, 2019, 30(6): 1632-1648.
[27] 余波, 台宪青, 马治杰. 云计算环境下基于属性和信任的RBAC模型研究[J]. 计算机工程与应用, 2020, 56(9): 84-92.
YU B, TAI X Q, MA Z J. Study on attribute and trust-based RBAC model in cloud computing[J]. Computer Engineering and Applications, 2020, 56(9): 84-92.
[28] XUAN S, ZHENG L, CHUNG I, et al. An incentive mechanism for data sharing based on blockchain with smart contracts[J]. Computers & Electrical Engineering, 2020, 83: 106587.

黄敏敏(1997—),女,广西贵港人,硕士研究生,主要研究方向为区块链、边缘计算、访问控制。
HUANG Minmin, born in 1997, M.S. candidate. Her research interests include blockchain, edge computing and access control.

袁凌云(1980—),女,云南昭通人,博士,教授,博士生导师,CCF高级会员,主要研究方向为物联网安全、区块链、传感器网络。
YUAN Lingyun, born in 1980, Ph.D., professor, Ph.D. supervisor, senior member of CCF. Her research interests include IoT security, blockchain and sensor network.

潘雪(1996—),女,云南昆明人,硕士研究生,主要研究方向为物联网安全、区块链、访问控制。
PAN Xue, born in 1996, M.S. candidate. Her research interests include IoT security, blockchain and access control.

张杰(1997—),男,安徽芜湖人,硕士研究生,CCF学生会员,主要研究方向为物联网安全、区块链、边缘计算。
ZHANG Jie, born in 1997, M.S. candidate, student member of CCF. His research interests include IoT security, blockchain and edge computing.