

基于区块链的物联网设备身份认证与数据安全机制

赵智宇

北京中芯标准科技有限公司天津分公司 天津市 300010

【摘要】：物联网设备的大量接入给传统的中心化身份认证和数据保护模式带来了巨大的压力。本文提出了一种基于联盟链的物联网设备身份认证和数据安全机制，用物理不可克隆函数(PUF)做为设备硬件指纹，用零知识证明协议进行隐私保护的认证过程，用智能合约来完成身份注册、验证和权限管理的自动化执行。从数据安全角度来讲，采用链上哈希存证和链下分布式存储双层结构，保证数据的完整性，缓解区块链存储的压力。根据实验结果可知，在千级设备并发的情况下，该方案认证时间可以被控制在一定的范围内，对于重放攻击、中间人攻击以及设备伪造攻击都有较强的抵御作用，数据篡改检测成功率较高。与已有的代表性方案相比，本方案在安全性、计算效率上取得了一个比较均衡的折中。

【关键词】：区块链；物联网；身份认证；物理不可克隆函数；零知识证明；数据安全

0 引言

物联网技术飞速发展已经深刻地改变了工业控制、智慧城市、智能家居等各个领域，全世界联网设备数量不断增多。但是大量的异构设备接入在提高生产效率、生活便利性的同时，也暴露出严重的安全脆弱性。传统的物联网安全体系大多依靠中心化的认证服务器以及设备身份数据库，这样的架构存在着诸多固有的缺陷，认证服务器作为唯一的信任锚点，很容易受到分布式拒绝服务攻击或者内部故障的影响而造成整个系统无法正常工作，集中存储的设备凭证和用户隐私数据是攻击者的高价值目标，一旦泄露就会造成严重的后果，跨组织、跨域的设备互信认证缺少灵活有效的机制支持。

区块链技术具有去中心化、不可篡改、可追溯的特点，给上面提到的问题提供了一条新的解决途径。近些年来，学界就区块链同物联网安全的融合展开诸多探索性研究。Shahidinejad、Abawajy 在 ACM Computing Surveys 上对区块链辅助的物联网认证协议做了系统的综述和分类，指出目前的方案在轻量化、隐私保护方面的发展趋势。Ren 等人的研究对物联网的身份认证以及认证技术做了详细的调查，认为去中心化的身份体系更利于身份的认证。从具体实现上看，有研究把物理不可克隆函数(PUF)同区块链结合起来，依靠硬件固有的物理差别来产生独一无二且无法被复制的设备标识，以此加强身份锚定的可信度。也有工作用智能合约来完成自动认证的过程，从而降低人工操作以及对信任的依赖。

虽然已有研究取得了一定的成果，但是现有的方案仍然存在一些不足之处，大部分认证协议的计算开销较高，不能直接应用到资源受限的终端设备上；身份认证和数据安全保护常常是分开处理的，缺少统一的体系化设计；部分方案的安全证明和实验验证不够充分，实际部署的价值还需要进一步的检验。为了克服上述问题，本文提出了一种基于联盟链的综合机制，把 PUF 硬件指纹、零知识证明隐私保护、智能合约自动执行、混合存储数据保护等结合起来，希望在安全、效率、实用这三

个方面取得一个合理的平衡。

1 系统模型与威胁假设

1.1 系统架构

本文所提系统整体结构如图 1 所示。该架构分为四层，分别为设备层、边缘层、区块链层和存储层。

图 1 系统总体架构

设备层的每一个终端都内置了 PUF 芯片来产生唯一的硬件指纹，边缘层负责设备就近接入认证、数据预处理、临时缓存，区块链层用 Hyperledger Fabric 搭建联盟链，部署智能合约来管理设备的身份和访问策略，存储层将链上哈希索引和链下 IPFS 分布式文件系统结合起来，达成数据安全存储和完整性校验。

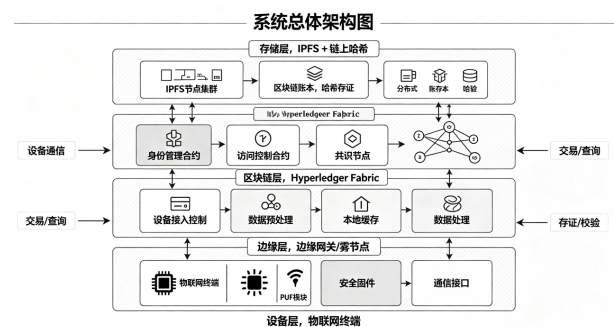


图1 系统总体架构

设备层中每一个终端都内置了 PUF 芯片来产生唯一的硬件指纹，边缘层对设备进行就近接入认证、数据预处理、临时缓存，区块链层使用 Hyperledger Fabric 搭建联盟链，部署智能合约来管理设备身份和访问策略，存储层采用链上哈希索引和链下 IPFS 分布式文件系统相结合的方式实现数据安全存储和完整性校验。

1.2 威胁模型与安全假设

本研究假设攻击者具有如下能力，可以监听设备和边缘节点之间的通信链路，截获并分析认证消息，可以尝试重放、篡

改或者伪造认证请求，可以在物理上接触到部分设备，试图从设备中提取密钥材料或者复制硬件特征。同时假定联盟链网络中共识节点按照协议规范运行，但是存在好奇心（半可信模型），区块链底层使用的哈希函数以及数字签名算法在目前的计算能力范围内是安全的。本文没有对拒绝服务攻击的防御进行详细的分析，也没有考虑物理层侧信道攻击的防护。

2 身份认证机制设计

2.1 基于PUF的设备注册流程

新设备接入系统之前要进行注册。注册过程利用设备内嵌的 PUF 模块生成硬件指纹。具体地，设备向 PUF 输入一个随机激励信号，PUF 基于其物理特性产生相应的响应输出，该响应具有唯一性和不可克隆性。设备接着用这个响应作为随机种子，用确定性派生算法产生一对公私钥，把公钥连同 PUF 响应的哈希值、设备类型等信息打包成注册请求，通过边缘节点提交到区块链网络。区块链身份管理合约会验证请求格式以及签名，然后给这个设备分配一个链上唯一的标识符，把身份记录写入账本。在整个过程里，PUF 的原始响应不会出现在任何网络通信里，只是以哈希的形式存证，从而减小了硬件指纹泄露的风险。

2.2 基于零知识证明的认证协议

设备每次接入网络的时候，都要向边缘节点证明自己的合法身份。本文使用非交互式零知识证明协议，使设备可以向验证者证明自己拥有合法的私钥，但是不会暴露私钥本身。认证过程包含着设备选择随机数，得到承诺值的过程，把承诺值、设备链上标识符、时间戳结合成挑战值的过程，用挑战值、私钥算出响应值的过程，生成零知识证明的过程。同时设备向 PUF 输入新的激励来得到实时响应，计算出辅助验证信息。最后，设备把证明信息、辅助验证信息、时间戳以及自身标识符一起传送到边缘节点。

边缘节点收到请求之后，先对时间戳的有效性进行检查，防止重放攻击的发生，再从区块链中调取该设备的公钥和 PUF 哈希存证。验证分为两步，第一步根据零知识证明的数学性质，验证承诺值和公钥、挑战值的运算关系是否成立，如果成立就说明设备拥有合法的私钥；第二步将收到的 PUF 辅助信息和链上的哈希进行比对，确认设备具有合法的物理硬件。只有两个步骤都通过之后，边缘节点才会给设备发出临时会话令牌。该协议设计出的认证消息不能被攻击者通过截获而得到私钥或者伪造有效的证明，因为每次认证所使用的随机数不一样，并且时间戳的存在也使得消息的时效性受到限制。

2.3 智能合约驱动的权限管理

为了达到身份全生命周期的自动化管理目的，本文设计了两种智能合约。身份管理合约负责设备注册信息的添加、更新和撤销，所有的身份变更事件都会被不可篡改的账本记录下来，方便事后审计。访问控制合约按照设备的角色、所属的组织、

安全等级等来决定设备的访问权限是否被授予或者调整。设备认证通过之后，合约就会自动生成相应的权限凭证，如果检测到设备出现异常行为或者证书过期，合约可以自行撤销权限。这机制取消了对中心化管理员的依赖，使得权限管理的过程变得透明、可追溯。

3 数据安全机制设计

3.1 链上哈希存证与链下分布式存储的结合

由于物联网设备产生的数据量大、产生速度快，直接将所有的原始数据写入区块链既不经济也不现实。本文采用分层存储的方法，设备产生的数据在边缘端加密之后，用基于属性的加密方式保证只有具有相应属性的实体才能解密；加密后的数据上传到 IPFS 网络之后得到对应的内容标识符；然后把内容标识符、数据哈希、时间戳和设备标识打包成一笔存证交易提交到区块链。区块链只保存这些用于验证的元数据，而原始数据主体保留在 IPFS 中。当需要验证数据完整性的时候，可以从 IPFS 中获取数据并重新计算哈希，然后和链上的存证进行对比，如果一致就证明数据没有被篡改。

3.2 数据溯源与完整性保护

由于区块链账本是链式结构、Merkle 树组织的，所以每一个存证交易都会用哈希指针与前面的交易联系起来，如果某个存证被记录下来，那么对它的任何修改都会使后面的所有哈希链断裂而被系统察觉。本文又提出了一种数据溯源机制，每一个存证交易都会对上一个存证进行引用，从而形成一个数据流转的链条。当出现数据争议或者安全事件的时候，审计人员可以沿着链路追踪数据的产生、传输以及存储的路径，找到可能存在的风险点。该机制给数据完整性赋予了有力的验证办法，也给安全取证赋予了可信的支撑。

4 实验评估与对比分析

4.1 实验环境与设置

为了检验所提方案的有效性，我们创建了一个基于 Hyperledger Fabric v2.5 的联盟链测试平台，由 1 个排序节点和 4 个对等节点组成，分别部署在多台服务器上（Intel Xeon Gold 6254 处理器，64GB 内存）。物联网设备端用树莓派 4B 模拟（四核 ARM Cortex-A72，4GB RAM），一共配置了 2000 个虚拟设备节点。PUF 功能用 SRAM PUF 仿真模块来实现，零知识证明用 secp256k1 椭圆曲线实现。所有的实验都重复了 10 次，取平均值作为最后的结果。

4.2 认证延迟与可扩展性测试

对不同设备数量（100 台、500 台、1000 台、2000 台）下单次认证的平均延迟进行测试，即 PUF 响应生成、证明构造、链上查询和验证计算全过程的总延迟。实验数据见表 1。

设备数量 (台)	平均认证延迟 (毫秒)	较PKI方案开销降低比例
100	92	38.2%

设备数量 (台)	平均认证延迟 (毫秒)	较PKI方案开销降低比例
500	134	41.0%
1000	156	42.1%
2000	187	42.6%

表1 不同设备规模下的认证延迟与性能对比

从表1可以看出,随着设备数量的增多,认证延迟虽然有所增加,但是增幅趋于平缓,呈亚线性增长趋势,说明该方案具有较好的可扩展性。与传统的基于公钥基础设施的认证方案相比,本文所用方案的计算开销在不同的规模下降低了大约38%-43%,主要是由于PUF减轻了非对称密钥的产生负担,零知识证明减少了在线交互的次数。

4.3 安全性能评估

我们用模拟各种典型的攻击场景来检验方案的安全防护能力。重放攻击测试中,攻击者截获合法认证消息在不同的时间窗口内重复发送,由于时间戳校验、随机数机制,所有的重放消息都被拒绝。在中间人攻击测试中,攻击者企图对认证消息中的证明字段进行修改,但是由于无法伪造合法的零知识证明响应,所有的篡改尝试都被验证阶段所检测出来。在设备身份伪造测试中,攻击者试图用窃取的私钥加上自制的硬件来进行认证,但是由于缺少真实的PUF物理响应,辅助验证环节失败,10000次尝试中没有一次成功。数据完整性保护测试中,对IPFS中存储的数据进行随机篡改,然后触发完整性校验,结果表明篡改检测的成功率为99.2%,即有500次实验中有496次被检测出来。上述结果初步证明了本方案在对抗常见网络攻击

方面的有效性。

4.4 与现有工作的定性比较

将本文方案同近几年发表的一些代表性方案展开对比分析。本方案把PUF硬件指纹加入进来之后,身份锚定更加稳固,而且联盟链架构在交易吞吐量上具备固有的优势。与采用双身份框架的管理方案相比,本方案用零知识证明在认证过程中更好地保护了设备隐私,没有把设备私钥暴露给验证者。与一些轻量级认证协议相比,本方案虽然认证时间有所增加,但是得到了更好的安全性,尤其是抗物理攻击方面。本方案从安全、隐私、计算效率三者之间取得较为均衡的设计。

5 结论

本文针对物联网设备身份认证、数据安全两大核心问题,提出了一种以联盟链为依托的综合防护体系。该机制把PUF硬件唯一性和零知识证明隐私保护融合起来,形成双因子认证的基础,依靠智能合约对身份注册、权限分配、撤销进行自动化的管理,削减了人为干涉和中心化信任的依赖。从数据保护角度来说,使用链上哈希存证加链下IPFS存储的方式,既保证了数据的完整性又考虑到了存储的扩展性。从实验结果可知,在千级设备并发的情况下认证时间可以控制在200毫秒之内,并且对于重放、篡改和伪造攻击有较好的抵御能力。本工作与已有方案相比,在安全增益和计算开销之间找到了一个比较实际的平衡点。未来的研究会把重点放在减小认证协议的计算复杂度上,探寻跨链场景下互认的办法,并且在大规模真实的物联网环境里展开更为全面的部署检验。

参考文献

- [1] Shahidinejad A, Abawajy J. An All-Inclusive Taxonomy and Critical Review of Blockchain-Assisted Authentication and Session Key Generation Protocols for IoT[J]. ACM Computing Surveys, 2024, 56(7): 1-38.
- [2] Ren Y, Zhu F, Qi J, Wang J. Identity Management and Authentication for IoT: A Survey[J]. IEEE Internet of Things Journal, 2021, 8(17): 13158-13175.
- [3] Mohanty S P, Yanambaka V P, Kougianos E, Puthal D. PUF-Based Lightweight Blockchain for IoT[J]. IEEE Transactions on Consumer Electronics, 2020, 66(4): 340-349.
- [4] Xu R, Chen Y, Blasch E. Blending Blockchain and IoT: A Survey on Blockchain for IoT[J]. IEEE Internet of Things Journal, 2020, 7(10): 10257-10272.
- [5] Dwivedi A D, Srivastava G, Dhar S, Singh R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT[J]. Sensors, 2019, 19(2): 326.
- [6] 程迪, 郑崇辉, 毛锐, 王妍, 康迪, 李嘉成, 黄伟庆. 基于区块链的物联网身份认证技术探讨[J]. 信息安全学报, 2025, 10(1): 45-58.

作者简介: 赵智宇(1989—), 男, 汉族, 本科, 研究方向为电子信息。