计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210300235

基于区块链的工业控制系统角色委派访问控制机制

郭 显 王雨悦 冯 涛 曹来成 蒋泳波 张 迪
兰州理工大学计算机与通信学院 兰州 730050

摘 要 IT和OT的融合模糊了工业控制系统“网络边界”的概念,细粒度的访问控制策略是保障工业企业网络安全的基石。基于角色委派的访问控制机制可把域中用户对网络资源的访问权限委派给其他域的用户或企业合作伙伴,这样为企业员工或企业合作伙伴远程访问企业网络资源提供了便利。然而,这种便利可能增加工业控制系统的攻击面。区块链技术固有的去中心化、防篡改、可审计等特征可以成为基于角色委派访问控制管理的基础架构,因而提出了基于区块链技术的角色委派访问控制方案(Delegatable Role-Based Access Control,DRBAC)。DRBAC包括用户角色管理及委派、访问控制、监控机制等几个重要组件,并基于智能合约实现该方案,DRBAC的目的是保证每个网络连接必须受到细粒度访问控制策略的保护。最后,通过搭建本地私有区块链网络测试分析了DRBAC的正确性、可行性和开销。

关键词:工业控制系统;区块链;智能合约;角色委派;访问控制
中图法分类号 TP393

Blockchain-based Role-Delegation Access Control for Industrial Control System

GUO Xian,WANG Yu-yue,FENG Tao,CAO Lai-cheng,JIANG Yong-bo and ZHANG Di
School of Computer and Communication,Lanzhou University of Technology,Lanzhou 730050,China

Abstract The concept of “network perimeter” in industrial control system is becoming vague due to the integration of IT and OT technology. The fine-grained access control strategy that intends to protect each network connection can ensure the network security of industrial control system. The role-delegation-based access control scheme can delegate an access right of user in a domain to a user in another domain or a company partner so that these users can remotely access the network resources of the industrial enterprise. However,these benefits resulted from the delegation may increase the attack surface for industrial control system. The blockchain technology with decentralization,tamper-proof,auditable and other characteristics can be considered as a basic framework of the role-delegation access control for network resources in industrial control system. This paper proposes a role-delegation access control scheme DRBAC based on blockchain. DRBAC includes several important components:user role management and delegation,access control,monitoring mechanism,etc. The DRBAC solution is implemented based on smart contract. The DRBAC ensures that each network connection must be protected by fine-grained access control strategies. Finally,the correctness,feasibility and overhead of DRBAC are tested and analyzed in a private blockchain network.

Keywords Industrial control system,Blockchain,Smart contract,Delegatable role,Access control

1 引言

工业控制系统(Industrial Control System,ICS)是包括公共事业、交通和制造业等在内的工业部门组织的基础,是关系国计民生的国家关键基础设施的一个组成部分,被广泛应用于电力、石化、市政设施、智能制造等行业。为了提高企业的生产效率和竞争力,与国家关键基础设施相关的工业企业正试图通过物联网、云计算、人工智能等新型技术推动数字化转型[1-5],“新基建”投资计划必将进一步提高我国ICS的数字化水平[6]。

但是,随着工业企业朝着数字化的不断转型,以及工业企业IT网络和OT网络的深度融合,增加了ICS的攻击面[7-9]。ICS频发的网络安全事件引起了各国的关注,Stuxnet,BlackEnergy,Crashoverride等工业企业网络安全事件表明:1)恶意内部员工仍是重要威胁;2)云、移动和虚拟化等技术模糊了网络“边界”的概念;3)复杂的工业控制系统供应链加剧了安全担忧,攻击者利用现场设备固件的漏洞,很容易破坏数据并将攻击传播到不同的控制系统;4)供应商远程设备维护和更新为攻击者提供了可乘之机。研究人员认为,缺乏安全和细粒度的访问控制机制是主要的影响因素,保护每个网络连接的

到稿日期:2021-03-23 返修日期:2021-06-24 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61461027);甘肃省自然科学基金(20JR5RA467)
This work was supported by the National Natural Science Foundation of China(61461027) and Natural Science Foundation of Gansu Province(20JR5RA467).
通信作者:郭显(iamxg@163.com)

细粒度访问控制策略是保障网络安全的基石[10-11]。

目前，传统的访问控制模型中，主要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)和基于能力的访问控制(Capability-Based Access Control，CapBAC)等，研究者基于这些模型提出了可应用于不同场景的访问控制方案[12-16]。其中基于 RBAC 的模型是 NIST 800-82[17]和 ISA-99[18]推荐的工业控制系统访问控制的基本模型，文献[19]为 RBAC 提供了基本的框架，通常被称为 RBAC96 模型。然而，这些传统的访问控制机制都由中央实体进行权限管理，因此其存在单点故障问题，且方案缺乏可扩展性及安全性。

工业化和信息化的广泛融合，使 ICS 访问控制策略的制定变得复杂，企业内部不同域的用户可能需要访问其他域管理员管理的网络资源，如云上资源；企业子公司员工可能需要通过外部网络远程访问企业总公司的网络资源；为了检查和更新企业设备软件，企业合作伙伴远程访问企业网络设备也是保障网络正常运行的关键。如何将对某一网络资源的访问权限委派[20]给需要访问该资源但无权限的用户是访问控制策略要解决的重要问题。基于 RBAC96 模型，文献[21]提出了灵活的基于权限的委派模型——PBDM 模型，可以仅将用户的部分访问权限分配给其他用户，支持角色和权限级别的委派。

访问控制策略的制定和管理是访问控制机制的关键组件，错误的访问权限及策略配置可能会造成严重后果，域外用户的权限委派更增加了 ICS 网络资源受到攻击的风险。另外，访问策略执行点的拒绝服务攻击可能导致工业企业运营中断；具有有效证书的恶意员工仍可能访问已授予其账户访问权限的资源；检查、记录来自非企业拥有系统的网络流仍然较为困难；用于网络安全威胁分析的网络日志可能成为攻击者的重要攻击目标。

区块链[22]是由去中心化的计算机集群管理的一系列不可篡改的数据记录，区块链的这种去中心化特征能够解决传统集中式管理带来的单点故障等问题；区块链共识机制[23-24]使得区块链上只有有效交易记录，以确保记录信息的不可否认性，已发布的交易的完整日志都将保留在区块链中；通过使用基于区块链的智能合约应用，如以太坊智能合约[25]，能在复杂条件下监视和强制执行访问权限；可以采用基于区块链的技术保存用户个人信息、日志数据和企业敏感数据等数据信息。区块链技术固有的不可篡改性、安全性、可审核性和分布式等特征可以成为工业控制系统访问控制管理的基础架构。在基本访问控制模型中，以区块链为基础架构应用到不同领域中的访问控制策略是研究领域的热点[26-42]。

文献[43-53]中主要包括委派在 RBAC，ABAC，CapBAC 等经典访问控制模型中的应用。文献[54]结合密码学技术和区块链技术提出了适用于“工业 4.0”的安全相互认证和细粒度访问控制方案 BSeIn，使用智能合约实现了认证和访问控制的执行过程。受文献[43，51-54]的启发，本文设计了一种基于区块链的角色委派访问控制方案 DRBAC，在 DRBAC 中，根据 PERA 企业参考模型[55]把工业企业网络分为不同的域，DRBAC 通过角色委派，不仅允许企业网络域中的用户访问其他域的资源，而且允许企业内合法用户和企业合作伙伴通过公共网络远程访问企业网络资源。DRBAC 的目标是使每个网络连接都受到访问控制策略的保护，并制定对网络连接的细粒度访问规则，以防止用户未经授权就访问企业资源和企业机密数据；DRBAC 访问管理机制结合监视和日志记录功能，能够以安全且可审核的方式存储和跟踪关键信息，制定自适应访问控制策略；基于以太坊智能合约实现了 DRBAC 角色委派访问控制方案。最后，本文通过在本地搭建私有区块链网络，验证了本文方案的正确性、可行性和效率。

本文第 2 节介绍了相关工作；第 3 节为研究基础，包括基于区块链的用户管理和访问控制通用模型、角色访问控制方案和角色委派访问控制方案介绍；第 4 节介绍了本文所采用的简化网络模型；第 5 节介绍了本文提出的基于区块链的角色委派访问控制方案 DRBAC；第 6 节介绍了基于智能合约的 DRBAC 方案的实现过程；第 7 节介绍了在搭建的私有区块链平台上验证测试 DRBAC 方案的方法，分析了方案的正确性、可行性和效率；最后总结本文并展望未来。

2　相关工作

为了解决 ICS 的访问控制问题，研究者已经进行了大量的研究，针对 Modbus 协议的安全问题，文献[15]采用 RBAC 对基于 Modbus 的系统进行授权和认证。针对工控系统的实时性，文献[16]提出了一种基于 DTE 的工业控制系统访问控制模型，该模型定义并应用了与工业控制系统计时需求相关的强制访问控制方案，根据系统需求控制系统中的控制流，并提高了访问控制的灵活性。

基于区块链的访问控制策略成为了近年来的研究热点，文献[37]提出了基于智能合约的访问控制列表方案，该方案由多个智能合约对用户静态、动态的权限进行验证，并为系统中每对主体和对象分别提供了一种访问控制方法。文献[38]是一种适用于跨组织的 RBAC 策略，该机制由智能合约和挑战与应答协议两部分组成，智能合约为用户分配角色，挑战与应答协议用于用户的身份验证。文献[40]通过位置服务器在 RBAC 中引入用户位置感知，用户在进行访问请求时，还会定位其所处的位置，给访问控制提供了更加动态、细粒度的审查机制。ABAC 根据主体分配的属性和访问策略做出访问控制决策，由于主体所拥有的多重属性可能需要多个不同的权威机构来验证，文献[41]提出了一种基于区块链的多权限属性访问控制方案，权限用于验证主体的属性，智能合约用于定义数据所有者、用户和多个属性权限之间的交互。文献[42]采用智能合约实现 ABAC 策略，评估策略所需的属性由智能合约管理，并且区块链技术使得策略评估过程具有可审核性。

大量文献在访问控制机制中应用了委派授权机制，文献[45]提出了基于属性委派的访问控制模型 ABDAC，重点研究了委派授权策略和委派的撤销，并引入了可信度动态调节机制，对用户的可信度进行实时计算并反馈给 ABDAC 模型。文献[47]提出了一种适用于多域电子医疗的 ABAC 委派方案，并利用智能合约管理属性的分配、委派及撤销，与现有的

可委派访问控制方案相比，其具有更好的属性撤销机制。文献[48]通过智能合约支持云中心的委派授权，并允许用户审计授权操作以及检查实际执行访问控制的方式。文献[49]提出了一种基于区块链的访问控制框架 CapChain，它允许用户共享和委派对物联网设备的访问权限，并采用区块链技术保护隐私，隐藏包括用户身份和相关功能等敏感信息。

文献[50]提出了 FairAccess 框架，使用区块链作为访问控制管理器，并引入了一种不同于比特币交易的新的交易类型，用于授予、获取、委派和撤销访问权限。文献[51]提出 BlendCAC，采用基于能力的访问控制方案，利用智能合约对访问权限进行注册、传播和撤销。该方案还引入了能力的委派机制，策略决策中心通过将部分身份验证与授权委派给域管理员，减轻其工作负载，使得方案更轻量级和细粒度。文献[52]在文献[51]的基础上，通过引入基于能力的联合委派模型来支持分层、多跳的委派，并对委派、授权和撤销机制进行了更深入的探讨。文献[53]在相同的成本下，提出了在能力委派的灵活性、细粒度以及一致性方面都优于文献[51-52]的 CapBAC 方案，该方案以行为单元定义能力令牌，为每个对象创建一个智能合约，用于存储和管理访问主体的能力令牌。文献[54]结合密码学和区块链技术提出了适用于“工业 4.0”的安全相互认证和细粒度访问控制方案 BSeIn，使用智能合约实现认证和访问控制执行过程，然而 BSeIn 方案没有考虑委派问题。

3 研究基础

3.1 基于区块链的访问控制模型

文献[28]提出了基于区块链的用户身份和访问管理基本模型，该模型由 3 个主要模块组成(见图 1)：身份管理、访问控制、监控与存储。图 1 中，绿色表示身份管理过程，蓝色表示访问控制过程，红色表示监控过程，而黑色表示与身份和访问控制过程相关的信息存储，这里的信息存储可能采用链上和链下两种存储方式，本文不考虑设备数据的存储。

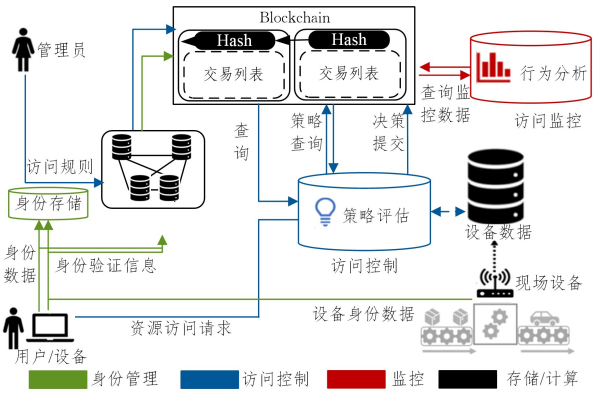

图 1 基于区块链的访问控制抽象模型[28](电子版为彩色)

Fig. 1 Abstract model of access control based on blockchain[28]

3.1.1 身份管理

用户、设备及服务的身份信息将以防篡改的方式保存在区块链上，并通过交易进行管理。可用注册、认证、更新或撤销等交易来新增、更新或删除用户、设备及服务的身份。

3.1.2 访问控制

利用区块链以防篡改的方式存储对“特定资源访问权限”的描述，并通过区块链交易来管理这些权限。访问控制策略由资源所有者(一般是管理员)定义，该资源所有者可以向区块链发出创建交易、更新交易和撤销交易请求来建立新的访问控制策略。资源所有者需要能够根据检测到的用户行为信息自适应地更改其访问控制策略，所有这些在区块链上的操作及更改(如策略更新和访问权限的转移等)都带有时间戳，并且以可审核、可追踪的方式记录到区块链中。

“访问策略执行点”在收到主体(用户/设备)对资源的访问请求时，如用户希望读取现场设备传感器上的数据，将通过该用户的身份信息基于认证机制对主体进行身份验证，并向区块链查询包含基于角色的访问控制相关策略数据的交易，然后建立标准的 XACML 策略，该策略会传输到策略决策点，并根据主体所具有的角色对其进行验证评估，授予其对资源的访问权限，如根据该用户的身份信息查询该用户对应的角色及其可能具有的权限。

3.1.3 监控和存储

区块链存储的防篡改、永久性等特征适合于存储管理用户个人信息、日志数据和企业敏感数据等数据信息。在监控方面，区块链本身可以被视为日志存储，任何用户/设备的动作都将附加到区块链上，包括身份的唯一标识符以及有关其动作的其他信息，这些信息可能是评估的相应权利或任何其他可用的特征。然后，可以通过对身份的行为与区块链中保留的历史使用模式进行比较来检测恶意活动，并且可以遍历区块链并搜索具有身份唯一标识符的所有日志来进行检索。与传统日志记录机制相比，一个优势是区块链内的去中心化数据存储，恶意攻击者无法通过仅针对一个日志服务器来轻松地操纵日志收集。由于日志是通过区块链技术存储在许多不同的设备上，攻击者需要保持对特定数量设备的控制。

基于区块链的技术能够开发可靠的监控系统，用户无法否认已批准的提交交易，因为区块链的可信性已由节点网络的共识机制验证，只有有效的交易才能保存在区块链中，以确保记录信息的不可否认性，结合智能合约的区块链可以提供强大的备份和监视功能。由于去中心化的存储方式能在任何时间离开或重新加入网络，已发布的交易的完整日志都将保留在区块链中，访问相应日志仅需要下载最新版本的区块链，只要网络中存在节点，就能够维护区块链的日志。

3.2 基于角色的访问控制

RBAC96[19]采用角色的概念来控制用户对资源的访问，每个角色都有对应的权限，给每个用户按照其职责分配相应的角色，用户就可以拥有此角色对应的权限。图 2 给出了 RBAC96 层次结构的主要组件，主要由 6 部分构成：用户、角色、对象、会话、权限和操作。权限是被赋予给角色的，一旦用户被授予某个角色，那么该用户就拥有此角色所具有的权限。会话代表用户和角色间的映射关系，用户必须通过会话才可以设置角色。其中，UA 代表用户角色分配，PA 代表角色与权限分配，RBAC96 要求用户和角色以及角色和权限之间都是多对多的关系。

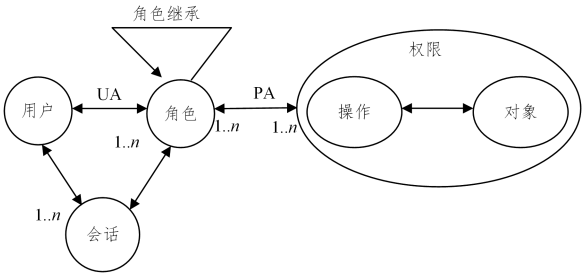

图 2　RBAC96 层次模型[19]

Fig. 2　RBAC96 hierarchical model[19]

RBAC96 遵循以下安全原则：最小特权原则和职责分离原则。最小特权原则指分配给用户的角色所对应的权限不能超过用户完成其工作任务所需的最大权限。职责分离原则指在用户完成其工作任务时分配两个职责上相互约束的角色。RBAC96 有两大显著的优点：1）它简化了用户与权限的复杂关系，通过将角色与权限关联，用户可以通过被授予不同的角色而获得不同的访问权限，使得对用户的授权管理变得非常简单和易于维护，从而使方案具有很大的伸缩性；2）RBAC 中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，可以降低授权的复杂性，减少组织的管理成本。

3.3　角色委派访问控制模型

文献[20]提出了基于角色的委派模型，但该框架主要针对用户对用户的委派，用户将自己的角色委派给他人，相当于是将自己的全部权限委派出去。然而，在很多情况下，尤其为了组织的整体安全考虑，用户可能只会将自己的部分权限进行委派。PBDM1 模型[21]支持角色、权限的委派，委派者通过创建委派角色，将要委派出去的权限分配给该角色，再将此角色授予被委派对象，从而达到委派的目的。

为了避免委派者将重要权限委派出去，在 PBDM1 中，将角色分为常规角色（RR）、委派角色（DTR）和可委派角色（DBR）。DBR 指可以通过创建委派角色将委派者的权限委派给其他用户的角色，每个 DBR 都基于一个 RR，分配给 DBR 的用户与它所基于的分配给 RR 的用户完全相同，即一组 RR 与 DBR 在用户与角色分配中可被看作单个角色。相应地，UA 也分为用户与常规角色分配（UAR）、用户与委派角色分配（UAD）以及用户与可委派角色分配（UAB），PA 也分为常规角色权限分配（PAR）、委派角色权限分配（PAD）与可委派角色权限分配（PAB）。图 3 给出了 PBDM1 模型。

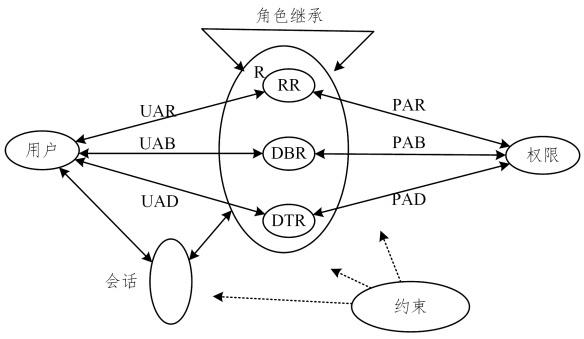

图 3　PBDM1 模型[21]

Fig. 3　PBDM1 model[21]

4　简化的工业企业网络模型

根据工业企业网络参考模型 PERA[55]，简化的工业控制系统网络模型如图 4 所示，主要包括企业区、DMZ 区和现场设备区。本文假设由云管理中心、不同区域的域管理员联合执行用户身份管理、角色委派、访问控制、监视和记录的任务。云中心负责在区块链网络上发布有关访问控制的所有合约：用户与角色管理合约、委派合约，访问控制合约、监视合约，并为申请访问的用户授予角色。当新用户加入网络时，由云中心对用户进行身份管理，并通过智能合约为每个用户分配与他们的身份信息相符合的角色。当某一域内的用户想要访问网络资源时，可通过向云中心或域管理员发送申请访问的交易，云中心或域管理员通过调用合约对用户进行策略评估，如果验证通过，则允许访问，验证失败则拒绝访问。当某一域中的用户或域外的用户想要访问另一域的网络资源时，该用户可以向另一域中拥有访问该网络资源权限的用户申请权限委派，从而达到访问的目的。

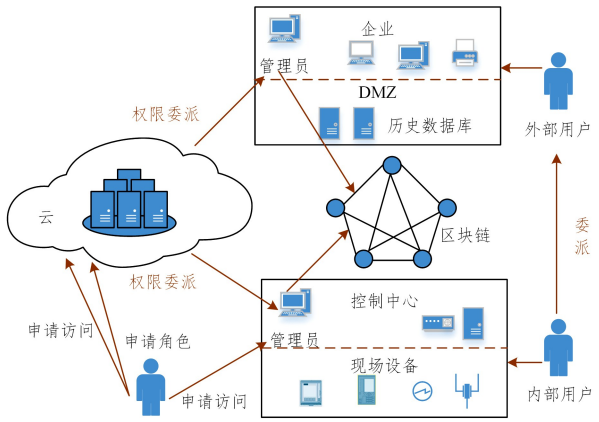

图 4　简化的工业控制系统网络模型

Fig. 4　Simplified industrial control system network model

5　基于区块链的 DRBAC 方案

5.1　用户与角色管理

系统中的用户大致分为两类：内部员工和有商业往来的客户。内部员工拥有他所在部门的属性，而商业客户也有其相对应的身份属性，如需设备供应商远程维护企业设备等。区块链网络节点必须拥有一个账户地址，才可与网络进行交互，因此系统中每个用户加入区块链网络后要创建一个由其公私钥对控制的账户地址，这是该用户的唯一标识符。为防止发生用户身份盗窃，需要将用户的身份信息以及对应的账户地址保存在区块链网络中进行集中管理与保护，防止恶意修改。若用户的身份发生变化，云中心可通过发送交易来对此记录进行更新或删除。

新用户通过发送交易向云中心申请角色，云中心调用智能合约，根据用户的身份信息为其授予相应的角色。系统中的角色按照用户的身份，主要分为两大类：内部角色和外部角色。外部角色有：需要访问系统设备数据的外部供应商、监管实体、系统集成商、商业合作伙伴等。系统规定这些具有外部角色的用户只能通过得到云中心或域管理员的委派授权才可访问系统设备或资源。系统内部角色有：初级操作员、高级操

作员、设备维修人员、现场技术人员、主管、操作工程师、系统管理员等。其中，系统中的内部角色及其对应权限如表 1 所列。

表 1 系统内部角色及其对应权限

Table 1 Internal roles in the system and their corresponding permissions

角色	操作
初级操作员	查看任何屏幕
高级操作员	初级操作员＋更改控制器的设置点，确认警报
主管	初级操作员＋高级操作员，更改警报点，禁用控制器、禁用警报
设备维修人员	查看设备信息，更改设备状态
现场技术人员	轮询和查看现场模拟数据、分析所有警报报告，简单配置
工程师	调优控制器，复杂配置，指派安全代码
系统管理员	拥有以上所有操作

5.2 角色委派

5.2.1 委派管理

角色及权限委派由委派者负责创建并管理，委派的权限既可以是委派者的全部权限也可以是部分权限，这样便实现了角色委派，也实现了部分权限委派，并且遵循最小权限委派原则，即委派者仅委派受委派者完成其工作任务所需的必要权限。系统中的常规角色与可委派角色是永久角色，而委派角色是由委派者设置的临时角色。常规角色和可委派角色间的权限、用户分配由云中心进行控制，委派角色的权限、用户分配则由域中需要委派的委派者进行管理，如云中心可以提前指定哪些角色或者权限可以被委派，从而达到对委派的管理。

5.2.2 委派撤销

由于常规角色与可委派角色是由云中心设置的，而委派权限的分配以及委派角色与用户的分配由域中需要委派的委派者管理，因此委派撤销可分为云中心撤销和委派者撤销两种。云中心可以实现如下操作：1）从可委派角色删除一个或多个权限；2）从常规角色和可委派角色中删除用户。委派者可以实现如下操作：1）从被委派者中删除用户，即撤销用户与委派角色的分配；2）从委派角色中删除一个或多个权限；3）撤销授权角色。

5.2.3 委派实例

在一些组织中，一个角色可以包含另一个角色关联的权限，当权限重叠时，可以建立角色的层次结构。为了明确角色与权限的重要性，本文对 ICS 的角色进行相应划分。图 5 为系统的角色层次结构图，角色之间有一定的重叠性，如主管拥有初级操作员、高级操作员拥有的权限，这是通过将初级操作员、高级操作员的角色分配给主管来获得的。为了描述委派的过程，表 2 列出了系统部分常规角色与用户以及权限的分配。

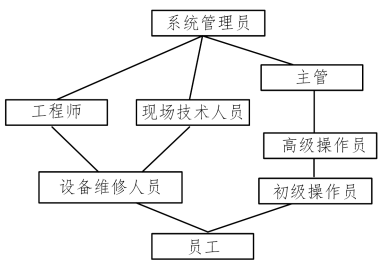

图 5 系统角色层次结构

Fig. 5 System role hierarchy structure

表 2 部分常规角色与用户、权限的分配

Table 2 Part of the regular roles and users, permission assignment

用户	角色	权限
用户 A	主管(SV,SV′)	更改警报点、禁用控制器、禁用警报
用户 B	高级操作员(SO,SO′)	更改控制器的设置点、确认警报
用户 C	初级操作员(JO,JO′)	查看任何屏幕

通过将部分权限分配给可委派角色可达到让域管理员更方便、安全地管理系统中的权限委派的目的。在用户与角色的分配中，每个可委派角色都基于一个常规角色，分配给可委派角色的用户与它所基于的分配给常规角色的用户完全相同，但在进行委派时，用户只能从可委派角色中进行权限的委派，而不能将分配给常规角色的权限委派给其他用户。

图 6 给出了部分常规角色与可委派角色的层次结构。图 6 中共有 3 个不同的角色层：常规角色(RR)、可委派角色(DBR)和委派角色(DTR)，图 7 则是这 3 种角色对应的权限分配。

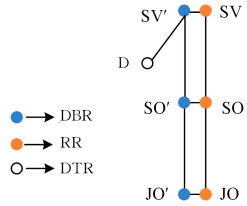

图 6 常规角色与可委派角色的层次结构

Fig. 6 Hierarchical structure for regular roles and delegatable roles

PAR

RR	权限
SV	禁用警报、更改警报点
SO	更改控制器的设置点
JO	

PAB

DBR	权限
SV′	禁用控制器
SO′	确认警报
JO′	查看屏幕

PAD

DTR	权限
D	禁用控制器 查看屏幕

图 7 常规角色、可委派角色、委派角色的权限分配

Fig. 7 Regular roles, delegatable roles and pemissions assignment for delegatable roles

当某一用户进行跨域访问时，需要向另一域中的用户申请权限委派，如当某一用户想要查看现场操作屏幕并获得更改警报点的权限时，该用户向拥有主管角色的用户 A 进行权限申请，用户 A 可以将他的部分可委派权限，即“禁用控制器”进行委派，并且由于系统中角色层次结构的对应关系，主管拥有初级操作员的全部权限。用户 A 也可以将初级管理员拥有的可委派权限进行委派。故用户 A 将通过以下 3 个阶段完成权限的委派：

(1)用户 A 创建委派角色 D。

(2)用户 A 通过角色与权限分配，将“SV′”“禁用控制器”权限委派给角色 D，还可通过角色与角色分配，将角色“JO′”委派给角色 D。

(3)用户 A 通过用户与角色分配，将委派角色 D 授予该用户。

至此，该用户就获得了主管的部分权限“禁用控制器”以及初级操作员的全部权限。然后他就可以向系统申请访问，以获得相应的资源。

5.3　访问控制

访问控制的流程如图 8 所示。拥有角色的用户可以通过发送交易，向云中心或者域管理员申请访问系统资源，如果用户想要跨域访问，则必须先申请权限的委派。为防止用户执行角色欺骗或越权访问而给系统带来严重威胁，云中心或者域管理员会对用户进行策略评估，检测用户是否拥有他所声称的角色，以及所拥有的权限。如果验证通过，则同意访问，若失败则拒绝访问。但如果一个用户策略评估失败的次数大于 2，为防止这些不良行为给系统带来的资源浪费以及潜在的危险，DRBAC 方案采用问责机制，将拥有不良行为的用户加入黑名单，除非云中心将其从黑名单移除，否则黑名单中的用户将永远被禁止访问任何系统资源。

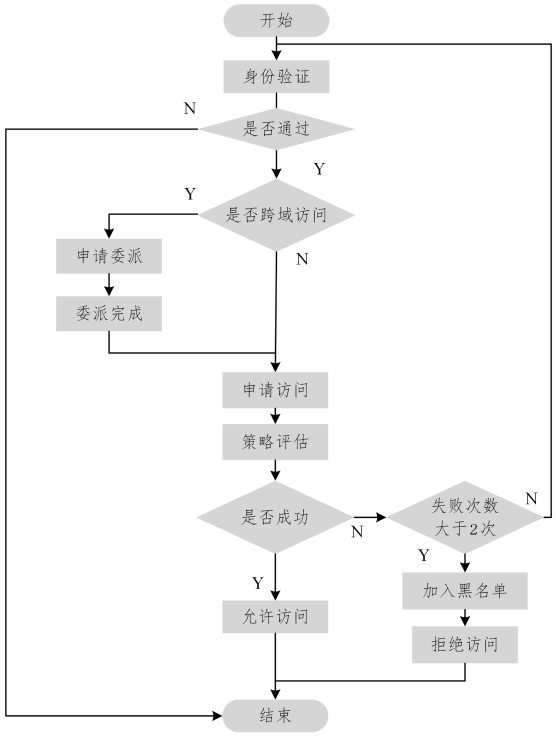

图 8　访问控制流程图

Fig. 8　Flow chart of access control

5.4　监控

审计跟踪、记录特定对象在给定的时间间隔内的所有活动，是 NIST[17] 强调的工业控制系统安全的重要特性。为了避免系统受到网络攻击，需要建立监视和纠错控制，以实现对系统进行本地或远程访问时所涉及的所有行为的问责与可追溯性。因此，在对系统进行访问控制时，要有安全日志记录，以及必须确保用户在访问关键基础设施时达到期望的信任级别，尤其对于系统外部用户，应该一直监视用户的行为，检测其异常行为并进行记录，从而限制非法用户的访问。

区块链本身可被视为一个防篡改的日志存储，因此用户对网络的操作都记录在区块链上，其中也包括用户的唯一标识符及其行为。由于区块链的共识机制以及分布式特性，已发出交易的完整日志都将保留在区块链中，用户不能否认已经被批准的交易。任何用户对系统的操作都将永久存储在区块链中，通过遍历区块链并搜索具有用户唯一身份标识符的所有日志，就可以发现用户的非法行为，如短时间内访问太过频繁、存在角色欺骗行为等。并且，由于区块链本身具有的去中心化的存储方式，攻击者无法轻易对日志记录进行修改或者删除。

6　基于智能合约的 DRBAC 方案的实现

如图 9 所示，DRBAC 的总体架构主要由 4 个合约实现：角色管理合约、访问控制合约、监控合约和角色委派合约。

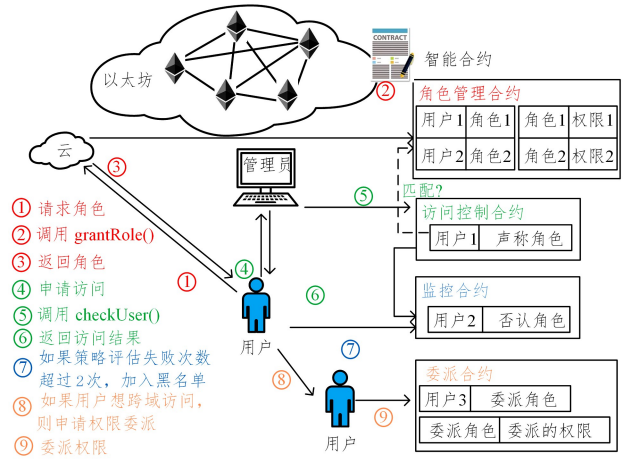

图 9　基于智能合约的访问控制体系结构

Fig. 9　Structure of access control system based on smart contract

角色管理合约定义了系统访问控制所需要的全部角色及其对应权限，并为每个申请访问的内外部用户分配适合其身份的角色；访问控制合约定义了访问控制策略，当用户向云中心或域管理员申请访问设备时，后者会调用该合约对该用户进行访问策略评估，检查用户是否拥有他所声称的角色，以及是否有相应的权限。另外，根据问责机制，访问控制合约会自动调用监控合约，通过给用户授予“DENY_ROLE”角色的方式，将用户加入黑名单；监控合约用于跟踪监视用户的行为，处理有非法行为的用户，如果用户进行策略评估时失败的次数大于 2，则将此用户加入黑名单，禁止访问；委派合约定义了用户进行跨域访问的方法，用户可向拥有该权限的其他用户申请权限委派，实现跨域访问。

6.1　DRBAC 访问控制操作

DRBAC 框架由角色管理合约、访问控制合约、监控合约和委派合约组成，由云中心负责在区块链网络上发布有关访问控制的所有合约，区块链中的每个节点通过所提供的合约地址和 RPC 接口与智能合约进行交互。图 10 给出了 DRBAC 智能合约的框架。

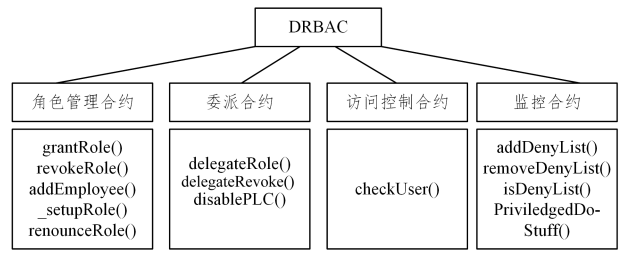

图 10　DRBAC 智能合约的框架

Fig. 10　Smart contract framework of DRBAC

DRBAC 模型中的智能合约的主要函数如下。

(1)grantRole()。将角色授予用户,输入参数为角色的"bytes32"标识符和用户账户地址。函数要求调用者必须为该角色的管理员。

(2)revokeRole()。撤销用户角色,输入参数为角色的"bytes32"标识符和用户账户地址。函数要求调用者必须为该角色的管理员。

(3)addEmployee()。将"员工"角色授予用户,输入参数为用户的账户地址。该函数会自动调用 grantRole()。

(4)_setupRole()。将角色授予用户,输入参数为角色的"bytes32"标识符和用户账户地址。与 grantRole()不同的是,这个函数不对调用的用户执行任何检查,即不要求调用的用户必须是该角色的管理员。这个函数只能在为系统设置初始角色时从构造函数中调用。

(5)renounceRole()。用户自己撤销自己的角色,输入参数为角色的"bytes32"标识符和用户账户地址。函数要求调用者必须与输入的用户账户地址一致("DENY_ROLE"角色除外),如用户发生身份被盗用、遇到一些危急情况时,可调用该函数撤销自己的角色。

(6)delegateRole()。将委派角色授予某用户,当拥有某角色的用户将自己拥有的部分权限委派出去时调用。输入参数为用户设置的临时委派角色的"bytes32"标识符和被委派者的账户地址。

(7)delegateRevoke()。撤销某用户的委派角色,当委派者要撤销自己授权的角色时调用。输入参数为委派角色的"bytes32"标识符和被委派者的账户地址。

(8)disablePLC()。禁用对资源的访问(如 PLC 控制器)是主管对应的权限,只有拥有主管角色的用户才可调用该函数。本文以主管拥有"禁用 PLC 控制器"的权限为例,说明委派机制。

(9)checkUser()。对用户进行策略评估,检查用户是否拥有他所声称的角色,输入参数为用户声称的角色的"bytes32"标识符和用户账户地址。如果策略评估成功,则发出 Successful 事件,否则发出 Failed 事件,如果用户失败的次数超过 2,则调用监控合约,将用户加入黑名单。

(10)addDenyList()。用户策略评估失败次数超过 2 时,会自动授予"DENY_ROLE"角色,输入为用户账户地址。

(11)removeDenyList()。可通过撤销用户的"DENY_ROLE"角色,将用户从黑名单中移除,输入参数为用户账户地址。

(12)isDenyList()。用于判断某用户是否属于黑名单中的一员,输入参数为用户账户地址。

(13)priviledgedDoStuff()。与 isDenyList()作用相似,只有不在黑名单中的用户才可调用。

6.2 DRBAC 访问控制流程

如图 11 所示,新用户加入区块链网络后向云中心申请角色,云中心调用合约,根据用户的身份信息为用户授予相应角色,并将结果更新于智能合约。角色可以通过 grantRole()和 revokeRole()函数动态地授予和撤销。如果用户想要跨域访问某资源,可以通过让委派者调用 delegateRole()得到访问该资源的权限。在用户申请访问之前,还需要进行最重要的一个步骤,即通过调用 checkUser()函数,对申请访问的用户进行策略评估,这是为防止不良非法行为的出现,如果用户出现角色欺骗、越权行为等,能及时加以制止。如果用户策略评估失败的次数超过 2,则会自动调用函数 addDeny(),将用户加入黑名单,该函数会给用户授予"DENY_ROLE"角色,从而达到将用户加入黑名单的目的,禁止其再次访问系统。合约以键-值数据结构存储所需的数据,生成的数据结构如表 3 所列。

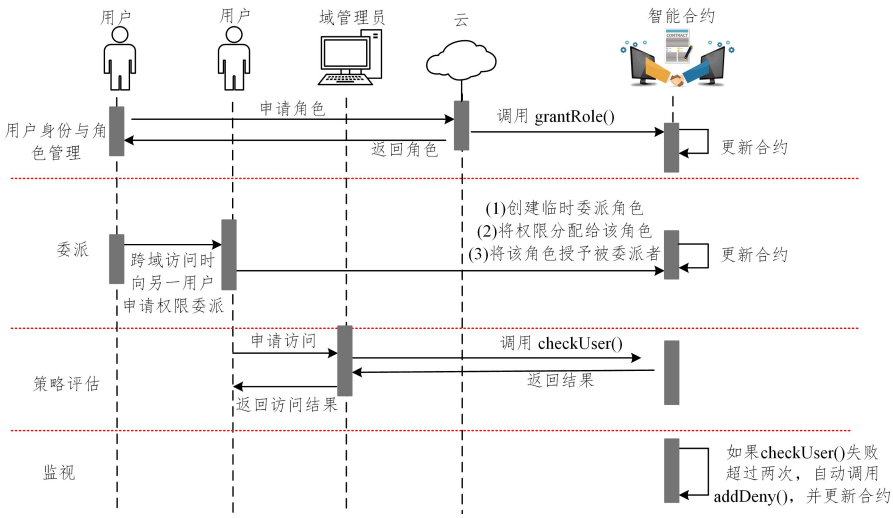

图 11 访问控制过程

Fig. 11 Access control process

表 3 数据结构

Table 3 Data structure

映射	键	值
_roles	bytes32	RoleData
Blacklist	Address	bool
illegalBehavior	Address	Person

6.3 DRBAC 访问控制算法

算法 1 是关于访问控制的算法,该算法接收用户账户地址与角色的"bytes32"标识符,并返回访问结果。第 1—4 行用于判断用户是否跨域访问,第 5—8 行是策略检查,验证用户声称的角色是否与其账户地址对应,第 10—12 行实现对验

证失败超过 2 次的用户进行问责处理，即将其加入黑名单中。第 19 行中的事件 returnResult(result)用于返回访问结果。

算法 1　访问控制算法

输入：bytes32 role，address account

输出：bytes32 role，address account

Require：policyCheck ← false，illegalbehaviorCheck ← true，policy list policies.

1. if the user want to cross-domain access then
2. request delegate and request access.
3. else
4. request access directly.
5. if the user is member of the asserted role then
6. p ← policies[bytes32][account].
7. if p.policy＝“allow” then
8. policyCheck ← true.
9. else
10. policyCheck ← false.
11. illegalBehavior[account].adr＝account；
12. illegalBehavior[account].count ＋＝ 1；

end if

13. if illegalBehavior[account].count ＞ 2 then
14. illegalbehaviorCheck← false.addDenyListed(account).
15. end if
16. end if
17. end if
18. result ← policyCheck and illegalbehaviorCheck.
19. Trigger event returnResult(result).

7　基于私有区块链的 DRBAC 方案验证

7.1　环境搭建及系统配置

本文使用以太坊平台实现 DRBAC 框架，以太坊是一个开放的区块链平台，允许部署智能合约，这些智能合约是由消息和交易触发的自执行脚本，由 solidity 语言编写。所有参与访问控制的设备通过安装一个 Go-Ethereum(简称 geth)客户机，来转换为以太坊节点，每个节点都可以直接与区块链交互、调用智能合约，并发送交易来运行智能合约的 ABIs，这些节点还可以充当矿工进行挖矿。智能合约通常提供许多函数或 ABIs，用于与之交互，可以通过从账户发送交易或从另一个合约发送消息来执行这些 ABIs。为了在系统的云中心和域管理员端编写、编译智能合约，本文使用 Remix 集成开发环境(IDE)。另外，采用 web3.js(即通过 HTTP 连接与相应的 geth 客户端进行交互)，以部署编译后的智能合约，在用户端也安装了 web3.js，以便与 geth 交互。

为了验证本文方案的正确性和有效性，并为访问控制框架的评估提供依据，本文采用一台台式机、一台笔记本电脑和两台 Raspberry Pi 单板电脑在本地搭建私人区块链平台，以模拟整个访问控制流程。笔记本电脑扮演云中心，一台 Raspberry Pi 充当域管理员，另一台作为申请访问的用户，台式机因其强大的计算能力而扮演矿工节点。实验所用的设备规格如表 4 所列。

表 4　设备规格

Table 4　Equipment specifications

设备	CPU	操作系统	内存
HUAWEI MateBook 14	Inter Core i7-10510U，2.30 GHz	Windows 10 Home(64 bit)	16 GB
Lenovo	Intel Core i3-4160T，3.10 GHz	Ubuntu	8GB
Raspberry Pi 3 Model B	quad-core ARMv8，1.2 GHz	Raspbian/ Linux kernel	1 GB LPDDR2-900 SDRAM

7.2　DRBAC 方案测试

图 12 给出了调用函数 addEmployee()给新注册的用户授权“员工”角色，这意味着该用户会拥有“员工”的全部权限。图 13 给出了在用户申请访问时域管理员对其进行策略评估的过程，通过调用函数 checkUser()，输入其声称角色与账户地址，如果返回 Successful 事件，则证明策略评估成功，准予访问。

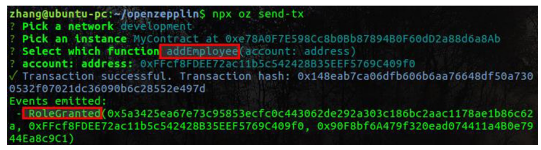

图 12　授予用户角色

Fig. 12　Grant user roles

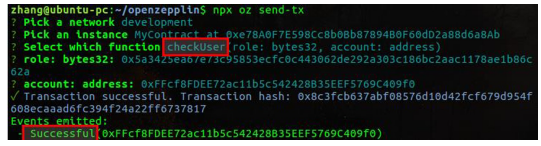

图 13　对用户进行策略评估

Fig. 13　Policy evaluation for users

相反，图 14 给出了一个验证失败的示例。如果用户验证失败，并且失败超过 2 次，那么在第三次时不仅会被拒绝访问，而且用户还会被加入黑名单，禁止其再次访问系统。为了验证上述函数的结果，由图 15 可以看到：调用 isDenyList()函数输入账户地址，结果返回 true，证实此用户已经被加入黑名单。当使用此账户地址调用函数 priviledgedDoStuff()，结果报错，显示无法调用函数。

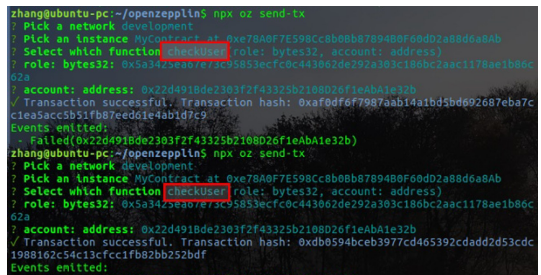

图 14　策略评估失败超过 2 次

Fig. 14　Policy evaluation failed more than two times

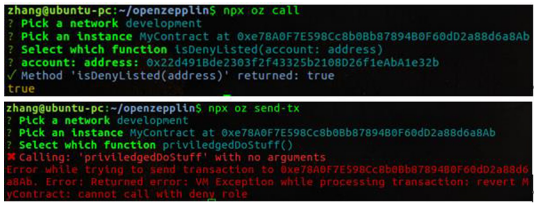

图 15 将用户加入黑名单并进行验证

Fig. 15 Add users to the blacklist and verify

为了验证角色委派过程，本文还是以拥有“主管”角色的用户 A 将其拥有的部分可委派权限委派给某一用户为例，如用户 A 拥有“禁用控制器”的可委派权限，即 disablePLC()，现在用户 A 将此权限委派给其他用户，用户 A 通过创建委派角色，将要委派的权限授予该角色，即将 disablePLC()函数设置为只有拥有委派角色才能调用它，并调用函数将委派角色授予该用户，从而完成委派，如图 16 所示。

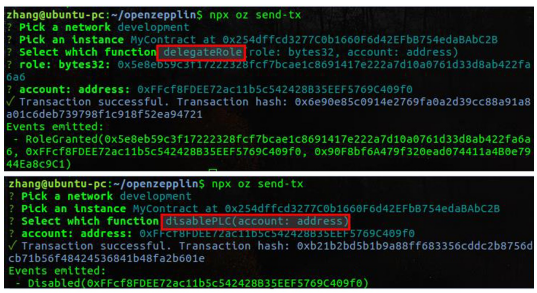

图 16 委派过程

Fig. 16 Process of delegation

7.3 结果分析

当合约中的代码被交易触发执行时，网络中每个负责传播、验证、执行交易的节点都要执行这段代码，执行的成本用燃油费(gas)表示。因此，在区块链中与智能合约交互或对区块链执行任何其他操作时，交易的发送方都要为此操作付出一定的代价，即需要支付相应的 gas。以太(ether)是以太坊的通用货币，gas 总是用 ether 支付。

在 2020 年 11 月实验评估期间，1 ether≈388.44 USD，而 1 gas≈1×10^{9} ether，这是执行交易的最小成本。图 17 给出了调用函数 priviledgedDostuff()时，发送交易所产生的 gas。

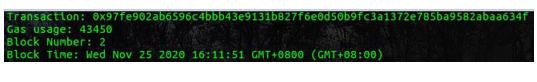

图 17 发送某交易时消耗的 gas

Fig. 17 Gas consumed when sending a transaction

表 5 列出了执行本文方案 DRBAC 框架时调用智能合约中的函数的相应成本。由此可以看出，创建智能合约的一次性成本为 0.5535 美元(与智能合约中函数的数目有关)。相比之下，执行合约中函数的成本比较低。表 5 还显示，grantRole()，checkUser()，addDenyListed()这 3 个函数的执行成本分别为 0.0347 美元、0.0261 美元、0.0345 美元，与智能合约中的其他函数相比，对它们的操作需要更高的成本，这是由于该操作需要多个执行步骤，尤其是对同一用户执行 checkUser()，如果用户连续 3 次策略评估都失败，则这时操作需要更高的成本。

表 5 调用不同函数的成本

Table 5 Cost of calling different functions

DRBAC function	Gas used	Cost/ether	USD/$
Create Contract	1 424 909	0.001 424 909	0.5535
grantRole()	89 375	0.000 089 375	0.0347
revokeRole()	24 325	0.000 024 325	0.0094
checkUser()	67 299	0.000 067 299	0.0261
delegateRole()	73 591	0.000 073 591	0.0286
disablePLC()	23 175	0.000 023 175	0.0090
addDenyListed()	88 948	0.000 088 948	0.0345
removeDenyListed()	24 123	0.000 024 123	0.0094
renounceRole()	22 594	0.000 022 594	0.0088
priviledgedDostuff	43 450	0.000 043 450	0.0169

结束语 本文采用 RBAC 策略以及基于角色的委派机制，结合区块链技术和智能合约机制，提出了基于区块链技术的角色委派访问控制方案(DRBAC)，该框架主要由用户角色管理及委派、访问控制、问责机制 3 部分组成，通过将 RBAC 和角色委派编码为智能合约，实现对系统中内部及外部用户分布式、可信、灵活的访问控制，来实现保护每个网络连接的目的。为了验证 DRBAC 的可行性，在本地私有区块链中进行测试并进行分析，结果证实本文方案可以为工业企业网络提供动态、细粒度的初步访问控制方案。除进一步改进和完善本文提出的方案外，考虑更深层的委派机制及智能合约的安全和隐私保护问题是未来的主要工作。

参 考 文 献

[1] LI Q, TANG Q L, CHEN Y T, et al. Research on Intelligent Manufacturing System Architecture, Reference Model and Standardization Framework[J]. Computer Integrated Manufacturing System, 2018, 24(3): 539-549.

[2] LI J, QIU J J, SHAO M K, et al. Research on the status quo, restriction factors and improvement countermeasures of the key technologies, products and industrial ecology of the integration of industrialization and industrialization in my country[J]. Computer Integrated Manufacturing System, 2019, 25(9): 2334-2343.

[3] WANG F Y, ZHANG J, ZHANG J, et al. Industrial Intelligent Networking: Basic Concepts, Key Technologies and Core Applications[J]. Acta Automatica Sinica, 2018, 44(9): 1606-1617.

[4] WANG W H, CHEN Z Y. Intelligent Manufacturing Security Model Based on Improved Blockchain[J]. Computer Science, 2021, 48(2): 295-302.

[5] FILKINS B, DOUG W, JASON D. SANS 2019 State of OT-ICS Cybersecurity Survey [EB/OL]. SANS Survey, 2019. https://www.sans.org/webcasts/2019-state-ot-ics-cybersecurity-survey-109625/.

[6] WANG Y T. “New infrastructure” boosts the overall upgrade of artificial intelligence infrastructure[J]. Communication World, 2020(7): 20-21.

[7] GONZALEZ D, ALHENAKI F, MIRAKHORLI M. Architectural Security Weaknesses in Industrial Control Systems (ICS) an Empirical Study Based on Disclosed Software Vulnerabilities [C]// 2019 IEEE International Conference on Software Architecture (ICSA). Hamburg, Germany, 2019: 31-40.

[8] SHA L T, XIAO F, CHEN W, et al. Backdoor privacy leakage perception method for industrial IoT environment[J]. Journal of Software, 2018, 29(7): 1863-1879.

[9] ZHANG W A, HONG Z, ZHU J W, et al. Overview of network intrusion detection methods for industrial control systems[J]. Control and Decision, 2019, 34(11): 2277-2288.

[10] ROSE S, BORCHERT O, MITCHELL S, et al. Zero Trust Architecture[R]. National Institute of Standards and Technology, 2020.

[11] 深云 SDP[EB/OL]. https://www.deepcloudsdp.com/index.html.

[12] ROSIC D, NOVAK U, VUKMIROVIC S. Role-Based Access Control Model Supporting Regional Division in Smart Grid System[C]// 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks. Madrid, 2013: 197-201.

[13] NASR P M, VARJANI A Y. An alarm based access control model for SCADA system[C]// 2015 Smart Grid Conference (SGC). Tehran, 2015: 145-151.

[14] YANG H. Research on Security Access Technology of Wind Farm SCADA System Based on Identity Authentication[D]. Beijing: North China Electric Power University, 2016.

[15] FIGUEROA-LORENZO S, AÑORGA J, ARRIZABALAGA S. A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach[J]. Sensors, 2019, 19(20): 4455.

[16] ES-SALHI K, ESPES D, CUPPENS N. DTE Access Control Model for Integrated ICS Systems[C]// Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). New York, NY, USA, 2019: 1-9.

[17] STOUFFER K, FALCO J, SCARFONE K. Guide to industrial control systems (ICS) security[J]. NIST Special Publication, 2011, 800(82): 16.

[18] GILSINN J. ISA-99-Industrial Automation & Control Systems Security ISA99 Committee • Addresses Industrial Automation and Control [EB/OL]. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99.

[19] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[20] BARKA E, SANDHU R. Framework for role-based delegation models[C]// Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00). New Orleans, LA, USA, 2000: 168-176.

[21] ZHANG X, OH S, SANDHU R. PBDM: a flexible delegation model in RBAC[C]// Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies (SACMAT'03). New York, NY, USA, 2003: 149-157.

[22] CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.

[23] ZENG S Q, HUO R, HUANG T, et al. A review of blockchain technology research: principles, progress and applications[J]. Journal on Communications, 2020, 41(1): 134-151.

[24] SHAO Q F, ZHANG Z, ZHU Y C, et al. Overview of enterprise-level blockchain technology[J]. Journal of Software, 2019, 30(9): 2571-2592.

[25] BUTERIN V. Ethereum: a next generation smart contract and decentralized application platform [EB/OL]. http://ethereum.org/ethereum.html.

[26] LIU A D, DU X H, WANG N, et al. Big data access control mechanism based on blockchain[J]. Journal of Software, 2019, 30(9): 2636-2654.

[27] DU R Z, LIU Y, TIAN J F. Access control method based on smart contract in the Internet of Things[J]. Computer Research and Development, 2019, 56(10): 2287-2298.

[28] NUSS M, PUCHTA A, KUNZ M. Towards blockchain-based identity and access management for internet of things in enterprises[C]// International Conference on Trust and Privacy in Digital Business. Cham: Springer, 2018: 167-181.

[29] SHI J S, LI R. Summary of blockchain access control under the Internet of Things[J]. Journal of Software, 2019, 30(6): 1632-1648.

[30] MAESA D D F, MORI P, RICCI L. Blockchain based access control[C]// IFIP International Conference on Distributed Applications and Interoperable Systems. Cham: Springer, 2017: 206-220.

[31] MAESA F D D, MORI P, RICCI L, Blockchain Based Access Control Services[C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax, NS, Canada, 2018: 1379-1386.

[32] JEMEL M, SERHROUCHNI A. Decentralized Access Control Mechanism with Temporal Dimension Based on Blockchain [C]// 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE). Shanghai, 2017: 177-182.

[33] WANG S, ZHANG Y, ZHANG Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. IEEE Access, 2018, 6: 38437-38450.

[34] HU S, HOU L, CHEN G, et al. Reputation-based distributed knowledge sharing system in blockchain[C]// Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous'18). New York, NY, USA, 2018: 476-481.

[35] FERDOUS M S, MARGHERI A, PACI F, et al. Decentralised Runtime Monitoring for Access Control Systems in Cloud Federations[C]// 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). Atlanta, GA, 2017: 2632-2633.

[36] ALANSARI S, PACI F, SASSONE V. A Distributed Access Control System for Cloud Federations[C]// 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). Atlanta, GA, 2017: 2131-2136.

[37] ZHANG Y Y, KASAHARA S, SHEN Y L, et al. Smart Contract-Based Access Control for the Internet of Things[J]. IEEE Internet of Things Journal, 2018, 6(2): 1594-1605.

[38] CRUZ J P, KAJI Y, YANAI N. RBAC-SC: Role-based access

control using smart contract[J]. IEEE Access, 2018, 6: 12240-12251.

[39] YAN Z, GAN G, RIAD K. BC-PDS: Protecting Privacy and Self-Sovereignty through Blockchains for OpenPDS[C]// 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE). San Francisco, CA, 2017: 138-144.

[40] RAHMAN M U, GUIDI B, BAIARDI F, et al. Context-Aware and Dynamic Role-Based Access Control Using Blockchain[C]// International Conference on Advanced Information Networking and Applications. Cham: Springer, 2020: 1449-1460.

[41] GUO H, MEAMARI E, SHEN C C. Multi-authority attribute-based access control with smart contract[C]// Proceedings of the 2019 International Conference on Blockchain Technology. 2019: 6-11.

[42] MAESA D D F, MORI P, RICCI L. A blockchain based approach for the definition of auditable Access Control systems [J]. Computers & Security, 2019, 84: 93-119.

[43] CRAMPTON J, KHAMBHAMMETTU H. Delegation in role-based access control[J]. International Journal of Information Security, 2008, 7(2): 123-136.

[44] ZHANG L, AHN G J, CHU B T. A rule-based framework for role-based delegation and revocation[J]. ACM Transactions on Information and System Security (TISSEC), 2003, 6(3): 404-441.

[45] WANG R. Research on attribute-based delegated access control model and its application in smart home[D]. Xi'an: Xidian University, 2019.

[46] 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.

[47] PUSSEWALAGE H S G, OLESHCHUK V A. Blockchain Based Delegatable Access Control Scheme for a Collaborative E-Health Environment[C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax, NS, Canada, 2018: 1204-1211.

[48] TAPAS N, MERLINO G, LONGO F. Blockchain-Based IoT-Cloud Authorization and Delegation[C]// 2018 IEEE International Conference on Smart Computing (SMARTCOMP). Taormina, 2018: 411-416.

[49] LE T, MUTKA M W. CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments[C]// 2018 IEEE International Conference on Smart Computing (SMARTCOMP). Taormina, 2018: 57-64.

[50] OUADDAH A, ABOU ELKALAM A, AIT OUAHMAN A. FairAccess: a new Blockchain-based access control framework for the Internet of Things[J]. Security and Communication Networks, 2016, 9(18): 5943-5964.

[51] XU R, CHEN Y, BLASCH E, et al. BlendCAC: A BLockchain-Enabled Decentralized Capability-Based Access Control for IoTs [C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax, NS, Canada, 2018: 1027-1034.

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

[53] NAKAMURA Y, ZHANG Y, SASABE M, et al. Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things[J]. Sensors, 2020, 20(6): 1793.

[54] LIN C, HE D, HUANG X, 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.

[55] ISA 95/PERA [EB/OL]. https://isa-95.com.

GUO Xian, born in 1971, associate professor, is a senior member of China Computer Federation. His main research interests include network and information security, blockchain and design and analysis of security protocol.