软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(3):1470−1490 [doi: 10.13328/j.cnki.jos.006778]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于区块链的物联网认证机制综述*

程冠杰[1], 邓水光[1], 温盈盈[1], 严学强[2], 赵明宇[2]

[1](浙江大学 计算机科学与技术学院, 浙江 杭州 310027)

[2](华为技术有限公司, 上海 201206)

通信作者: 邓水光, E-mail: dengsg@zju.edu.cn

摘　要: 随着物联网 (Internet of Things, IoT) 技术的高速发展, 各类智能设备数量激增, 身份认证成为保障 IoT 安全的首要需求. 区块链作为一种分布式账本技术, 提供了去信任的协作环境和安全的数据管理平台, 使用区块链技术驱动 IoT 认证成为学术界和工业界关注的热点. 基于云计算和云边协同两种架构分析 IoT 身份认证机制设计的主要需求, 总结区块链技术应用于 IoT 场景面临的挑战; 梳理现有 IoT 身份认证机制的工作, 并将其归结为基于密钥的认证、基于证书的认证和基于身份的认证; 分析应用区块链技术的 IoT 认证工作, 并根据认证对象和附加属性对相关文献进行归纳和总结. 从形式化和非形式化两个方向总结基于区块链的 IoT 认证机制的安全性分析方法. 最后展望了未来研究方向.

关键词: 物联网; 区块链; 身份认证; 多层认证; 边缘计算

中图法分类号: TP393

中文引用格式: 程冠杰, 邓水光, 温盈盈, 严学强, 赵明宇. 基于区块链的物联网认证机制综述. 软件学报, 2023, 34(3): 1470–1490. http://www.jos.org.cn/1000-9825/6778.htm

英文引用格式: Cheng GJ, Deng SG, Wen YY, Yan XQ, Zhao MY. Survey on Blockchain-based Internet of Things Authentication Mechanisms. Ruan Jian Xue Bao/Journal of Software, 2023, 34(3): 1470–1490 (in Chinese). http://www.jos.org.cn/1000-9825/6778.htm

Survey on Blockchain-based Internet of Things Authentication Mechanisms

CHENG Guan-Jie[1], DENG Shui-Guang[1], WEN Ying-Ying[1], YAN Xue-Qiang[2], ZHAO Ming-Yu[2]

[1](College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China)

[2](Huawei Technologies Co. Ltd., Shanghai 201206, China)

Abstract: With the rapid development of the Internet of Things (IoT), the number of smart devices has increased sharply, and identity authentication becomes the primary requirement for ensuring IoT security. Blockchain, as a distributed ledger technology, provides a trusted collaboration environment and a secure data management platform. The utilization of blockchain technology to drive IoT authentication has been a hotspot in academia and industry. This study analyzes the main requirements of authentication mechanism design based on cloud computing and cloud-edge collaboration and summarizes the challenges in applying blockchain technology to IoT scenarios. Relevant research on IoT authentication mechanisms is presented and classified into three categories of key-based authentication, certificate-based authentication, and identity-based authentication. Moreover, the existing IoT authentication studies using blockchain technology are analyzed, and related literature is reviewed according to authentication objects and additional attributes. This study also summarizes the security analysis method for the blockchain-based IoT authentication mechanism from formal and informal perspectives and finally points out the prospect of the technology.

Key words: Internet of Things (IoT); blockchain; identity authentication; multi-layer authentication; edge computing

随着物联网 (Internet of Things, IoT) 技术的飞速发展, 各类智能设备的数量正经历爆炸性增长, 根据 Juniper Research 的数据, 全球连接的 IoT 设备将从 2018 年的 210 亿台增长到 2023 年的 500 亿台[1].

* 基金项目: 浙江省重点研发项目 (2022C01145); 国家自然科学基金 (U20A20173, 62125206)
收稿时间: 2021-08-02; 修改时间: 2021-11-12; 采用时间: 2022-08-23; jos 在线出版时间: 2022-12-30
CNKI 网络首发时间: 2023-02-08

传统的 IoT 架构包含感知层、网络层和应用层, 其中感知层包含大规模的智能设备, 负责采集环境数据或物体状态信息, 然后通过网络层传输给云计算平台进行存储、管理与分析, 并将结果发送给应用层, 应用层是 IoT 与用户交互的接口, 为用户提供具体服务. 随着 IoT 技术被应用于越来越多的实际场景, 传统 IoT 架构的脆弱性和不安全性展露出来, 各个层次常见的攻击类型如表 1 所示. IoT 设备由于资源受限、自组织能力弱等缺陷选择将存储与计算任务外包给云服务提供商 (cloud service provider, CSP)[2], 但是基于云的中心化架构存在许多潜在的安全威胁. 首先, 中心化的云服务器容易受到单点攻击, 进而对整个系统造成难以恢复的损坏. 其次, 数据所有者 (data owner, DO) 将数据存储在云端, 失去了对 IoT 数据的实际掌控权, CSP 无需通知 DO 即可操纵存储数据, 因此存在窃取用户/设备隐私和篡改数据的风险[3]. 此外, 由于 IoT 设备的异构性、设备的频繁进退、设备间相互访问、设备部署环境的复杂性, 以及缺乏监督等因素, 导致 IoT 应用普遍缺乏安全性. 综上, 不论是从 IoT 架构和环境的角度还是设备自身特征的角度, 急需一套身份认证机制为保障 IoT 应用的安全性开启第一道防护.

表 1　传统物联网层次结构和常见攻击

层次	常见攻击类型
感知层	侧信道攻击、DoS攻击、女巫攻击
网络层	中间人攻击、网络监听、路由攻击
应用层	算法伪造攻击、注入攻击、重放攻击

传统的 IoT 认证方案大多使用基于公钥基础设施 (public key infrastructure, PKI) 的数字证书[4]. PKI 是建立在公私钥基础上实现安全传递信息和身份确认的一个通用框架, 包括认证机构 (certification authority, CA)、注册机构 (registration authority, RA) 和数据库 3 个核心组件. RA 对用户/设备身份进行验证, 校验数据合法性, 验证通过则将申请发送给 CA; CA 接受来自 RA 的请求, 负责证书的颁发和撤销; 数据库负责数据 (如密钥与用户信息等)、日志、统计信息的存储与管理. CA 收到数字证书申请后, 将申请者的公钥、身份信息、数字证书的有效期等信息作为消息原文进行哈希生成摘要, 并用 CA 的私钥生成签名, 数字签名与申请者的原文消息共同组成数字证书. 实体通信过程中, 验证方收到数字证书后, 使用 CA 公钥对数字签名进行解密生成消息摘要, 对消息原文计算哈希生成摘要, 将两份摘要进行比对即可验证证书内容的真实性和完整性, 进而实现对用户/设备的身份认证. 这实际上是一种基于中心化机构 (CA) 信用背书的方案, 使用 PKI 体系的传统认证机制显然面临 3 种缺点: 首先, CA 和数据库服务器作为中心化实体易受网络攻击; 其次, 证书生成操作完全依赖于 CA, 存在泄露用户隐私和生成虚假证书的风险. 最后, 基于 PKI 的认证体系引入高昂的证书管理成本, 包括证书状态检测、证书路径构建、证书撤销等.

区块链技术由于去中心化、防篡改、可追溯、安全透明、可编程等优势, 已被广泛应用于供应链、数字金融、智慧农业、物联网等领域[5]. 区块链系统基于分布式网络、密码学算法、共识机制、博弈论、智能合约等技术为分布式协作应用创造了一个去信任的网络平台, 并提供了一个用算法信用替代传统基于中心化机构作为信用背书的解决方案. 区块链的去中心化特性天生适配大规模、分布式的 IoT 场景, 因此许多工作将区块链技术应用到 IoT 场景中, 提出了去中心化的 IoT 管理架构[5]. 在 IoT 认证研究中, 融合区块链与其他密码学技术提出了取代基于 PKI 体系的传统认证机制的新方案, 并将终端设备的移动性、身份隐私保护、设备异构性、交互性等附加属性与不同 IoT 场景的特定认证需求 (比如跨域认证、实时认证等) 纳入研究范围, 从而设计出一些新型认证机制.

本文根据 IoT 场景的现实特征与 IoT 实体的特殊性质分析了 IoT 身份认证机制设计的主要需求, 并指出了将区块链技术应用于 IoT 场景面临的挑战和现有解决思路. 此外, 本文总结了有关 IoT 身份认证的工作, 从密钥使用的角度将其分为基于对称密钥和非对称密钥的认证、基于证书的认证和基于身份的认证. 根据区块链技术在 IoT 认证工作中的功能, 从数据账本、激励机制、合约平台 3 个方面对相关文献进行了梳理和分析, 并根据认证对象 (用户、设备) 和附加属性 (跨域认证、轻量级认证、匿名认证、多层认证) 对基于区块链技术的 IoT 认证工作进行了分类和归纳. 最后从形式化和非形式化两个角度对 IoT 认证机制的安全性分析方法进行了归纳, 为安全可靠

的 IoT 认证机制设计提供通用的安全性分析思路.

本文第 1 节介绍 IoT 身份认证机制设计的主要需求与将区块链技术应用于 IoT 场景面临的挑战. 第 2 节首先梳理了现有的 IoT 认证工作, 并进行了分类与对比, 其次回顾并总结运用了区块链技术的 IoT 认证工作. 第 3 节总结并归纳现有工作中针对 IoT 认证机制的安全性分析方法. 第 4 节对未来基于区块链的 IoT 身份认证问题进行了探讨和展望, 为进一步的研究做参考.

1 物联网认证需求与挑战

1.1 定 义

在海量、多维、异构的 IoT 环境下, 保障进入网络的设备和用户的身份合法性是维护 IoT 系统安全的首要前提. 身份认证结果是系统对是否允许用户/设备参与 IoT 事件交互以及是否授予数据请求者访问权限做出决策的主要依据. 根据认证目标的不同, 可以将现有认证工作分为 4 类: 对知识的认证 (是否知道某些信息), 对财产的认证 (是否是某种财产的所有者), 对身份的认证 (是否是使用特定服务或产品的合法实体) 和对消息的认证 (保障信息传输的完整性和安全性). 前两者通常用于两方或者更多方完成一项特定任务时的协作场景, 需要以知识或财产为认证媒介, 消息认证应用于实体交互过程中的完整性证明, 而身份认证则为非信任环境下的多方协作环境提供了安全前提. 本文主要考虑 IoT 身份认证. 根据认证对象的不同, 身份认证可以分为 3 类: 对进入网络请求数据的用户/设备的认证, 对 IoT 终端设备与边缘设备的认证, 以及对 CSP 和云服务器的认证.

1.2 认证需求

根据实际 IoT 场景的特征与 IoT 设备的特殊性质, 本文针对传统基于云计算的 IoT 架构与基于边缘计算的云-边-端新型 IoT 架构总结出认证机制设计的几点需求.

(1) 完整性: IoT 认证机制的完整性并非指传统网络安全中的数据完整性认证, 即保障数据在传输过程或存储阶段未被篡改, 请求者所获数据与原始数据一致[6], 而是指认证方案需要包含设备注册、密钥生成、认证、密钥协商、设备删除、状态更新等完整的工作周期, 各个阶段方案相互关联为 IoT 系统中的实体提供完整的认证流程.

(2) 安全性: 在缺乏人工监督的 IoT 环境中, 即使一台 IoT 设备已通过其他节点的身份验证, 由于执行任务期间的软件或系统漏洞, 仍然存在被恶意攻击的风险. 入侵者通常会通过修改网络实体, 在设备中留下后门, 为以后的系统渗透做准备. 还可能进一步修改设备中的密钥配置文件, 对整个网络造成严重破坏. 因此, 为了迅速发现潜在的入侵风险, 需要在认证阶段设计一套安全机制检测数据是否被篡改, 保障系统安全性.

(3) 交互性: IoT 技术的最终愿景是为了打破应用孤立导致的数据孤岛, 实现海量、异构、非信任实体间的数据共享, 以促进应用间的高效协作, 为用户提供快速、安全、低成本的 IoT 服务. 因此, IoT 实体间的交互是必不可少的. 交互认证是指相互通信/协作的实体双方需要在信息传递前验证彼此身份的合法性. 由于实体的异构性和状态差异导致交互认证存在一些挑战亟待解决.

基于云计算的 IoT 架构无法满足持续增长的 IoT 数据对安全隐私和可扩展性的需求, 很多学者将边缘计算作为对云计算的扩展引入 IoT 环境. 边缘计算作为一种新的计算模式, 将 CSP 的资源下沉到网络边缘, 实现针对 IoT 终端用户的本地化服务, 提供分布式、低延时、高带宽的优势, 大大提高了云服务的可扩展性[7]. 云计算擅长全局性、非实时、长周期的大数据处理与分析, 边缘计算更适用于局部性、实时、短周期的数据处理与分析. 在云边协同环境下, 边缘设备在接入网络时需要向云端完成身份认证并由云端为其部署部分服务, 而 IoT 用户/设备只需在边缘设备进行身份注册, 无需向云端发送认证请求. 因此云边协同应用于 IoT 场景形成了一个云-边-端一体化的新型 IoT 认证架构, 如图 1 所示. 显然, 适用于传统云计算的安全机制无法直接复用到新型认证架构中, 针对云-边-端新型 IoT 架构的身份认证机制增加了以下设计需求.

(4) 多层级: 云-边-端三层架构中涉及跨层交互, 即各个层级设备之间存在数据传输和通信协作. 如图 1 所示, 云服务器通过核心网将服务部署到边缘设备, 边缘设备对 IoT 数据实施预处理并将一些非实时、算力密集型任务

发送给云端处理, IoT 设备在边缘端进行注册并将感知数据直接发送给边缘设备. 因此, 为了保障跨层交互的安全性, 在基于云-边-端的 IoT 场景中, CSP、边缘设备与 IoT 终端设备在执行协作任务前需要执行多层级认证过程.

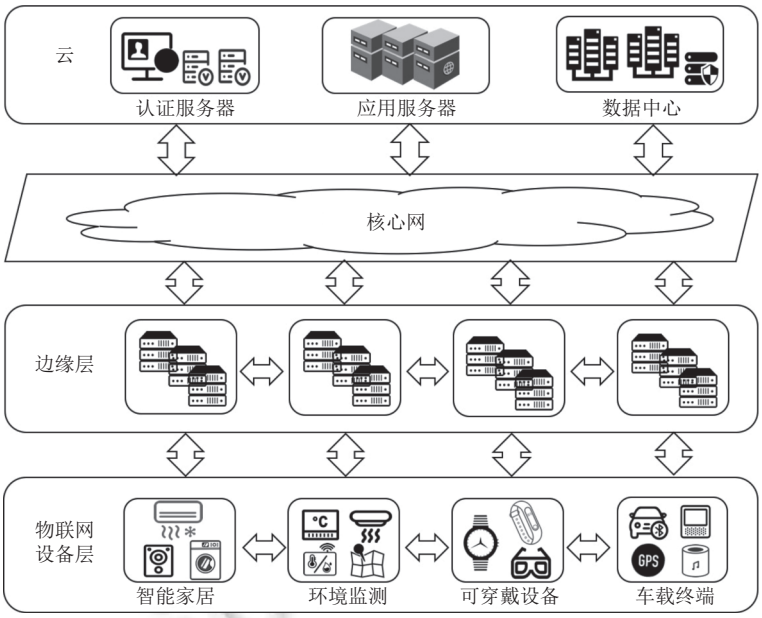

图 1 云-边-端新型物联网架构

(5) 跨域: 认证机制设计的跨域需求具体可分为 3 种情况, 首先是跨服务域: 由于每个边缘设备的覆盖范围以及部署的资源有限, 因此需要多个边缘设备进行跨域协作来为终端用户/设备提供实时完整的服务. 其次是跨设备域: 每个设备可能属于不同的设备制造商, 设备出厂前由设备制造商特定的公钥生成中心 (public key generator, PKG) 生成公私钥, 因此将异构设备集成到 IoT 系统中时会面临设备之间的公私钥体系无法兼容的窘境, 所以需要考虑设计统一的密钥生成机制以实现跨设备域的兼容认证. 最后是跨管理域: 实际 IoT 应用中一套完整的请求响应流程可能需要属于不同网络设备运营商的设备之间进行协作, 服务执行流程中负责不同环节的设备可能部署在不同的运营商管理范围内, 因此需要进行跨管理域认证以保障安全协作, 以实现完整的服务流程.

此外, IoT 身份认证受到 IoT 终端设备数量庞大、资源受限、延时敏感等特殊性质和用户服务体验的约束, 因此还需要考虑到以下设计需求.

(6) 隐私保护: 随着信息化社会的发展, 人们的隐私保护意识逐渐提升. 终端用户和设备在网络交互过程中对身份和数据的隐私保护需求需要在认证方案设计中纳入考虑范围. 正如前文所述, 中心化的实体机构存在篡改数据和窃取隐私的风险, 因此需要设计一套降低中心化实体依赖的隐私保护方案, 使得身份与数据信息始终处于安全状态. 目前很多工作正尝试将新兴的隐私计算技术比如安全多方计算[8], 全同态加密[9], 可信执行环境[10], 零知识证明[11−14]等应用于 IoT 场景以达到隐私保护的目的.

(7) 轻量实时: IoT 终端设备往往只承担数据采集及传输的工作, 不需要进行复杂的计算操作, 因此通常认为终端设备具有资源受限的特性. 因此所设计的认证方案需要尽可能实现轻量级, 适应终端设备算力不足的特点, 降低设备参与认证的资源门槛. 但是不能刻意追求轻量级而降低服务实时性和质量, 大多数 IoT 应用 (如自动驾驶、智慧医疗、交通预警等) 对服务实时性具有较高要求, 因为 IoT 数据存在生命有效期, 设备认证、数据处理、信息传输等导致的响应延时将导致应用决策滞缓, 影响用户服务体验和服务质量.

(8) 可扩展性: 最后, 需要将认证方案的可扩展性纳入考量. 随着 IoT 设备数量的持续增长, 可扩展性成为设计身份认证方案必不可少的考虑因素, 以满足海量异构设备同时申请认证的情况, 谨防由于认证机制的复杂性导致带宽不足、流量拥挤等问题, 进而影响 IoT 服务的可用性. 此外, 无论是边缘设备还是 IoT 终端设备都可能频繁加

入和退出网络, 因此需要实时更新各层级设备的认证状态列表, 并保证分布式情形下所有节点所维护的认证列表的一致性.

1.3 挑 战

首先简要介绍区块链技术架构, 然后针对第 1.2 节所提出的 IoT 身份认证需求, 总结了 4 点将区块链技术应用于 IoT 应用的工作中面临的技术挑战以及对应的解决思路.

区块链的技术架构如图 2 所示, 自底向上分为数据层、网络层、共识层、激励层、合约层和应用层[15]. 其中数据层封装了底层数据的存储方式、区块结构以及哈希算法、非对称加密等密码学技术, 实现了分布式账本可追溯、不可篡改的技术支持; 网络层建立在 IP 通信协议与点对点 (peer-to-peer, P2P) 网络基础上, 包括组网机制、数据传播机制和验证机制; 共识层封装了网络节点的各类共识算法, 用于选出记账节点并维护账本的一致性; 激励层集成了基于加密货币的经济激励, 在公有链中使用; 合约层封装了各类脚本和算法, 是区块链可编程特性的来源, 智能合约部署在数据层的区块中; 应用层封装了基于区块链技术的各种实际应用场景, 从技术架构角度可以将应用分为 3 类: 第一是基于智能合约技术将复杂业务规则转化为自动执行的代码的业务平台[16−18], 其次是基于区块链经济激励为多方协作应用构建激励机制, 以激励各方诚实主动地参与任务协作[19]; 第三是基于区块链账本去中心化、防篡改、可追溯、公开透明的特性为应用构建可信的数据管理平台[20−22].

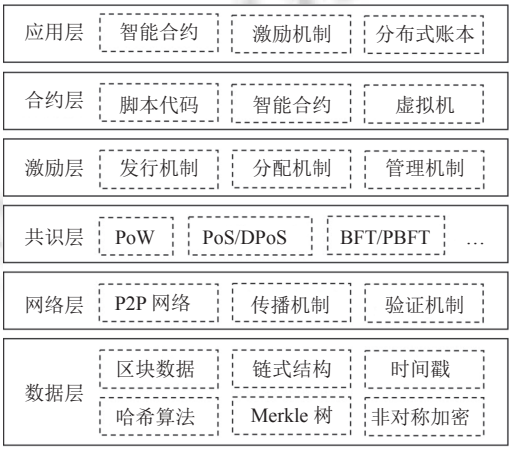

图 2 区块链技术架构

很多现有工作将区块链技术运用于 IoT 应用为访问控制[16]、数据存储[19]、数据完整性认证[22]等问题提出了许多优秀的解决方案, 但是由于区块链技术的瓶颈与 IoT 应用的固有特征, 导致基于区块链技术的 IoT 解决方案依旧面临一些现实的挑战. 本文总结了下述 4 点挑战并归纳了对应挑战的现有解决方案.

(1) 区块链网络依靠共识机制来记录交易并保证状态一致性, 运行共识算法需要网络节点消耗大量算力资源, 但是算力资源的积聚保障了共识算法的安全性[23]. 此外, 由于 IoT 设备在持续不断地采集数据, 随着时间的推移区块链账本数据不断增长, 存储空间受限的 IoT 节点将无法保存完整的区块链副本, 以至于无法参与区块链的维护, 从而导致区块链网络去中心化程度和安全性的降低, 失去了使用区块链技术的优势. 因此, 在将区块链技术运用到 IoT 认证工作时需要首先解决 IoT 设备资源不足无法运行区块链节点的问题. 针对这一挑战, 目前有 4 种解决思路: 1) 首先是设计轻量级的共识机制, 以适配算力受限的 IoT 设备. 传统区块链共识算法要求节点计算无意义的哈希函数, 此过程造成大量资源浪费, 同时不利于在资源受限场景部署区块链. 因此, 许多专家和学者对传统区块链共识算法进行优化, 提出了许多轻量级共识算法, 但是这类优化方案要么降低了系统去中心化程度, 要么引入了复杂的关系依赖[24]; 2) 设计轻量级账本存储方案, 以有效解决 IoT 数据不断增长带来的问题. 这种方案可以概括为数据卸载[25]、区块压缩[26]、分片技术[27]、本地交易[28]这 4 种路线. 数据卸载即通过删除“无用”的历史交易数据的方法来缓解节点的存储压力. 区块压缩即通过与共识机制有机结合, 将历史区块数据进行压缩处理, 充分提高

节点存储空间利用率. 这两种方案都会破坏账本数据完整性并且增加了区块处理时延. 分片技术即利用分片思想将区块链网络分割为许多更小的网络分片, 每个网络分片只需要运行更小范围的共识, 处理更少的交易和存储更少的账本数据, 但是单个分片的安全性和抵御攻击的能力较差. 本地交易是使得连接到同一节点的设备产生的交易仅存储在该节点内, 通过这种本地交易的形式能够有效降低区块链账本的增长速度, 进而缓解节点的存储压力. 但这种方案依赖于特定的系统框架, 无法作为通用的解决思路; 3) 将 IoT 设备作为区块链轻节点, 无需运行共识和参与验证, 只需要同步区块头数据. 这种方案由额外部署的具备较强资源的设备担任区块链维护节点, 负责共识机制运行、区块生成和验证, 但是大大提高了 IoT 系统配置成本; 4) 将感知层 IoT 设备的上层设备 (如网关、边缘服务器等) 作为区块链节点. 感知层设备不参与或间接参与维护区块链网络, 与上层设备通过链下安全信道进行数据交互和互操作.

(2) 为了应对大规模 IoT 设备持续输出数据流的情形, 系统的并发性需要得到保障. 因此将区块链应用于 IoT 认证工作时需要满足 IoT 应用高吞吐量的需求. 然而, 为了保障系统安全性, 区块链系统不得不牺牲部分性能运行共识机制. 为了满足产业区块链需求, 目前有一些工作已经在尝试设计实现高吞吐量的 l 联盟区块链平台作为性能不足的解决方案[29,30]. 高性能联盟区块链的设计角度主要包括以下 3 个方面[31]: 1) 业务逻辑和共识分离. 如果将交易执行任务交由外部业务系统完成, 区块链网络只负责交易排序和合法性验证, 那么系统的吞吐量则可以有很大的提升; 2) 存储优化. 使用链上链下相结合的存储方式, 减小链上存储压力和读写频率, 进而提高交易处理性能; 3) 数字签名验证优化. 主要包括多交易打包签名和基于 GPU 和 FPGA 加速两种思路. 虽然上述方案可以提升基于区块链的 IoT 系统性能, 但是距离大规模 IoT 应用对高并发性的需求还具有一定差距.

(3) 区块链网络中的交易内容公开透明, 网络节点可以很轻松地查阅并验证交易信息. 虽然区块链使用非对称加密技术将交易的发送方与接收方地址进行了匿名化隐藏, 但是依旧存在通过交易分析窃取身份隐私的风险, 攻击者还可以通过线下定位的方式将交易信息与实际对象对应起来[32], 使得用户身份隐私与数据隐私面临严重泄露的风险. 显然这与 IoT 应用对于隐私保护的需求相违背. 目前研究者们提出了一系列区块链隐私保护技术来抵抗账本信息隐私泄露攻击, 现有的隐私保护技术可以归纳为地址混淆、信息隐藏、通道隔离 3 大类[33]. 账本分析技术假设同一交易的所有输入地址属于同一用户, 研究者针对该假设提出一种交换资产、混淆地址的攻击防御机制, 即地址混淆机制. 通过将不同用户的资产互相交换, 达到混淆不同用户地址的效果, 这样攻击者会将不同用户的账户地址误认为属于同一用户, 进而达到保护隐私的目的[34]. 虽然地址混淆机制能够在一定程度上保护账本隐私, 但是混淆的结果仍会在公开账本中存储, 攻击者可以通过分析带有特征的混淆交易来推断用户隐私. 为了增强隐私性, 研究者们尝试基于零知识证明、环签名、同态加密等密码学算法将交易发起者、接受者、交易金额等账本信息进行加密隐藏[35]. 但是这种方案提升了链上操作的复杂度和节点维护成本. 通道隔离机制是从网络层面对账本数据进行隔离, 实现数据只对通道内节点可见[36]. 通过对账本进行隔离, 每个节点只处理并存储自己所在通道的数据, 防止攻击者访问数据, 进而保护用户隐私. 但是区块链网络中通道部署成本高昂, 节点创建和通道进出需要进行额外的网络配置, 缺乏灵活性和动态性.

(4) 将区块链技术融合到 IoT 认证场景中, 应用中的 IoT 设备数量越多, 每个区块链节点的工作负载越大[37]. 因为每个节点都在生成和验证交易, 意味着随着节点数量增多, 每个节点要验证的交易数量越多以及维护的交易账本容量越大. 但是, 节点数量的增多意味着更多的算力投入区块链网络, 有利于系统的安全性保障. 因此需要在不削弱 IoT 系统安全性的前提下设计轻量级区块链的解决方案. 当前的轻量级区块链应用架构可以划分为以下 3 种类型: 1) IoT 设备以全节点身份参与区块链网络. 这类架构不需要额外部署其他资源强大的设备, 通过研究轻量级的共识算法与数据存储方案使得资源受限的 IoT 设备以全节点的身份参与共识、执行数据存储、交易验证的工作. 但是这种方案使得 IoT 设备承担了除采集、处理和交换数据等核心任务之外的工作负担, 影响了 IoT 系统的工作效率; 2) IoT 设备以轻节点身份参与区块链网络. 这种方案通过额外部署其他资源强大的设备充当全节点维护区块链, 而资源受限的 IoT 设备以轻节点的身份参与区块链, 不需要存储完整的区块链账本[38]. 但是额外部署的区块链节点需要向第三方信任机构进行身份认证, 导致区块链网络的去中心化程度降低; 3) IoT 设备同时以轻节点和全节点身份参与区块链网络[39]. 这种方案充分考虑了 IoT 的分层结构 (如表 1 所示), 将资源受限的感知层

设备作为轻节点, 考虑到 IoT 网络层和应用层的设备具有一定的计算和存储能力, 因此可以选择轻量级的共识算法以及数据存储方式, 使得这两层的 IoT 设备以全节点的身份维护区块链网络. 这种根据 IoT 架构中各层设备特征与区块链网络有机结合形成的轻量级架构有效解决了资源受限的 IoT 设备无法满足高工作负载的问题, 但是目前缺乏实际可验证的系统.

2 研究进展与比较分析

目前学术界针对 IoT 身份认证已经提出了很多解决方案, 这部分首先将现有的 IoT 身份认证方案进行了总结和分类, 然后对比分析了区块链技术在 IoT 认证工作中的应用, 并根据认证对象以及认证属性对相关文献进行了梳理和总结.

身份认证大致分为两类: 一类基于生物特征认证, 另一类基于密码学算法支持. 前者利用用户的指纹、虹膜、声音等生物特征和行走姿势、步态等行为特征作为标识进行身份认证[40], 这些标识不易丢失且难以复制, 使认证系统克服了密钥管理的难度, 但是需要提前采集生物特征信息, 需要用户实时参与, 此外无法适用于传感器等硬件设备的认证; 后者使用基于密码学的数学方法设计认证协议, 使用密码学算法验证用户身份的合法性. 常见的密码学技术有基于对称加密算法的消息认证码 (message authentication code, MAC), 基于非对称加密算法的数字签名和群签名、环签名等技术. 由于基于生物特征的身份认证需要借助于特定的硬件, 增加了认证成本, 且无法满足大规模并行认证的需求, 因此本文主要考虑基于密码学算法的认证方案. 目前的认证方案从密钥使用的角度可以分为 3 类, 分别是基于对称密钥与非对称密钥的认证机制, 基于证书的认证机制和基于身份的认证机制.

2.1 基于对称密钥和非对称密钥的认证机制

对称加密使用相同的密钥进行加解密操作, 该算法的优点是加解密效率和加密强度都很高, 但是参与方需要提前持有密钥, 因此需要在认证前设计一个密钥分发机制, 通常由一个密钥分发中心 (key distribution center) 来实现. MAC 是基于对称密钥的认证机制中最常用的技术. Bellare 等人[41]提出了两种相关的 MAC 方案, 分别称为嵌套结构 MAC (nested construction MAC, NMAC) 和基于哈希的 MAC (hash-based MAC, HMAC), HMAC 可以与任何迭代加密哈希函数一起使用[42]. 但是基于 MAC 技术的认证方案由于缺乏可扩展性, 无法适用于部署了大规模设备的环境. 因此, MAC 认证技术更适用于相对小规模的 IoT 应用[4].

基于非对称加密的认证机制具有良好的可伸缩性. 它依赖于以下事实: 密钥是成对创建的, 并且由私钥 (公钥) 加密的数据只能由相应的公钥 (私钥) 解密. 公钥可以在不安全的通道中传输, 而私钥则秘密地保存在所有者一方. 基于非对称加密和哈希算法创建的数字签名技术被广泛运用于 IoT 认证, Alizai 等人[43]为 IoT 设备认证提出了一种将数字签名和设备能力相结合的多因素认证机制, Mughal 等人[44]提出了一种轻量级的数字签名算法同时满足系统安全性需求和设备资源限制. 除普通的数字签名应用场景外, 针对一些特定的安全需求, 产生了一些特殊数字签名技术, 包括盲签名、多重签名、群签名、环签名等. 数字签名算法的安全性基于非对称加密的数学问题的求解复杂性, 在数字签名算法构建过程中需要选取合适的随机数作为配置参数, 配置参数不合理的使用或泄露都会造成安全风险, 因此需要从服务体验的角度降低认证方案复杂度.

2.2 基于证书的认证机制

基于证书的认证机制借助于 PKI 体系, 由 CA 为设备的公钥进行签名, 使得系统内的其他设备都可以使用 CA 的公钥对该证书进行合法性验证, 验证成功则认可该证书中所提供的设备公钥. Porambage 等人[45]为无线传感网络提出了一个基于证书的两阶段认证机制, 加密证书存储在边缘节点中, 使得机制面临克隆攻击的风险. Sciancalepore 等人[46]为工业物联网 (industrial Internet of Things, IIoT) 系统使用椭圆曲线 Qu-Vanstone 隐式证书和椭圆曲线 Diffie-Hellman 技术设计了一个密钥管理协议, 提供节点认证和密钥协商. Moosavi 等人[47]使用基于证书的数据包传输安全协议 (datagram transport level security, DTLS) 为基于 IoT 的医疗系统开发了一套认证和授权架构.

除此之外还有很多基于证书的 IoT 认证方案[48−50], 这类方案一方面引入了证书管理和验证的高昂成本, 另一方面对中心化实体 CA 施加了安全可信的强假设. 然而在现实场景中, CA 极易受到潜在攻击并易于发生操作错误[51].

2.3 基于身份的认证机制

基于身份的认证机制是利用身份基加密技术 (identity-based cryptography, IBC)[52], 核心是使用用户和设备具有唯一性和抗否认性的身份信息 (例如用户的邮件地址、身份证号、电话号码等) 计算出公钥, 而不需要第三方机构保障公钥的真实性, 从而降低了系统的证书管理成本和对中心化机构的依赖. Heo 等人[53]为电力线通信提出了一种基于 IBC 的设备相互认证方案, 由于不需要使用公钥证书, 因此降低了认证证书部署和管理的复杂度. Li 等人[54]提出一种基于 IBC 的云计算认证方案, 但是只考虑了云服务器与设备使用者之间的认证, 设备与设备间的认证没有涉及. 林俊燕等人[55]提出了一种基于 IBC 的无线传感器网络认证加密方案, 通过 IBC 密钥加密对称密钥实现密钥安全分发, 进而实现 IoT 数据的加密传输. 虽然目前已经存在将 IBC 运用于 IoT 认证的大量尝试, 但是 IBC 技术依旧存在潜在的安全风险: 通常用户私钥是由密钥生成中心 (key generation center, KGC) 计算得出, 意味着 KGC 拥有所有用户的公私钥信息, 因此认证方案的可信度依赖于 KGC 的可靠性, 恶意的 KGC 可以轻松窃取私钥信息施加攻击. 基于此, 演化出了无证书加密 (certificateless cryptography) 技术, KGC 根据 IoT 用户/设备身份为其生成部分私钥, 用户/设备使用秘密值和部分私钥生成实际私钥[56].

2.4 区块链技术在认证方案中的应用

区块链技术的引入并不是为了给 IoT 应用提供新的认证方案, 而是基于分布式账本去中心化、防篡改、可追溯的优势和智能合约可编程的特性结合上述 3 类基于密码学的认证方案为 IoT 认证提供安全可信的运行环境和管理平台. 本文通过调研现有使用区块链技术的 IoT 认证工作, 将区块链技术在其中的功能按图 2 所示区块链的技术架构进行了分类, 主要包含 3 类, 分别称为数据账本、激励机制、合约平台.

(1) 数据账本

区块链本质上是一个分布式账本, 网络节点通过“挖矿”实现对交易的记账过程, 维护网络的正常运行. 以比特币网络[57]为例, 一个区块包含 6 个字段, 如图 3 所示, 分别是前一个区块的哈希, 用以将区块链接起来; 版本号, 表示本区块遵守的验证规则; 时间戳, 表示当前区块生成的时间; 难度值, 表示当前目标哈希值; 随机数是矿工计算出的值; Merkle 根是储存了所有交易的 Merkle 树的根哈希. 区块体是基于 Merkle 树实现的交易存储结构, 实现了交易的快速验证以及防篡改. 用户发起一笔交易并广播到网络中, 然后全网节点接收并验证交易, 交易被打包至节点本地区块中, 全网共识结束后, 获胜节点将其本地区块追加到主链. 比特币采用工作量证明 (proof of work, PoW) 共识算法, 核心是通过引入分布式节点的算力竞争来保证链上数据的一致性.

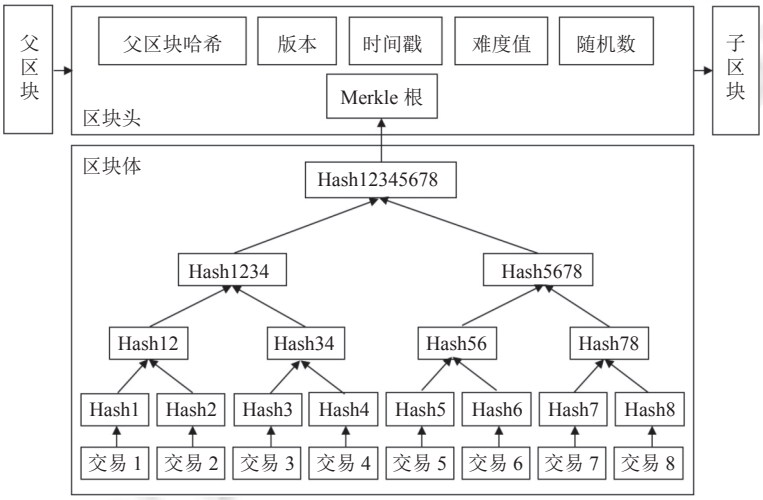

图 3 区块结构

目前许多工作通过修改区块和交易的结构将区块链作为分布式数据账本存储 IoT 认证流程中的交互信息以及关键数据例如密钥和证书, 以获得防篡改、安全隐私等特性. Li 等人[58]使用区块链和无证书加密算法提出了一

个去中心化的 IoT 数据存储和设备认证方案, 将 IoT 设备对数据存储和数据访问的服务请求作为交易记录在链上, 比如一个医疗传感器 A 想将数据存储在分布式哈希表的 Addr 位置, 交易将被写成以下格式: T=(IDA, Timestamp, Action = store data in Addr). Cui 等人[59]将 IoT 节点按资源情况分为基站、簇头和普通节点, 然后设计了一个本地-公共的混合区块链架构, 本地链负责对普通节点的身份认证, 公共链负责对簇头节点的身份认证, 对注册和认证阶段的交易信息进行了格式化定义, 将节点的身份信息存储到链上. Li 等人[60]将设备 ID、公钥和其他关键数据的哈希值存储到区块链上, 进入网络的设备首先通过链上存储的注册信息进行认证, 认证通过后再计算设备的关键信息的哈希值与链上数据进行对比, 以检测潜在的安全威胁. 文中将设备注册、身份认证和完整性验证相关的请求和响应信息作为交易内容. Wu 等人[61]将区块链技术用于 IoT 设备认证, 提出了一个双因素认证方案. 其中区块链存储每个认证实体的关系信息, 即在带外通道中充当认证实体身份验证器的相关设备, 此外还为验证结果提供存储. Kaur 等人[62]结合区块链与椭圆曲线加密 (elliptic curve cryptography) 为车联网提出了一个轻量级的跨数据中心认证方案, 其中区块链账本用来存储和维护网络状态信息. 类似地, Yao 等人[63]提出了一种基于区块链的轻量级匿名身份验证机制, 用于分布式车联网服务. 他们的重点是使用区块链和加密算法实现跨数据中心的身份验证. Hammi 等人[64]使用以太坊平台创建了一个去中心化的 IoT 设备认证机制, 数据以交易的形式在实体间进行传递, 保障了安全性与完整性. Yazdinejad 等人[65]在 5G 场景下提出了一种新的身份验证方法, 利用区块链和软件定义网络 (software defined networking, SDN) 技术来消除在异构单元间的切换中不必要的重新验证. 其中区块链实现了设备注册、密钥生成、认证和恶意行为监测等功能. Yazdinejad 等人在[66]中基于区块链账本在分布式医疗网络中为病患实现了一个去中心化的认证系统, 他们更改了传统区块链中的交易结构, 包含病患的身份信息和相关医疗数据, 通过区块链实现病患的注册、认证和信息共享. Lin 等人[67]集成了区块链和群签名技术在智能家居场景下提出了一种匿名认证方案, 所有来自群成员的请求信息都会被记录在链上, 进而提供可靠的行为审核. 针对 IoT 环境下雾计算架构的安全隐私问题, Mounnan 等人[68]基于区块链技术在 IoT 环境下为雾计算实现了一个访问控制方案, 其中区块链用于存储和部署数据所有者定义的访问策略, 控制用户访问相应 IoT 设备, 此外还负责所有注册、认证和访问控制操作. Zhang 等人[69]设计了一个基于区块链的分布式用户认证方案, 用户将身份信息存储在链上, 加密其他私人信息并存储到链下, 用户登录网站或应用时, 区块链提供对应的认证信息.

(2) 激励机制

区块链的激励层主要包括经济激励的发行制度和分配制度, 其功能是提供激励措施, 鼓励节点参与区块链中的安全验证工作, 并将经济因素纳入到区块链技术体系中, 激励遵守规则参与记账的节点并惩罚不遵守规则的节点[15]. 例如比特币网络会给诚实的矿工支付打包区块的奖励以及交易费, 激励矿工诚实地参与交易记账. 需要注意的是, 区块链中的激励行为是去中心化的, 在网络创建初期就设定好了激励运行和维护机制, 全网节点都是机制的参与者和监督者. 此外, 区块链的激励行为公开透明, 每一笔奖励都可以溯源.

目前许多工作基于区块链为认证实体设计激励机制, 刺激分布式实体更积极地参与安全认证流程. Alghamdi 等人[70]针对轻量级 IoT 用户基于区块链技术提出了一种安全的服务供应方案, 使用运行权威共识 (proof of authority, PoA) 的联盟链平台, 根据服务提供商的信用提出了一种激励机制, 鼓励服务提供商提供更精确的服务. Lin 等人[71]提出了一个分布式的 IoT 知识交易市场, 开发了一条联盟链用于维护市场的知识管理和交易, 设计了一种新的加密货币“知识币”, 还提出了一种基于非合作博弈的知识定价策略以及对市场的激励机制. 作者在同样的研究场景下通过构建两阶段的 Stackleberg 博弈模型, 提出了一个能源知识交易激励机制, 并提出了最优的经济激励和动力传递策略[72]. Wu 等人[73]提出了一种区块链驱动的 IoT 激励平台, 称为 SmartRetro, 可以激励和吸引更多的分布式探测器参与系统漏洞检测并提交检测结果, 利用智能合约, SmartRetro 的消费者可以收到有关其已安装 IoT 系统的自动安全反馈, 激励会通过合约实现自动分配, 无需中心化机构参与. Wang 等人[74]基于区块链平台为群智感知应用提出了一种保护隐私的激励机制, 利用区块链中的加密货币作为奖励, 矿工通过感知数据的评估标准来验证交易, 高质量数据的贡献者将获得代币奖励. 类似地, He 等人[75]为分布式 P2P 应用提出了一种基于区块链的激励机制, 该机制使用诸如比特币的加密货币来激励用户进行合作. 由于区块链系统中的用户和矿工可能相互勾结, 作者又提出了一种安全定价策略, 并将其整合到区块链激励机制中. Jia 等人[76]在群智感知网络中基于

区块链提出了一种将隐私保护和虚拟积分相结合的混合激励机制, 矿工将用户信息存储到链上并获得相应的虚拟货币奖励.

(3) 合约平台

智能合约是区块链可编程特性的基础[77], 广义上讲, 智能合约就是使用特定编程语言编码的一组规则, 一旦满足触发响应条件, 区块链系统便会自动执行合约脚本实现相应操作, 无需第三方机构参与. 智能合约一旦编写好部署到区块中便无法修改, 因此满足了区块链的不可篡改性. 因此, 智能合约为区块链提供了一种可编程模式, 将实际应用场景中的实体交互规则和复杂交易流程以合约形式部署在链上, 按照既定规则自动执行, 维护系统的数据安全和稳定运转.

目前一些工作基于智能合约的可编程特性和自治性, 将认证机制的交互流程以合约的形式实现并部署到区块链上, 为认证机制构建安全可信的运行环境. 在 Cui 等人[59]提出的混合区块链模型中, 由基站将智能合约部署到公共链来实现对簇头节点的注册与认证, 然后簇节点将智能合约部署在各自的本地链上以验证普通节点的注册并响应认证请求. Li 等人[60]通过智能合约从设备端接收服务请求, 然后根据具体请求类型在区块链中执行设备注册、身份认证和完整性验证操作. Almadhoun 等人[78]融合基于区块链技术的雾计算架构提出了一种 IoT 用户身份验证方案, 其中雾计算节点与以太坊智能合约对接, 对访问 IoT 设备的用户进行身份验证. 合约中包含各个雾节点与其所管理的 IoT 设备的映射以及设备允许访问的用户列表, 通过智能合约控制注册、认证和访问控制功能. Wu 等人[61]基于商业区块链 Eris 系统实现了 IoT 设备认证的原型, 包含两类智能合约, 分别是设备合约和关系合约, 设备合约存储设备信息, 关系合约存储关联设备的配对关系. 相关设备通过调用合约将认证实体的认证结果存储到链上. Hammi 等人[64]通过部署智能合约实现同一个虚拟区域内部的 IoT 设备之间的认证. 在 Lin 等人[67]提出的匿名认证方案中, 智能合约被用来记录来自用户的请求和网关的响应, 以提供可信的节点行为审计功能. 在 Mounnan 等人[68]提出的认证方案中, 通过智能合约检测用户的属性是否满足区块链上存储的访问结构, 检测成功则向用户授予访问令牌, 用户通过访问令牌联系管理此 IoT 设备的雾节点进行进一步认证. Zhang 等人[69]基于智能合约为每个用户授权可访问其线下存储信息的网站/应用, 当用户登录网站/应用时, 服务提供商首先对用户进行身份认证, 然后通过智能合约验证是否具有获取用户私人信息的权限. Chen 等人[79]在 WiFi 网络中提出了一种基于智能合约的位置感知身份验证方案, 设计了 3 类智能合约, 分别负责在注册阶段保障密钥的机密性和设备信息的安全性; 确保身份信息查询, 公钥查询和聚合签名验证在身份验证阶段正确执行; 并保障当存储空间不足时, IoT 设备依旧可以正确响应.

(4) 梳理总结

根据上述调研我们可以总结出 4 点结论: 首先, 完全基于区块链技术的 IoT 认证工作将用户/设备的身份信息或其他关键信息在认证阶段直接存储或先进行哈希再将哈希值存储在链上, 在用户申请访问数据时查询区块链进行信息验证, 思路简洁但是缺乏安全保障, 因此基于区块链技术的 IoT 认证工作通常都会与特定密码学算法结合; 其次, 通过修改交易结构将 IoT 数据存储在区块链账本中的工作通常都会进一步部署智能合约实现实体的注册、认证与监管等功能, 以维护分布式账本的方式实现去中心化的认证; 此外, 基于区块链设计的 IoT 激励机制可大致分为两类, 一类是将系统中的加密货币作为奖励, 通过运行共识机制来分配奖励, 第 2 类则借助于附加的经济学模型 (如 Stackleberg Game[72]), 将激励模型通过智能合约部署到区块链网络中; 最后, 在基于区块链技术的 IoT 认证工作中通常会附加一些认证属性, 例如跨域认证、轻量级认证和匿名认证等, 以适应实际的 IoT 场景特征与认证实体的特殊性质. 我们根据认证对象 (设备和用户) 的不同和 4 类附加认证属性 (跨域认证、轻量级认证、匿名认证和多层认证), 将近些年基于区块链的 IoT 认证工作进行了梳理[4,58–70,78,80–118], 如表 2 所示.

观察表 2 可以发现两个主要问题: 首先, 大多数现有基于区块链的 IoT 认证工作都是面向网络设备的认证, 包括采集数据的设备、存储设备、通信设备、访问设备等, 而面向用户的认证工作较少, 但是部分工作会将终端用户与设备视为相同概念[89–91]. 然而现实 IoT 场景中应该将数据所有者、服务提供商、访问用户等用户实体与各层级的设备区分开, 对进入网络的设备与用户都需要进行认证操作. 其次, 在附加属性认证中, 很多工作考虑到了跨域认证、轻量级认证和匿名认证, 但极少数工作会考虑多层认证, 现有工作[59,67,86,88,112]大多考虑终端设备与下一跳

节点 (例如集线器节点[112]) 之间的相互认证, 而忽视了云-边-端一体化架构下的多层次认证, 例如云服务器与边缘设备、边缘设备与 IoT 设备, 以及每层级设备与设备之间的相互认证. 此外, 部分工作同时将多个属性作为认证方案设计的约束条件以满足复杂 IoT 场景的需求[62,63], 为第 1.2 节提出的多认证需求融合设计做出了尝试.

表 2 基于区块链的物联网认证工作分类

工作	分类	相关文献
认证对象	用户	[66,67,69,70,78,80,88,91–94,101,106,108,111,112,116]
	设备	[4,58,60–65,67–91,95–105,107,109,110,113–115,117,118]
附加属性认证	跨域认证	[4,59,62,63,65,66,80–94]
	轻量级认证	[62,63,70,95–104,112]
	匿名认证	[4,63,67,88,105–117]
	多层认证	[59,67,86,88,112]

3 基于区块链的物联网认证机制安全性分析

区块链依托内生的分布式、防篡改、可追溯和智能合约等特性为 IoT 认证提供了安全可信的运行环境和管理平台, 如第 2.4 节所述, 研究人员针对不同认证对象和场景提出了众多基于区块链的 IoT 认证方案. 安全性分析是判断和验证所设计的认证机制是否具备正确性、有效性、安全性和可靠性的必不可少的重要途径. 如表 3 所示, 本文将现有针对基于区块链的 IoT 认证机制的安全性分析方法抽象为形式化和非形式化两个方向, 并进行了详细总结, 为 IoT 认证机制归纳出通用的安全性分析策略.

表 3 安全性分析方法

方法分类	分析技术	模型内容
形式化分析	模态逻辑技术	BAN逻辑, GNY逻辑, AT逻辑, SVO逻辑等
	模态检测技术	Dolev-Yao模型, 通讯顺序进程方法等
	定理证明技术	Paulson归纳法, Schneider阶函数, 串空间等
非形式化分析	CIAAN模型分析	Confidentiality, Integrity, Availability, Authentication/Authorization, Non-repudiation
	STRIDE模型分析	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
	典型攻击防御分析	女巫攻击, 重放攻击, 中间人攻击, DDoS攻击, 单点故障, 隐私泄露攻击等

3.1 形式化分析

安全协议的形式化分析是采用一种标准的方法实施分析, 以验证安全协议是否满足安全目标或存在某些安全漏洞[119]. 由于 IoT 认证机制是由非信任的多方参与协作, 因此协议可能存在人工无法识别的安全问题. 形式化分析通过数学模型更准确地定义 IoT 认证机制的特性和约束. 目前的形式化分析工作主要是基于模态逻辑、模态检测和定理证明 3 种理论技术体系展开的[120].

(1) 模态逻辑技术

模态逻辑技术通过对通信双方的交互信息进行分析, 利用一系列的公理和假设展开逻辑推理, 进而判断安全协议是否存在设计漏洞. 推理过程大致可以分为以下 4 步: 首先, 将 IoT 认证过程进行形式化描述; 其次, 设置 IoT 认证机制的初始化假设; 再次, 对认证协议的目标进行形式化描述; 最后, 使用形式化逻辑根据假设和认证协议流程进行推导, 分析各个主体最终产生的知识, 由此判断认证协议是否满足设定的安全目标. 基于模态逻辑技术的形式化分析方法主要包含 BAN 逻辑[121]、GNY 逻辑[122]、AT 逻辑[123]、SVO 逻辑[124]等.

(2) 模态检测技术

模型检测技术为安全协议定义状态集和状态迁移函数, 通过显式状态搜索或者隐式不动点计算验证系统性

质. 模型检测技术一般会为协议定义安全属性, 然后通过分析该安全属性是否得到满足来判断认证机制的有效性. 基于模态检测技术的形式化分析方法主要包括 Dolev-Yao 模型[125]、通讯顺序进程方法[126]等. 由于其具备高度自动化、可以针对漏洞生成攻击实例, 并且能定位问题存在的位置等特点, 模型检测技术被广泛应用于 IoT 认证协议的形式化安全性分析. 此外, 模型检测技术也被用于设计安全协议的形式化分析工具, 比如 AVISPA[127]. 众多基于区块链的 IoT 认证工作使用 AVISPA 作为检测安全漏洞的可靠工具[62,98,128].

(3) 定理证明技术

定理证明技术将安全协议描述为一个公理系统, 将协议的安全目标表述为公理系统中需要证明的定理, 进而将 IoT 认证机制是否符合安全目标的问题转化为论证公理系统中的定理是否成立[120]. 基于定理证明技术的形式化分析方法主要包括 Paulson 归纳法[129]、Schneider 阶函数[130]、串空间模型[131]等.

3.2 非形式化分析

非形式化分析指通过分析是否满足特定特性或者是否可以有效预防典型攻击来验证认证机制的有效性和可靠性. 当前基于区块链的 IoT 认证工作中常用的非形式化分析方法可以总结为 CIAAN (Confidentiality, Integrity, Availability, Authentication/Authorization, Non-repudiation) 模型分析[59,78,80], STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) 模型分析[132]和典型攻击防御分析[59,86,98,105]这 3 种.

(1) CIAAN 模型分析

CIAAN 分别表示 5 种用于验证认证机制是否满足的特性. 其中 Confidentiality 表示认证过程中交互数据的机密性, 一个有效的认证机制应该满足认证过程中的数据无法被非法用户获取. Integrity 表示交互数据的完整性, 即认证过程中应当保障数据不能被非法篡改, 通常使用哈希算法实现这一目标. Availability 表示服务和数据对于合法用户总是可获取的, 因此系统需要有效防止 DDoS 攻击、女巫攻击等网络攻击. Authentication/Authorization 用于认证用户身份的真实性和合法性, 以判断其是否具备访问数据和服务的权限. 这是认证机制要求具备的最基本的特性. Non-repudiation 是指用户无法否认其执行过的操作, 在区块链中使用数字签名签署交易来保障这个需求.

(2) STRIDE 模型分析

STRIDE 模型是微软基于 CIAAN 提出的一个威胁模型, 广泛应用于对安全协议和系统潜在安全风险的分析. STRIDE 模型主要总结了 6 类安全风险. 其中 spoofing 表示伪装成系统中的合法设备来建立通信, 对应于 CIAAN 中的“Authentication”目标. Tampering 表示对公共消息和通信数据进行非法篡改, 对应于 CIAAN 中的“Integrity”目标. Repudiation 表示否认曾经的行为, 对应于 CIAAN 中的“Non-repudiation”目标. Information disclosure 表示将信息泄露给非授权实体, 对应于 CIAAN 中的“Confidentiality”目标. Denial of service 表示拒绝服务攻击, 影响认证协议的正常运行, 对应于 CIAAN 中的“Availability”目标. Elevation of privilege 表示非法提升权限获得访问特权, 对应于 CIAAN 中的“Authorization”目标.

(3) 典型攻击防御分析

1) 女巫攻击: 女巫攻击中攻击者通过创建大量的假名身份来破坏网络服务. 在基于区块链的 IoT 认证机制中, 为了防止女巫攻击, 所有实体均需要具备一个唯一可验证的身份, 只有通过记账节点的验证和共识后才会将设备的所有交易信息存储到链上, 不合法的节点交易会在验证阶段被筛除.

2) 重放攻击: 重放攻击是指攻击者发送一个接收方已接收过的交易, 来达到欺骗系统的目的. 通常使用添加时间戳、随机数和流水号 3 种方式来预防重放攻击. 添加时间戳的方式不需要在交易中额外保存其他信息, 但是认证双方需要保证精确的时钟同步. 当 IoT 系统很庞大且跨域范围较广, 这一点很难达成. 添加随机数的方式不需要认证双方时钟同步, 只需要记住相同的随机数. 但是为系统引入了保存和查询随机数的开销. 添加流水号的方式即认证双方交易中添加一个有序递增的整数, 只要接收到一个不连续的流水号, 就认定有重放威胁. 该方法优点是不需要时间同步并且保存的信息量比随机数方式小. 但是一旦攻击者对报文解密成功, 就可以获得流水号, 从而可以每次将流水号递增欺骗认证端.

3) 中间人攻击: 中间人攻击是指攻击者与通讯的两端分别建立联系, 并交换其所收到的数据, 使通讯的两端认为他们正在通过一个私密的连接与对方直接对话, 但事实上整个对话都被攻击者完全控制. 现有的认证方案中通常使用数字证书[47]预防此类攻击, 因为攻击者无法伪造正确的数字证书. 此外, 由于交易被记录在链上, 接收方可以通过查询交易并验证数字签名以判别交易发送方的身份信息.

4) DDOS 攻击: DDoS 攻击是指攻击者对网络在短时间内发起大量请求, 耗尽服务器的资源, 使其无法响应正常的访问, 导致服务中断. 在基于区块链的 IoT 认证方案中, 区块链节点发起一笔交易需要支付一定手续费, 这大大增加了攻击者发动 DDoS 的成本. 其次, 生成一个区块需要消耗非常高昂的算力、存储资源, 对于 PoW 共识而言, 需要超过全网 51% 的算力才能施加攻击, 显然是不切实际的. 此外, 由于区块链分布式和冗余存储的特性, 一个节点的崩溃不会影响系统的正常运行和服务的可获得性.

5) 单点故障: 攻击者将攻击目标聚焦于单一对象, 通过此对象的失效影响整个 IoT 系统的服务可获得性和系统可靠性. 通过分析 IoT 认证机制是否预防单点故障来判断系统中是否存在安全隐患.

6) 隐私泄露攻击: 由于区块链账本公开透明, 攻击者可以通过访问链上数据窃取 IoT 系统隐私. 如第 1.3 节所述, 现有方案主要通过地址混淆、信息隐藏、通道隔离 3 种方式为链上数据赋予隐私保护的特性. 是否实现隐私保护是判别 IoT 认证机制是否安全的关键指标之一.

形式化的安全性分析方法通过理论模型严谨地证明 IoT 认证机制的安全漏洞防范特性, 但是流程复杂且需要建立完备的假设条件; 非形式化安全分析方法通过讨论安全特性实现更简洁的安全性验证, 但是缺乏严密的证明. 因此, 两者的有机结合可能更适合于基于区块链的 IoT 认证机制的安全性论证.

4 研究展望

前人的研究为基于区块链的 IoT 身份认证工作奠定了坚实的基础, 但是考虑到将云边协同架构引入 IoT 环境带来的新的认证需求以及 IoT 设备本身的海量、异构、资源受限等特性, IoT 身份认证还需要进行广泛深入地研究.

4.1 云边端架构下的区块链平台搭建

如第 1.2 节所述, 结合了云端全局、长周期的数据管理能力与边缘端局部、低延时的数据处理能力的云边协同架构已成为 IoT 架构发展的新趋势. 边缘设备在接入网络时向云端发送认证请求, 而 IoT 用户/设备只需在边缘端进行身份注册, 无需向云端发送认证请求, 大大简化了 IoT 认证的复杂度, 提高了服务体验. 但是边缘计算的分布式特性与海量异构设备的多层交互导致传统云架构下的网络安全机制无法适用于新型的云-边-端 IoT 三层架构, 因此对身份认证机制设计提出了新的需求. 边缘设备的资源种类和服务覆盖范围有限, 需要多台设备间实现服务迁移调度以满足任务需求, 但是设备间缺乏可信的协作机制. 区块链基于 P2P 和非对称加密技术为非信任实体提供了安全协作环境, 但是不同边缘设备对协作权限与协作效率具有特殊标准, 因此对区块链平台的构建提出了不同需求. 区块链从“准入限制”的角度可分为公有链、私有链和联盟链. 其中公有链中任何人可参与共识, 且能按照达成共识所扮演的角色获得对应奖励, 但是服务具有可扩展性瓶颈、吞吐量较弱. 私有链设置了严格的准入规则, 规定节点读写区块链的权限. 由于私有链具有明确的控制层次结构, 因此大大提升了协同效率, 但是失去了去中心化的优势. 联盟链介于公有链和私有链之间, 将少数具有同等权利的参与方视为验证节点, 只要验证者达成共识即可更改系统规则, 权衡了去中心化和协同效率.

因此构建满足不同服务提供商对 IoT 认证效率与权限需求的区块链平台将成为云-边-端架构下基于区块链技术的 IoT 认证的研究重点.

4.2 区块链与 IoT 融合瓶颈研究

如第 1.3 节所述, 将区块链技术集成到 IoT 应用具有资源消耗、性能瓶颈、隐私需求还有数据膨胀 4 点挑战. 首先, IoT 设备普遍存在计算能力低、联网能力弱、电池续航短等问题, 无法适应资源消耗型的共识算法. 区块链的去中心化架构需要共识机制来确保数据的最终一致性, 对节点资源的需求无法避免. 无论是使用算力较强的网

关部署区块链节点还是设计轻量级的共识算法都是迫切需要深入探讨的研究课题. 其次, 区块链的交易性能无法满足 IoT 认证的并发性需求. 以比特币[57]为例, 比特币中的交易是 7 笔/s, 加上共识确认需要 1 h 写入区块链, 这种延时引起的反馈时延对于实时性敏感的 IoT 应用是无法接受的. 并且区块链的交易透明性与 IoT 用户/设备对隐私的需求相排斥, 需要使用额外的密码学方案对传输数据和身份信息进行隐私保护. 最后, 区块链是一个只能增加不能删除的数据存储技术, 随着 IoT 认证信息持续增长, 区块链账本的存储需求不断扩大, 对 IoT 架构中的节点提出了严峻挑战. 因此需要采取链上链下相协作的存储模式. 不管是采用本地存储、中心化数据库存储还是分布式存储, 都迫切需要解决 IoT 认证信息的存储瓶颈.

因此, 如何解决将区块链技术引入 IoT 认证面临的技术挑战将成为未来另一个研究重点.

4.3 密钥分发与管理机制研究

基于密码学的信息安全解决方案是保护信息隐私和系统安全的核心措施. 在 IoT 认证工作中, 不管是基于对称和非对称加密的认证机制还是基于证书与基于 IBC 的认证, 都离不开密钥的分发与管理. 然而现阶段大多数工作都省略了密钥生成的细节[6], 默认设备在初始化阶段已经拥有加密密钥对和签名密钥对. 密钥管理包括密钥的生成、存储、分配、更新、吊销、控制和销毁等内容. 由于基于不同密码学算法的密钥生成和维护具有不同的复杂性, 因此密钥分发和管理机制的设计对 IoT 认证机制的效率具有很大影响. 其次, 系统和信息的安全性本质上是对密钥的保护而不是对硬件和算法本身的保护, 如果密钥在传输或存储过程中被窃取或更改, 系统则会面临严重的安全威胁. 因此忽视密钥管理会影响 IoT 认证机制的安全性和实际可行性.

密钥分发与管理机制主要具有以下 3 点需求: 密钥无法被非法窃取和更改; 密钥需要定期更换; 密钥的分配与管理过程对用户透明, 降低用户操作复杂度. 因此, 在未来基于区块链的 IoT 认证工作中需要针对密钥的分发与管理进行深入研究.

4.4 多场景协作的认证机制研究

IoT 的本质是基于海量终端的协作, 全面感知数据, 进而辅助应用执行智能决策. 未来的 IoT 应用会打破数据孤岛形成多场景协作的共享生态[17], 因此需要关注多场景协作下的 IoT 认证机制研究. 主要体现在两点需求, 一是同场景内各层设备间的相互认证, 二是跨场景的设备相互认证. 不同 IoT 场景中的终端设备呈现出不同的特性, 可以总结为以下 5 点: 海量、异构、多维、轻量、实时. 异构表示设备源自不同的生产商, 具有不同的通信协议和密钥管理方法; 多维包括状态多维和功能多维, 例如静态的室温感知设备与动态的定位设备; 轻量表示 IoT 终端设备资源受限, 无法部署复杂的安全机制; 实时表示设备对任务的反馈延时敏感, 需要得到及时处理. 因此如何在满足各 IoT 场景中设备特性的前提下设计场景内部认证以及跨场景相互认证的安全机制是未来的一个研究难点.

5 总 结

身份认证是 IoT 系统安全性的基本保证, 只有建立安全的身份认证机制才能进一步实施访问控制和数据共享. 随着区块链技术的发展, 基于区块链的 IoT 身份认证成为学术界和工业界共同的研究热点.

本文分析了传统架构和云-边-端架构下 IoT 身份认证机制设计的主要需求, 总结了在 IoT 应用中使用区块链技术面临的挑战和现有解决思路, 将现有 IoT 身份认证的工作从密钥使用的角度分为基于对称密钥和非对称密钥的认证、基于证书的认证和基于身份的认证. 根据区块链技术在 IoT 认证工作中的功能, 对现有基于区块链的 IoT 认证工作进行了对比分析, 并从认证对象 (用户、设备) 和附加属性 (跨域认证、轻量级认证、匿名认证、多层认证) 两个维度对文献进行了分类和归纳. 将针对 IoT 认证机制的安全性分析方法抽象为形式化和非形式两类, 并进行了详细介绍, 为研究者设计基于区块链的 IoT 认证机制的安全性分析方法提供通用的解决思路.

具有分布式特性的区块链技术天然适用于 IoT 场景, 尽管目前仍存在一些待解决的问题, 但可以预期的是, 随着各种轻量级共识机制、可扩展性方案的研究, 区块链将有力推动 IoT 认证工作的进展.

References:

[1] Chen M, Hao YX. Task offloading for mobile edge computing in software defined ultra-dense network. IEEE Journal on Selected Areas

in Communications, 2018, 36(3): 587–597. [doi: 10.1109/JSAC.2018.2815360]

[2] Mohiuddin I, Almogren A. Security challenges and strategies for the IoT in cloud computing. In: Proc. of the 11th Int'l Conf. on Information and Communication Systems (ICICS). Irbid: IEEE, 2020. 367–372. [doi: 10.1109/ICICS49469.2020.239563]

[3] Zhou J, Cao ZF, Dong XL, Vasilakos AV. Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine, 2017, 55(1): 26–33. [doi: 10.1109/MCOM.2017.1600363CM]

[4] Shen M, Liu HS, Zhu LH, Xu K, Yu HB, Du XJ, Guizani M. Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942–954. [doi: 10.1109/JSAC.2020.2980916]

[5] Wang X, Zha X, Ni W, Liu RP, Guo YJ, Niu XX, Zheng KF. Survey on blockchain for Internet of Things. Computer Communications, 2019, 136: 10–29. [doi: 10.1016/j.comcom.2019.01.006]

[6] Hao K, Xin JC, Wang ZQ, Wang GR. Outsourced data integrity verification based on blockchain in untrusted environment. World Wide Web, 2020, 23(4): 2215–2238. [doi: 10.1007/s11280-019-00761-2]

[7] Yu W, Liang F, He XF, Hatcher WG, Lu C, Lin J, Yang XY. A survey on the edge computing for the Internet of Things. IEEE Access, 2018, 6: 6900–6919. [doi: 10.1109/ACCESS.2017.2778504]

[8] Von Maltitz M, Carle G. Leveraging secure multiparty computation in the Internet of Things. In: Proc. of the 16th Annual Int'l Conf. on Mobile Systems, Applications, and Services. Munich: ACM, 2018. 508–510. [doi: 10.1145/3210240.3223569]

[9] Song WT, Hu B, Zhao XF. Privacy protection of IoT based on fully homomorphic encryption. Wireless Communications and Mobile Computing, 2018, 2018: 5787930. [doi: 10.1155/2018/5787930]

[10] Ayoade G, Karande V, Khan L, Hamlen K. Decentralized IoT data management using blockchain and trusted execution environment. In: Proc. of the 2018 IEEE Int'l Conf. on Information Reuse and Integration (IRI). Salt Lake City: IEEE, 2018. 15–22. [doi: 10.1109/IRI.2018.00011]

[11] Flood P, Schukat M. Peer to peer authentication for small embedded systems: A zero-knowledge-based approach to security for the Internet of Things. In: Proc. of the 10th Int'l Conf. on Digital Technologies. Zilina: IEEE, 2014. 68–72. [doi: 10.1109/DT.2014.6868693]

[12] Martín-Fernández F, Caballero-Gil P, Caballero-Gil C. Authentication based on non-interactive zero-knowledge proofs for the Internet of Things. Sensors, 2016, 16(1): 75. [doi: 10.3390/s16010075]

[13] Beydemir A, Soğukpinar İ. Lightweight zero knowledge authentication for Internet of Things. In: Proc. of the 2017 Int'l Conf. on Computer Science and Engineering (UBMK). Antalya: IEEE, 2017. 360–365. [doi: 10.1109/UBMK.2017.8093410]

[14] Walshe M, Epiphaniou G, Al-Khateeb H, Hammoudeh M, Katos V, Dehghantanha A. Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments. Ad Hoc Networks, 2019, 95: 101988. [doi: 10.1016/j.adhoc.2019.101988]

[15] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016, 42(4): 481–494 (in Chinese with English abstract). [doi: 10.16383/j.aas.2016.c160158]

[16] Xu RH, Chen Y, Blasch E, Chen GS. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the IoT. Computers, 2018, 7(3): 39. [doi: 10.3390/computers7030039]

[17] Park JS, Youn TY, Kim HB, Rhee KH, Shin SU. Smart contract-based review system for an IoT data marketplace. Sensors, 2018, 18(10): 3577. [doi: 10.3390/s18103577]

[18] Islam MN, Kundu S. Poster abstract: Preserving IoT privacy in sharing economy via smart contract. In: Proc. of the 3rd IEEE/ACM Int'l Conf. on Internet of Things Design and Implementation (IoTDI). Orlando: IEEE, 2018. 296–297. [doi: 10.1109/IoTDI.2018.00047]

[19] Ren YJ, Liu YP, Ji S, Sangaiah AK, Wang J. Incentive mechanism of data storage based on blockchain for wireless sensor networks. Mobile Information Systems, 2018, 2018: 6874158. [doi: 10.1155/2018/6874158]

[20] Zhu LH, Wu YL, Gai KK, Choo KKR. Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 2019, 91: 527–535. [doi: 10.1016/j.future.2018.09.019]

[21] Yang Z, Yang K, Lei L, Zheng K, Leung VCM. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 2019, 6(2): 1495–1505. [doi: 10.1109/JIOT.2018.2836144]

[22] Wang HY, Zhang JW. Blockchain based data integrity verification for large-scale IoT data. IEEE Access, 2019, 7: 164996–165006. [doi: 10.1109/ACCESS.2019.2952635]

[23] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Çapkun S. On the security and performance of proof of work blockchains. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 3–16. [doi: 10.1145/2976749.2978341]

[24] Kably S, Arioua M, Alaoui N. Lightweight blockchain network architecture for IoT devices. In: Proc. of the 2020 Int'l Symp. on

Advanced Electrical and Communication Technologies (ISAECT). Marrakech: IEEE, 2020. 1–6. [doi: 10.1109/ISAECT50560.2020.9523686]

[25] Ehmke C, Wessling F, Friedrich CM. Proof-of-property: A lightweight and scalable blockchain protocol. In: Proc. of the 1st Int'l Workshop on Emerging Trends in Software Engineering for Blockchain. Gothenburg: ACM, 2018. 48–51. [doi: 10.1145/3194113.3194122]

[26] Kim T, Noh J, Cho S. SCC: Storage compression consensus for blockchain in lightweight IoT network. In: Proc. of the 2019 IEEE Int'l Conf. on Consumer Electronics (ICCE). Las Vegas: IEEE, 2019. 1–4. [doi: 10.1109/ICCE.2019.8662032]

[27] Zamani M, Movahedi M, Raykova M. RapidChain: Scaling blockchain via full sharding. In: Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security. Toronto: ACM, 2018. 931–948. [doi: 10.1145/3243734.3243853]

[28] Biswas S, Sharif K, Li F, Maharjan S, Mohanty SP, Wang Y. PoBT: A lightweight consensus algorithm for scalable IoT business blockchain. IEEE Internet of Things Journal, 2020, 7(3): 2343–2355. [doi: 10.1109/JIOT.2019.2958077]

[29] Gupta S, Hellings J, Rahnama S, Sadoghi M. Building high throughput permissioned blockchain fabrics: Challenges and opportunities. Proc. of the VLDB Endowment, 2020, 13(12): 3441–3444. [doi: 10.14778/3415478.3415565]

[30] Yu ST, Lv K, Shao Z, Guo YC, Zou J, Zhang B. A high performance blockchain platform for intelligent devices. In: Proc. of the 1st IEEE Int'l Conf. on Hot Information-centric Networking (HotICN). Shenzhen: IEEE, 2018. 260–261. [doi: 10.1109/HOTICN.2018.8606017]

[31] Zhu L, Yu H, Zhan SX, Qiu WW, Li QL. Research on high-performance consortium blockchain technology. Ruan Jian Xue Bao/Journal of Software, 2019, 30(6): 1577–1593 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5737.htm [doi: 10.13328/j.cnki.jos.005737]

[32] Wang H, Wang Y, Cao ZG, Li Z, Xiong G. An overview of blockchain security analysis. In: Proc. on the 15th China Cyber Security Annual Conf. Beijing: Springer, 2018. 55–72. [doi: 10.1007/978-981-13-6621-5_5]

[33] Zhang A, Bai XY. Survey of research and practices on blockchain privacy protection. Ruan Jian Xue Bao/Journal of Software, 2020, 31(5): 1406–1434 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

[34] Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for Bitcoin. In: Proc. of the 2015 Int'l Conf. on Financial Cryptography and Data Security. San Juan: Springer, 2015. 112–126. [doi: 10.1007/978-3-662-48051-9_9]

[35] Zhao Y, Zhao J, Jiang LS, Tan R, Niyato D, Li ZX, Lv LJ, Liu YB. Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet of Things Journal, 2021, 8(3): 1817–1829. [doi: 10.1109/JIOT.2020.3017377]

[36] Poon J, Dryja T. The Bitcoin lightning network: Scalable off-chain instant payments. 2016. https://readpaper.com/paper/633537424487690240

[37] Misra S, Mukherjee A, Roy A, Saurabh N, Rahulamathavan Y, Rajarajan M. Blockchain at the edge: Performance of resource-constrained IoT networks. IEEE Trans. on Parallel and Distributed Systems, 2021, 32(1): 174–183. [doi: 10.1109/TPDS.2020.3013892]

[38] Raghav N, Andola N, Venkatesan S, Verma S. PoEWAL: A lightweight consensus mechanism for blockchain in IoT. Pervasive and Mobile Computing, 2020, 69: 101291. [doi: 10.1016/j.pmcj.2020.101291]

[39] Sagirlar G, Carminati B, Ferrari E, Sheehan JD, Ragnoli E. Hybrid-IoT: Hybrid blockchain architecture for Internet of Things-pow sub-blockchains. In: Proc. of the 2018 IEEE Int'l Conf. 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: IEEE, 2018. 1007–1016. [doi: 10.1109/Cybermatics_2018.2018.00189]

[40] Yang T, Zhang GH, Liu L, Zhang YQ. A survey on authentication protocols for Internet of Things. Journal of Cryptologic Research, 2020, 7(1): 87–101 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000352]

[41] Bellare M, Canetti R, Krawczyk H. Keying hash functions for message authentication. In: Proc. of the 16th Annual Int'l Cryptology Conf. Berlin: Springer, 1996. 1–15. [doi: 10.1007/3-540-68697-5_1]

[42] Rechberger C, Rijmen V. On authentication with HMAC and non-random properties. In: Proc. of the 11th Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer, 2007. 119–133. [doi: 10.1007/978-3-540-77366-5_13]

[43] Alizai ZA, Tareen NF, Jadoon I. Improved IoT device authentication scheme using device capability and digital signatures. In: Proc. of the 2018 Int'l Conf. on Applied and Engineering Mathematics (ICAEM). Taxila: IEEE, 2018. 1–5. [doi: 10.1109/ICAEM.2018.8536261]

[44] Mughal MA, Luo X, Ullah A, Ullah S, Mahmood Z. A lightweight digital signature based security scheme for human-centered Internet of Things. IEEE Access, 2018, 6: 31630–31643. [doi: 10.1109/ACCESS.2018.2844406]

[45] Porambage P, Schmitt C, Kumar P, Gurtov A, Ylianttila M. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In: Proc. of the 2014 IEEE Wireless Communications and Networking Conf. Istanbul: IEEE, 2014. 2728–2733. [doi: 10.1109/WCNC.2014.6952860]

[46] Sciancalepore S, Capossele A, Piro G, Boggia G, Bianchi G. Key management protocol with implicit certificates for IoT systems. In: Proc. of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems. Florence: ACM, 2015. 37–42. [doi: 10.1145/2753476.2753477]

[47] Moosavi SR, Gia TN, Rahmani AM, Nigussie E, Virtanen S, Isoaho J, Tenhunen H. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 2015, 52: 452–459. [doi: 10.1016/j.procs.2015.05.013]

[48] Raza S, Shafagh H, Hewage K, Hummen R, Voigt T. Lithe: Lightweight secure CoAP for the Internet of Things. IEEE Sensors Journal, 2013, 13(10): 3711–3720. [doi: 10.1109/JSEN.2013.2277656]

[49] Ni JB, Lin XD, Shen XS. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. IEEE Journal on Selected Areas in Communications, 2018, 36(3): 644–657. [doi: 10.1109/JSAC.2018.2815418]

[50] Hernández-Ramos JL, Pawlowski MP, Jara AJ, Skarmeta AF, Ladid L. Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications, 2015, 33(4): 690–702. [doi: 10.1109/JSAC.2015.2393436]

[51] Matsumoto S, Reischuk RM. IKP: Turning a PKI around with decentralized automated incentives. In: Proc. of the 2017 IEEE Symp. on Security and Privacy (SP). San Jose: IEEE, 2017. 410–426. [doi: 10.1109/SP.2017.57]

[52] Baek J, Newmarch J, Safavi-Naini R, Susilo W. A survey of identity-based cryptography. In: Proc. of the 2004 Australian Unix Users Group Annual Conf. 2004. 95–102.

[53] Heo J, Hong CS, Choi MS, Ju SH, Lim YH. Identity-based mutual device authentication schemes for PLC system. In: Proc. of the 2008 IEEE Int'l Symp. on Power Line Communications and Its Applications. Jeju: IEEE, 2008. 47–51. [doi: 10.1109/ISPLC.2008.4510397]

[54] Li HW, Dai YS, Tian L, Yang HM. Identity-based authentication for cloud computing. In: Proc. of the 1st IEEE Int'l Conf. on Cloud Computing. Beijing: Springer, 2009. 157–166. [doi: 10.1007/978-3-642-10665-1_14]

[55] Lin JY, Zhang ZL, Yuan ZW. Research on authentication encryption mechanism based on IBC in Internet of Things. Journal of Information Security and Communications Privacy, 2020, (8): 95–101 (in Chinese with English abstract). [doi: 10.3969/j.issn.1009-8054.2020.08.012]

[56] Han S, Xie MD, Yang BL, Lu RX, Bao HY, Lin JH, Hong HB, Gu MX, Han S. A certificateless verifiable strong designated verifier signature scheme. IEEE Access, 2019, 7: 126391–126408. [doi: 10.1109/ACCESS.2019.2938898]

[57] Nakamoto S, Bitcoin A. A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[58] Li RN, Song TY, Mei B, Li H, Cheng XZ, Sun LM. Blockchain for large-scale Internet of Things data storage and protection. IEEE Trans. on Services Computing, 2019, 12(5): 762–771. [doi: 10.1109/TSC.2018.2853167]

[59] Cui ZH, Xue F, Zhang SQ, Cai XJ, Cao Y, Zhang WS, Chen JJ. A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Trans. on Services Computing, 2020, 13(2): 241–251. [doi: 10.1109/TSC.2020.2964537]

[60] Li DX, Peng W, Deng WP, Gai FY. A blockchain-based authentication and security mechanism for IoT. In: Proc. of the 27th Int'l Conf. on Computer Communication and Networks (ICCCN). Hangzhou: IEEE, 2018. 1–6. [doi: 10.1109/ICCCN.2018.8487449]

[61] Wu LF, Du XJ, Wang W, Lin B. An out-of-band authentication scheme for Internet of Things using blockchain technology. In: Proc. of the 2018 Int'l Conf. on Computing, Networking and Communications (ICNC). Maui: IEEE, 2018. 769–773. [doi: 10.1109/ICCNC.2018.8390280]

[62] Kaur K, Garg S, Kaddoum G, Gagnon F, Ahmed SH. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In: Proc. of the 2019 IEEE Int'l Conf. on Communications Workshops (ICC Workshops). Shanghai: IEEE, 2019. 1–6. [doi: 10.1109/ICCW.2019.8757184]

[63] Yao YY, Chang XL, Mišić J, Mišić VB, Li L. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 2019, 6(2): 3775–3784. [doi: 10.1109/JIOT.2019.2892009]

[64] Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 2018, 78: 126–142. [doi: 10.1016/j.cose.2018.06.004]

[65] Yazdinejad A, Parizi RM, Dehghantanha A, Choo KKR. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. IEEE Trans. on Network Science and Engineering, 2021, 8(2): 1120–1132. [doi: 10.1109/TNSE.2019.2937481]

[66] Yazdinejad A, Srivastava G, Parizi RM, Dehghantanha A, Choo KKR, Aledhari M. Decentralized authentication of distributed patients in hospital networks using blockchain. IEEE Journal of Biomedical and Health Informatics, 2020, 24(8): 2146–2156. [doi: 10.1109/JBHI.2020.2969648]

[67] Lin C, He DB, Kumar N, Huang XY, Vijayakumar P, Choo KKR. Homechain: A blockchain-based secure mutual authentication system

for smart homes. IEEE Internet of Things Journal, 2020, 7(2): 818–829. [doi: 10.1109/jiot.2019.2944400]

[68] Mounnan O, El Mouatasim A, Manad O, Hidar T, El Kalam AA, Idboufker N. Privacy-aware and authentication based on blockchain with fault tolerance for IoT enabled fog computing. In: Proc. of the 5th Int'l Conf. on Fog and Mobile Edge Computing (FMEC). Paris: IEEE, 2020. 347–352. [doi: 10.1109/FMEC49853.2020.9144845]

[69] Zhang L, Li H, Sun LM, Shi ZQ, He YH. Poster: Towards fully distributed user authentication with blockchain. In: Proc. of the 2017 IEEE Symp. on Privacy-aware Computing (PAC). Washington DC: IEEE, 2017. 202–203. [doi: 10.1109/PAC.2017.28]

[70] Alghamdi TA, Ali I, Javaid N, Shafiq M. Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain. IEEE Access, 2020, 8: 1048–1061. [doi: 10.1109/ACCESS.2019.2961612]

[71] Lin X, Li JH, Wu J, Liang HR, Yang W. Making knowledge tradable in Edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach. IEEE Trans. on Industrial Informatics, 2019, 15(12): 6367–6378. [doi: 10.1109/TII.2019.2917307]

[72] Lin X, Wu J, Bashir AK, Li JH, Yang W, Piran J. Blockchain-based incentive energy-knowledge trading in IoT: Joint power transfer and AI design. IEEE Internet of Things Journal, 2022, 9(16): 14685–14698. [doi: 10.1109/JIOT.2020.3024246]

[73] Wu B, Li Q, Xu K, Li RY, Liu ZT. Smartretro: Blockchain-based incentives for distributed IoT retrospective detection. In: Proc. of the 15th IEEE Int'l Conf. on Mobile Ad Hoc and Sensor Systems (MASS). Chengdu: IEEE, 2018. 308–316. [doi: 10.1109/MASS.2018.00053]

[74] Wang JZ, Li MR, He YH, Li H, Xiao K, Wang C. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access, 2018, 6: 17545–17556. [doi: 10.1109/ACCESS.2018.2805837]

[75] He YH, Li H, Cheng XZ, Liu Y, Yang C, Sun LM. A blockchain based truthful incentive mechanism for distributed P2P applications. IEEE Access, 2018, 6: 27324–27335. [doi: 10.1109/ACCESS.2018.2821705]

[76] Jia B, Zhou T, Li W, Liu ZC, Zhang JT. A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Sensors, 2018, 18(11): 3894. [doi: 10.3390/s18113894]

[77] Wang S, Ouyang LW, Yuan Y, Ni XC, Han X, Wang FY. Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Trans. on Systems, Man, and Cybernetics: Systems, 2019, 49(11): 2266–2277. [doi: 10.1109/TSMC.2019.2895123]

[78] Almadhoun R, Kadadha M, Alhemeiri M, Alshehhi M, Salah K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In: Proc. of the 15th IEEE/ACS Int'l Conf. on Computer Systems and Applications (AICCSA). Aqaba: IEEE, 2018. 1–8. [doi: 10.1109/AICCSA.2018.8612856]

[79] Chen YL, Wang XJ, Yang YL, Li H. Location-aware Wi-Fi authentication scheme using smart contract. Sensors, 2020, 20(4): 1062. [doi: 10.3390/s20041062]

[80] Ali G, Ahmad N, Cao Y, Khan S, Cruickshank H, Qazi EA, Ali A. xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. IEEE Access, 2020, 8: 58800–58816. [doi: 10.1109/ACCESS.2020.2982542]

[81] Liu DL, Li D, Liu X, Ma L, Yu H, Zhang H. Research on a cross-domain authentication scheme based on consortium blockchain in V2G networks of smart grid. In: Proc. of the 2nd IEEE Conf. on Energy Internet and Energy System Integration (EI2). Beijing: IEEE, 2018. 1–5. [doi: 10.1109/EI2.2018.8582227]

[82] Zheng JW, Dong XW, Shen YL, Tong W. Decentralized and secure cross-domain data sharing scheme based on blockchain for application-centric IoT. Journal of Information Science & Engineering, 2020, 36(4): 821–836.

[83] Guo SY, Wang FN, Zhang N, Qi F, Qiu XS. Master-slave chain based trusted cross-domain authentication mechanism in IoT. Journal of Network and Computer Applications, 2020, 172: 102812. [doi: 10.1016/j.jnca.2020.102812]

[84] Dong S, Yang H, Yuan JQ, Jiao LB, Yu A, Zhang J. Blockchain-based cross-domain authentication strategy for trusted access to mobile devices in the IoT. In: Proc. of the 2020 Int'l Wireless Communications and Mobile Computing (IWCMC). Limassol: IEEE, 2020. 1610–1612. [doi: 10.1109/IWCMC48107.2020.9148358]

[85] Li GS, Wang Y, Zhang B, Lu SQ. Smart contract-based cross-domain authentication and key agreement system for heterogeneous wireless networks. Mobile Information Systems, 2020, 2020: 2964562. [doi: 10.1155/2020/2964562]

[86] Guo SY, Hu X, Guo S, Qiu XS, Qi F. Blockchain meets edge computing: A distributed and trusted authentication system. IEEE Trans. on Industrial Informatics, 2020, 16(3): 1972–1983. [doi: 10.1109/TII.2019.2938001]

[87] Zhang ZW, Zhong C, Guo SY, Wang FN. A master-slave chain architecture model for cross-domain trusted and authentication of power services. In: Proc. of the 7th Int'l Conf. on Information Technology: IoT and Smart City. Shanghai: ACM, 2019. 483–487. [doi: 10.1145/3377170.3377225]

[88] Li CL, Wu Q, Li HW, Liu J. Trustroam: A novel blockchain-based cross-domain authentication scheme for Wi-Fi access. In: Proc. of the 14th Int'l Conf. on Wireless Algorithms, Systems, and Applications. Honolulu: Springer, 2019. 149–161. [doi: 10.1007/978-3-030-23597-0_12]

[89] Zhang HX, Chen XS, Lan X, Jin HJ, Cao Q. BTCAS: A blockchain-based thoroughly cross-domain authentication scheme. Journal of Information Security and Applications, 2020, 55: 102538. [doi: 10.1016/j.jisa.2020.102538]

[90] Jia XD, Hu N, Su S, Yin S, Zhao Y, Cheng XD, Zhang C. IRBA: An identity-based cross-domain authentication scheme for the Internet of Things. Electronics, 2020, 9(4): 634. [doi: 10.3390/electronics9040634]

[91] Wang JH, Li SS, Wei SJ. Identity-based cross-domain authentication by blockchain via PKI environment. In: Proc. of the 2nd CCF China Blockchain Conf. Chengdu: IEEE, 2019. 131–144. [doi: 10.1007/978-981-15-3278-8_9]

[92] Zheng JW, Dong XW, Zhang T, Chen JF, Tong W, Yang XZ. MicrothingsChain: Edge computing and decentralized IoT architecture based on blockchain for cross-domain data shareing. In: Proc. of the 2018 Int'l Conf. on Networking and Network Applications (NaNA). Xi'an: IEEE, 2018. 350–355. [doi: 10.1109/NANA.2018.8648780]

[93] Sun S, Chen SD, Du R. Trusted and efficient cross-domain access control system based on blockchain. Scientific Programming, 2020, 2020: 8832568. [doi: 10.1155/2020/8832568]

[94] Dang FF, Gao F, Liang HC, Sun Y. Multi-dimensional identity authentication mechanism for power maintenance personnel based on blockchain. In: Proc. of the 2020 Int'l Wireless Communications and Mobile Computing (IWCMC). Limassol: IEEE, 2020. 215–219. [doi: 10.1109/IWCMC48107.2020.9148178]

[95] Tahir M, Sardaraz M, Muhammad S, Khan MS. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability, 2020, 12(17): 6960. [doi: 10.3390/su12176960]

[96] Fayad A, Hammi B, Khatoun R, Serhrouchni A. A blockchain-based lightweight authentication solution for IoT. In: Proc. of the 3rd Cyber Security in Networking Conf. (CSNet). Quito: IEEE, 2019. 28–34. [doi: 10.1109/CSNet47905.2019.9108958]

[97] Khalid U, Asim M, Baker T, Hung PCK, Tariq MA, Rafferty L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Computing, 2020, 23(3): 2067–2087. [doi: 10.1007/s10586-020-03058-6]

[98] Jangirala S, Das AK, Vasilakos AV. Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. IEEE Trans. on Industrial Informatics, 2020, 16(11): 7081–7093. [doi: 10.1109/TII.2019.2942389]

[99] Danish SM, Lestas M, Asif W, Qureshi HK, Rajarajan M. A lightweight blockchain based two factor authentication mechanism for lorawan join procedure. In: Proc. of the 2019 IEEE Int'l Conf. on Communications Workshops (ICC Workshops). Shanghai: IEEE, 2019. 1–6. [doi: 10.1109/ICCW.2019.8756673]

[100] Sidorov M, Ong MT, Sridharan RV, Nakamura J, Ohmura R, Khor JH. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access, 2019, 7: 7273–7285. [doi: 10.1109/ACCESS.2018.2890389]

[101] Mohanty SN, Ramya KC, Rani SS, Gupta D, Shankar K, Lakshmanaprabu SK, Khanna A. An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy. Future Generation Computer Systems, 2020, 102: 1027–1037. [doi: 10.1016/j.future.2019.09.050]

[102] Satamraju KP, Malarkodi B. Proof of concept of scalable integration of Internet of Things and blockchain in healthcare. Sensors, 2020, 20(5): 1389. [doi: 10.3390/s20051389]

[103] Djilali HB, Tandjaoui D. Efficient distributed authentication and access control system management for Internet of Things using blockchain. In: Proc. of the 5th Int'l Conf. on Mobile, Secure, and Programmable Networking. Mohammedia: Springer, 2019. 51–60. [doi: 10.1007/978-3-030-22885-9_5]

[104] Alkhazaali AH, ATA O. Lightweight fog based solution for privacy-preserving in IoT using blockchain. In: Proc. of the 2020 Int'l Congress on Human-computer Interaction, Optimization and Robotic Applications (HORA). Ankara: IEEE, 2020. 1–10. [doi: 10.1109/HORA49412.2020.9152923]

[105] Wang J, Wu LB, Choo KKR, He DB. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Trans. on Industrial Informatics, 2020, 16(3): 1984–1992. [doi: 10.1109/TII.2019.2936278]

[106] Yu Y, Zhao YQ, Li YN, Du XJ, Wang LH, Guizani M. Blockchain-based anonymous authentication with selective revocation for smart industrial applications. IEEE Trans. on Industrial Informatics, 2020, 16(5): 3290–3300. [doi: 10.1109/TII.2019.2944678]

[107] Lin C, He DB, Huang XY, Kumar N, Choo KKR. BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. IEEE Trans. on Intelligent Transportation Systems, 2021, 22(12): 7408–7420. [doi: 10.1109/TITS.2020.3002096]

[108] Zhang QK, Li YJ, Wang RF, Li JY, Gan Y, Zhang YH, Yu X. Blockchain-based asymmetric group key agreement protocol for Internet of vehicles. Computers & Electrical Engineering, 2020, 86: 106713. [doi: 10.1016/j.compeleceng.2020.106713]

[109] Mwitende G, Ye YL, Ali I, Li FG. Certificateless authenticated key agreement for blockchain-based WBANs. Journal of Systems Architecture, 2020, 110: 101777. [doi: 10.1016/j.sysarc.2020.101777]

[110] Gabay D, Akkaya K, Cebe M. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. IEEE Trans. on Vehicular Technology, 2020, 69(6): 5760–5772. [doi: 10.1109/TVT.2020.2977361]

[111] Zhang QK, Li YJ, Li JY, Gan Y, Zhang YH, Hu JJ. Blockchain-based asymmetric group key agreement protocol for mobile ad hoc network. In: Proc. of the 5th Int'l Symp. on Security and Privacy in Social Networks and Big Data. Copenhagen: Springer, 2019. 47–56. [doi: 10.1007/978-981-15-0758-8_4]

[112] Xu JB, Meng XW, Liang W, Peng L, Xu ZS, Li KC. A hybrid mutual authentication scheme based on blockchain technology for WBANs. In: Proc. of the 1st Int'l Conf. on Blockchain and Trustworthy Systems. Guangzhou: Springer, 2019. 350–362. [doi: 10.1007/978-981-15-2777-7_28]

[113] Lu ZJ, Liu WC, Wang Q, Qu G, Liu ZL. A privacy-preserving trust model based on blockchain for VANETs. IEEE Access, 2018, 6: 45655–45664. [doi: 10.1109/ACCESS.2018.2864189]

[114] Malik N, Nanda P, Arora A, He XJ, Puthal D. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In: Proc. of the 17th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications/12th IEEE Int'l Conf. on Big Data Science and Engineering. New York: IEEE, 2018. 674–679. [doi: 10.1109/TrustCom/BigDataSE.2018.00099]

[115] Zheng D, Jing CM, Guo R, Gao SY, Wang L. A traceable blockchain-based access authentication system with privacy preservation in VANETs. IEEE Access, 2019, 7: 117716–117726. [doi: 10.1109/ACCESS.2019.2936575]

[116] Xiang XY, Wang MY, Fan WG. A permissioned blockchain-based identity management and user authentication scheme for E-Health systems. IEEE Access, 2020, 8: 171771–171783. [doi: 10.1109/ACCESS.2020.3022429]

[117] Wang XL, Zeng PJ, Patterson N, Jiang F, Doss R. An improved authentication scheme for Internet of vehicles based on blockchain technology. IEEE Access, 2019, 7: 45061–45072. [doi: 10.1109/ACCESS.2019.2909004]

[118] Mohanta BK, Sahoo A, Patel S, Panda SS, Jena D, Gountia D. DecAuth: Decentralized authentication scheme for IoT device using Ethereum blockchain. In: Proc. of the 2019 IEEE Region 10 Conf. (TENCON). Kochi: IEEE, 2019. 558–563. [doi: 10.1109/TENCON.2019.8929720]

[119] Feng DG, Fan H. Survey on theories and methods of formal analyses for security protocols. Journal of the Graduate School of the Chinese Academy of Sciences, 2003, 20(4): 389–406 (in Chinese with English abstract). [doi: 10.3969/j.issn.1002-1175.2003.04.001]

[120] Gao S, Hu AQ, Shi L, Chen XB. A survey on formal analysis of security protocols. Journal of Cryptologic Research, 2014, 1(5): 504–512 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000047]

[121] Burrows M, Abadi M, Needham RM. A logic of authentication. Proc. of the Royal Society A: Mathematical Physical and Engineering Sciences, 1989, 426(1871): 233–271. [doi: 10.1098/rspa.1989.0125]

[122] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. In: Proc. of the 1990 IEEE Computer Society Symp. on Research in Security and Privacy. Oakland: IEEE, 1990. 234–248. [doi: 10.1109/RISP.1990.63854]

[123] Abadi M, Tuttle MR. A semantics for a logic of authentication (extended abstract). In: Proc. of the 10th Annual ACM Symp. on Principles of Distributed Computing. Quebec: ACM, 1991. 201–216. [doi: 10.1145/112600.112618]

[124] Syverson PF, van Oorschot PC. A unified cryptographic protocol logic. Technical Report, Washington DC: Naval Research Laboratory, 1996.

[125] Dolev D, Yao AC. On the security of public key protocols. IEEE Trans. on Information Theory, 1983, 29(2): 198–208. [doi: 10.1109/TIT.1983.1056650]

[126] Lowe G, Roscoe B. Using CSP to detect errors in the TMN protocol. IEEE Trans. on Software Engineering, 1997, 23(10): 659–669. [doi: 10.1109/32.637148]

[127] Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuellar J, Drielsma PH, Heám PC, Kouchnarenko O, Mantovani J, Mödersheim S, Von Oheimb D, Rusinowitch M, Santiago J, Turuani M, Viganò L, Vigneron L. The AVISPA tool for the automated validation of Internet security protocols and applications. In: Proc. of the 17th Int'l Conf. on Computer Aided Verification. Edinburgh: Springer, 2005. 281–285. [doi: 10.1007/11513988_27]

[128] Srinivas J, Das AK, Wazid M, Kumar N. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. IEEE Trans. on Dependable and Secure Computing, 2020, 17(6): 1133–1146. [doi: 10.1109/TDSC.2018.2857811]

[129] Paulson LC. The inductive approach to verifying cryptographic protocols. Journal of Computer Security, 1998, 6(1–2): 85–128.

[130] Schneider S. Using CSP for Protocol Analysis: The Needham-Schroeder Public-key Protocol. Hiroshima: University of London, Royal Holloway, Department of Computer Science, 1996.

[131] Fabrega FJT, Herzog JC, Guttman JD. Strand spaces: Why is a security protocol correct? In: Proc. of the 1998 IEEE Symp. on Security and Privacy. Oakland: IEEE, 1998. 160–171. [doi: 10.1109/SECPRI.1998.674832]

[132] Peng K, Li M, Huang H, *et al*. Security challenges and opportunities for smart contracts in Internet of Things: A survey. IEEE Internet of Things Journal, 2021, 8(15): 12004–12020.

附中文参考文献:

[15] 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494. [doi: 10.16383/j.aas.2016.c160158]

[31] 朱立, 俞欢, 詹士潇, 邱炜伟, 李启雷. 高性能联盟区块链技术研究. 软件学报, 2019, 30(6): 1577–1593. http://www.jos.org.cn/1000-9825/5737.htm [doi: 10.13328/j.cnki.jos.005737]

[33] 张奥, 白晓颖. 区块链隐私保护研究与实践综述. 软件学报, 2020, 31(5): 1406–1434. http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

[40] 杨婷, 张光华, 刘玲, 张玉清. 物联网认证协议综述. 密码学报, 2020, 7(1): 87–101. [doi: 10.13868/j.cnki.jcr.000352]

[55] 林俊燕, 张兆雷, 袁智伟. 物联网中基于IBC的认证加密机制研究. 信息安全与通信保密, 2020, (8): 95–101. [doi: 10.3969/j.issn.1009-8054.2020.08.012]

[119] 冯登国, 范红. 安全协议形式化分析理论与方法研究综述. 中国科学院研究生院学报, 2003, 20(4): 389–406. [doi: 10.3969/j.issn.1002-1175.2003.04.001]

[120] 高尚, 胡爱群, 石乐, 陈先棒. 安全协议形式化分析研究. 密码学报, 2014, 1(5): 504–512. [doi: 10.13868/j.cnki.jcr.000047]

程冠杰(1996－), 男, 博士生, CCF 学生会员, 主要研究领域为区块链, 物联网, 可信数据管理, 身份认证.

严学强(1970－), 男, 博士, 高级工程师, 主要研究领域为网络架构, 数据治理, 联邦学习, 分布式计算, 隐私保护.

邓水光(1979－), 男, 博士, 教授, 博士生导师, CCF 杰出会员, 主要研究领域为服务计算, 边缘计算, 流程管理, 软件工程, 大数据.

赵明宇(1977－), 男, 博士, 高级工程师, 主要研究领域为无线网络架构, 分布式架构, 数据服务, 区块链, 边缘 AI.

温盈盈(1994－), 女, 博士生, 主要研究领域为云计算, 系统性能优化.