基于区块链技术的物联网隐私数据安全访问认证

乔 博[1]
QIAO Bo

摘 要 物联网隐私数据的传统存储和管理方式使得数据容易被篡改，而区块链具有不可篡改的特性。区块链记录的数据一旦写入便无法更改，确保了数据的完整性和高度可信。基于此，提出一种基于区块链技术的物联网隐私数据安全访问认证方法。其中，构建了以区块链为核心的隐私数据保护机制，通过为隐私数据设置安全访问权限标签，实现了对数据访问权限的有效划分，有效防止了未经授权的访问和数据篡改。在身份认证环节，当用户尝试访问隐私数据时，系统会即时计算用户提供的属性信息与系统中存储的账号信息之间的相似度分数。一旦该分数超过预设的安全阈值，系统便会确认用户身份合法，并授权其访问相应的隐私数据。这种基于精确身份认证的方法，确保了只有符合条件的用户才能访问其专属的隐私数据。实验结果显示，所提出的方法在面对模拟的威胁攻击时，数据泄露率远低于其他对比方法，且均控制在 10% 以内。同时，其加密和解密操作的响应时间均不超过 10 s，证明了所提出的方法在保障数据安全的同时，也保持了高效的数据处理能力。

关键词 区块链技术；物联网；隐私数据；保护机制；安全访问认证

doi：10.3969/j.issn.1672-9528.2024.10.038

0 引言

在当前数据泄露和网络安全事件频发的严峻形势下，物联网隐私数据的安全访问和认证成为行业内外共同关注的焦点。物联网技术的广泛应用使得海量的数据被实时收集和传输，这些数据中往往蕴含个人隐私、企业核心机密等敏感信息，一旦泄露或遭非法访问，将引发难以估量的后果。因此，如何确保这些数据在传输、存储和使用过程中的安全性，成为物联网技术发展中亟待解决的重要问题。

针对物联网隐私数据的安全访问与认证，学术界与业界持续探索创新解决方案。文献 [1] 借助云计算平台强大的计算和存储能力，实现了物联网数据的集中化管理与精细化访问控制，有效提升了系统效能。文献 [2] 通过加密技术对物联网数据进行保护，利用动态访问权限管理策略实现细粒度的数据访问控制。这种方法可以有效地防止数据在传输和存储过程中被非法访问或篡改，确保数据的机密性与完整性。上述两种方法的加密手段往往伴随着较高的计算成本，对于资源受限的物联网设备可能并不适用，且加密技术本身也可能存在被破解的风险，不能完全保证数据的安全性。文献 [3] 提出的混合云存储模型，通过融合私有云和公有云的优势，在提供灵活部署、数据隔离及灾难恢复能力的同时，也带来了管理与成本控制的复杂性挑战。文献 [4] 探讨了属性加密技术在跨域安全共享中的应用，其细粒度的访问控制与跨域数据共享能力显著增强了隐私保护效果，但同样面临着计算资源开销大及密钥管理复杂的难题。

为了克服上述方法的不足，本文提出了一种基于区块链技术的物联网隐私数据安全访问认证方法。区块链技术以其独特的去中心化、不可篡改和透明可追溯等特性，为物联网隐私数据安全访问认证提供了新的解决思路。通过将数据以区块的形式进行链式存储，区块链技术能够确保数据在传输和存储过程中的安全性和完整性。利用密码学技术，区块链可以实现对数据的加密和签名验证，防止数据被篡改或伪造。同时，区块链的去中心化特性使得数据不再依赖于单一的信任中心，而是由多个节点共同维护和管理，从而提高了系统的鲁棒性和可靠性。

1 利用区域链技术建立隐私数据保护机制

为了加强物联网隐私数据的安全访问认证，采用了区块链技术，构建了一套全面而高效的隐私数据保护机制。该机制充分利用区块链的不可篡改性和去中心化特性，确保隐私数据在传输和存储过程中的完整性和安全性。设计了一种多层区块链架构，该架构由一条主链和若干从链组成。主链负责跨链请求的解析与协调，确保数据交互的透明和公正；而从链则作为特定领域的可信平台，专注于该领域内的数据管理和访问控制。

1. 郑州财经学院 河南郑州 450000

在主链层面，利用智能合约等先进技术，对隐私数据的访问权限进行了严格的控制和审计，确保了数据交互的合规性与安全性。主链还作为连接各个从链的桥梁，促进了不同领域数据在遵守规则前提下的互联互通。在从链层面，定义了数据节点与交互节点两种关键角色。数据节点专注于隐私数据的加密存储与安全处理，采用先进加密算法保障数据在本地存储时的绝对安全。交互节点则负责与其他链路及外部网络的通信，确保数据的顺畅流通与高效交换[5]。这种分工提高了系统效率，并增强了整体安全性。此外，引入了分布式存储技术，将隐私数据分散存储在多个节点上，降低了单点故障风险，并增强了数据的抗篡改能力。结合实时监控与异常检测机制，能够及时发现并应对潜在的恶意节点和数据篡改行为，确保系统稳定运行和数据安全。隐私节点如图 1 所示。

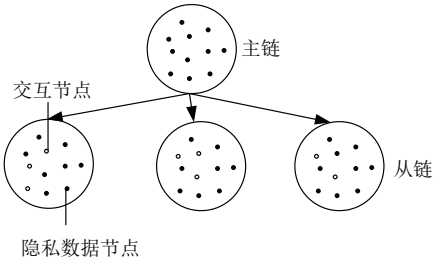

图 1 存储节点

如图 1 所示，在区块链网络中，隐私数据节点根据其在不同区块的特性和需求，采用了多样化的存储和管理方法。为了更有效地管理这些隐私数据，引入基于区块链技术的层级式节点，其中每个节点根据其可信度和功能被赋予不同的权限等级。利用区块链技术的去中心化和安全特性，量化隐私数据的安全性。隐私数据安全指数 P 的计算公式为：

$$P=\sum_{i=1}^{N}\left(R_iW_i\right) \tag{1}$$

式中：N 表示区块内参与节点的数量，R_i 表示第 i 个数据项的值，W_i 表示第 i 个数据项的权重。

基于上述隐私数据安全指数，建立了隐私数据保护机制，该机制在保障数据安全的同时，保持数据的统计特性不变，便于数据共享时的聚类分析。

基于隐私数据安全指数 P 的约束条件，设置安全访问权限标签和标识。为每个数据拥有者或生产者分配独特的标识，这些标识不仅代表了数据的来源，更清晰地标识了数据中包含的隐私信息类型。通过这一标识，快速识别并区分不同敏感级别的数据。为访问这些隐私数据的对象设置了标签[6]，这些标签是根据数据的隐私等级和安全需求来定义的，每一个标签都是由一系列标识构成的集合，它们精确地反映了被标注实体所具备的隐私信息类型。标签的多样性确保了访问权限的精细控制，从而降低了数据泄露的风险。实体是指被标签标注的对象，包括数据拥有者、生产者以及访问数据的过程。利用一个统一的集合来表示所有实体，以便进行统一的管理和监控。

对于数据的访问权限，设进程标签为 L_P，数据标签为 L_d，这两个标签可以看作是一个集合。集合中的元素代表不同的安全特性或隐私类型。定义一个包含关系来判断进程是否有权访问数据：

$$A_c \Leftrightarrow L_P \supseteq L_d \tag{2}$$

通过比较这两个标签，决定一个进程是否有权访问特定的数据。如果 L_P 包含 L_d，即当进程标签满足或高于数据标签的要求时，访问请求才会被允许。

2 实现物联网隐私数据访问认证

在物联网环境中，隐私数据的安全性是首要考虑的问题。通过严格的身份认证流程，可以确保只有经过授权的合法用户才能访问敏感数据，从而有效防止数据泄露给未经授权的第三方。虽然区块链技术提供了数据不可篡改性和去中心化的优势，但并不能直接解决身份认证问题。因此，结合区块链的隐私保护机制与严格的身份认证流程，可以形成更加全面的安全防护体系。传统的单一属性认证（如仅依赖用户名和密码）存在被破解的风险。为了提高安全性，在身份认证过程中，通过加密传输和存储这些敏感信息，并结合区块链的隐私保护机制。通过综合评估符合身份标签用户的多个属性来判定其身份，可以增强系统安全性、提高身份认证的准确性、适应多样化的认证需求、保障用户隐私。

定义用户属性集合为 $A=[a_1, a_2, \cdots, a_n]$，其中 a_n 表示用户的第 n 个属性，如用户名、密码、生物识别信息（如指纹、虹膜扫描）或其他动态验证信息（如手机验证码）等[7]。每个属性都有其对应的特征空间，将用户的属性值映射到这些特征空间中进行量化分析。计算待认证用户属性与数据库中存储的账户属性之间的相似度。设 S_n 为第 n 个属性的相似度，其计算方式依赖于具体的相似度衡量指标，如字符串相似度、地理距离等。

为了综合考虑多个属性的影响，为每个属性分配一个权重 W_n，权重的大小反映了该属性在身份认证中的重要性。为了克服传统主观赋权法的局限性，采用基于历史操作信息的属性信息熵值法[8]来计算权重。信息熵 $H(a_n)$ 反映了属性 a_n 的不确定性，计算公式为：

$$H\left(a_n\right)=-\sum_{j=1}^{M}p\left(a_n^j\right)\log_2 p\left(a_n^j\right) \tag{3}$$

式中：M 表示属性状态数，$p(a_n^j)$ 表示属性 a_n 处于第 j 个状态的概率。权重 W_n 则可以通过归一化信息熵得到：

$$W_n=\frac{1-H\left(a_n\right)}{\sum_{k=1}^{n}\left[1-H\left(a_k\right)\right]} \tag{4}$$

综合相似度分数，结合了多种属性信息，为每个属性赋予不同权值，最终得到一个综合评估结果。这种评估方法不仅考虑了属性的多样性，还充分考虑了不同属性在身份识别中的重要性。综合相似度 S 为：

$$S=\sum_{n=1}^{M}W_nS_n \tag{5}$$

综合相似度分数能够反映出用户提供的属性信息集合与系统中存储的账号信息之间的匹配程度，直接决定了用户身份的真实性。设置访问阈值为 η，则可以得出，若 $S>\eta$，认为用户提供的属性信息与系统中某个账号信息高度一致，进而确认用户的身份，从而允许该用户访问相应的隐私数据[9]。若 $S<\eta$ 则认为身份认证不成功，不允许该用户访问相应的隐私数据。这种方法不仅提高了身份认证的准确性，还有效地保障了用户的隐私安全[10]。

3 实验

为了验证本文提出的基于区块链技术的物联网隐私数据安全访问认证方法的有效性，进行对比测试。选择了两种具有代表性的方法作为对照组：一是文献 [1] 提出的基于云计算的分布式隐私数据访问权限控制方法，二是文献 [2] 提出的基于加密技术的隐私数据动态访问权限管理方法。

3.1 实验准备

在准备物联网隐私数据安全访问认证实验时，采用了开源的区块链框架（Ethereum）结合 Docker 容器技术，构建了一个高度可配置的区块链开发平台。该平台不仅提供了强大的区块链网络功能，还通过 Docker 容器技术确保了实验环境的灵活性和可移植性。区块链开发平台如图 2 所示。

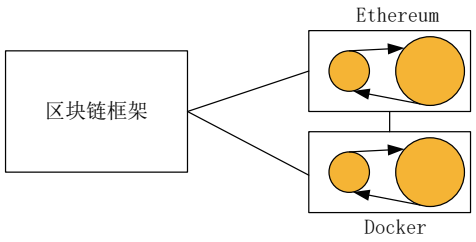

图 2 区块链开发平台

为确保测试结果客观公正，将三种隐私数据访问认证方法应用于统一的模拟物联网环境中，并对这几种方法的加密与解密性能进行了全面的评估。测试的重点在于物联网设备的用户数据访问流程，其中模拟用户需要通过相应的认证机制验证权限后才能访问系统。该环境模拟了真实场景中的用户行为，通过严格的权限管理机制来验证每种方法在保护数据安全性方面的效能。详细的测试环境如表 1 所示。该配置确保了网络系统能够高效地处理数据访问请求，包括历史数据的回溯查询和新数据的创建与管理。用户接入系统后，可以查阅历史数据记录，并根据需求发起新的数据访问请求。

表 1 测试环境配置

项目	详细描述
操作系统	Windows 10 专业版
数据库系统	SQL Server 2016
浏览器	安全浏览器
服务器配置	CPU：Intel Xeon E5-2680 v4 内存：32 GB DDR4 ECC REG 硬盘：4 TB SATA 网络接口：千兆以太网
存储空间	存储 2.5 TB 模拟数据
网络环境	局域网连接，带宽 1 Gbit/s
防火墙	Windows Defender 防火墙
其他	测试环境定期备份

为了验证不同安全访问权限认证方法的性能，在区块链开发平台上集成了这三种方法，并通过模拟真实的网络环境进行连接。测试平台中包含了关键配置文件、模拟物联网数据、用户权限信息、访问日志记录以及测试脚本等五种核心文件，具体数据如表 2 所示。

表 2 测试平台包含的核心文件

文件类型	文件名	描述
关键配置文件	config.json	包含区块链网络配置、节点设置、端口号、加密参数等关键信息，用于初始化测试环境。
模拟物联网数据	iot_data.csv	包含模拟的物联网设备生成的数据，如传感器读数、设备状态等，用于测试数据访问和验证功能。
用户权限信息	user_permissions.db	存储用户的身份信息和相应的访问权限，如可读、可写等，用于验证用户的访问权限。
访问日志记录	access_log.txt	记录用户访问网络系统的所有操作，包括查询、修改、删除等，用于追踪和分析用户行为。
测试脚本	test_scripts.py	包含自动化测试脚本，用于模拟用户访问网络系统的各种场景，以验证安全访问权限认证方法的性能。

设定上述五种核心文件的消息字段长度为 80 字节，与之对应的加解密密文字段长度为 150 字节。

3.2 实验结果分析

为了验证三种不同加密方法的可靠性，分别测试了它们在加密和解密这五种核心文件时的数据泄露率。在网络环境中模拟威胁攻击，以测试不同加密方法在攻击模式下的表现。攻击模式下的测试结果如图 3 所示。分析图 3 的实验结果可知，在面对模拟威胁攻击时，本文所提出的安全访问认证方法展现出了显著的防护效果。与另外两种对比方法相比，本文方法的数据泄露率保持在一个非常低的水平，所有测试场景中的泄露率均未超过 10%。以上实验结果不仅验证了该方

法在实际应用中的高效性和可靠性，而且展示了其在保护物联网隐私数据安全方面的巨大潜力。本文方法的核心优势体现在以下几个方面：首先，区块链的去中心化特性有效地分散了安全风险，避免了单点故障的发生，从而增强了系统的整体稳定性；其次，精细化的安全访问权限标签和基于属性信息的准确身份认证机制，确保了只有经过严格验证的用户才能访问敏感数据，大大降低了未授权访问的可能性；最后，区块链的不可篡改性和透明性保证了数据交互的可追溯性和安全性，为物联网环境下的隐私保护提供了坚实的保障。

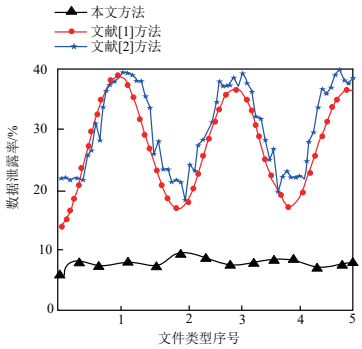

图 3 数据泄露率结果

为了进一步验证本文提出方法的实用性与效率，针对加密和解密五种核心文件的过程，分别测试了三种不同方法的响应时间。在数据安全访问权限的严格认证流程中，数据加密作为保障数据完整性和安全性的核心环节，其重要性不言而喻，而解密则是确保数据能够被合法用户顺利访问与使用的必要步骤。分阶段实施这两个关键步骤，以全面评估并确认数据的安全访问权限得到有效认证。具体的测试对比结果，如表 3 所示。

表 3 攻击模式下加密解密相应时间

单位：s

项目	文件类型序号	本文方法	文献 [1] 方法	文献 [2] 方法
加密	1	9.5	28.5	32.1
	2	5.8	33.5	29.5
	3	5.6	25.6	28.7
	4	6.4	23.4	25.3
	5	5.8	27.8	23.9
解密	1	5.4	22.3	28.9
	2	6.2	24.5	29.2
	3	5.9	26.2	27.6
	4	6.1	21.1	26.5
	5	5.3	25.6	25.8

通过对表 3 中的实验结果进行深入分析可知，本文所提出的方法在加密解密操作的响应时间这一关键性能指标上展现出了显著的优势。与表中的其他两种对比方法相比，本文方法在处理加密和解密请求时，其响应时间更为迅捷，所有测试场景下的响应时间均控制在 10 s 以内。这一结果不仅表明了本文方法在实际应用中的高效性，而且反映出其在提升用户体验和系统整体性能方面的巨大潜力。本文方法之所以能够在加密解密响应时间上取得如此优异的表现，主要在于采用了先进的加密算法和优化的数据处理流程。这些技术手段不仅提高了数据处理的效率，还减少了不必要的计算开销，从而确保了系统在面对大量并发请求时，仍能保持快速且稳定的响应能力。

4 结语

区块链技术的应用为物联网隐私数据的安全访问认证带来了显著的改进。通过去中心化的架构，不仅消除了传统 IoT 系统中的单点故障和攻击风险，还显著提升了系统的鲁棒性和安全性。本研究所提出的基于区块链的物联网隐私数据保护机制，通过设置精细化的安全访问权限标签和实施准确的身份认证流程，有效地保障了隐私数据的安全性，并确保了只有合法用户才能访问其专属数据。实验结果表明，该机制在实际应用中表现出色，其数据泄露率远低于传统方法，展现出在面对安全威胁时的卓越防御能力。因此，本研究不仅为物联网隐私数据保护提供了一个高效的技术解决方案，也为未来物联网安全领域的深入研究和发展奠定了坚实的基础。

参考文献：

[1] 曹敏，曹东朗 . 多源海量隐私大数据可靠性访问权限安全认证 [J]. 计算机仿真，2024,41(5): 395-399.
[2] 刘东，任海玲 . 基于差分隐私的大数据安全访问权限认证仿真 [J]. 计算机仿真，2021,38(8):421-424+486.
[3] 闫攀，周莉，闫会峰 . 混合云存储下物联网隐私数据保护模型研究 [J]. 计算机仿真，2023, 40(2):530-534.
[4] 冯绮航 . 考虑属性加密的物联网隐私数据跨域安全共享模型 [J]. 现代电子技术，2023,46(1):91-95.
[5] 曹美荣 . 基于区块链的物联网隐私数据保护技术研究与实践 [J]. 网络空间安全，2024,15(1):118-123.
[6] 林秋雄 . 基于区块链技术的物联网数据信息协同共享研究 [J]. 物流工程与管理，2024,46(2):36-39.
[7] 宋祺鹏，王继东，张丽伟，等 . 本地化差分隐私下的电力物联网终端数据隐私保护方法 [J]. 重庆邮电大学学报 (自然科学版)，2023,35(6):1001-1010.
[8] 赵鸽 . 基于区块链技术的校园全光无线网安全访问认证研究 [J]. 信息系统工程，2023, 26(10):87-90.
[9] 李斌，何辉，赵中英，等 . 基于区块链的多源网络大数据安全访问权限认证仿真 [J]. 电信科学，2024, 40(2):107-115.
[10] 闵庆学，李贺男 . 物联网隐私数据风险及保护分析研究 [J]. 通信管理与技术，2021, 52(4):65-67.

【作者简介】

乔博（1994—），女，河南巩义人，硕士，助教，研究方向：计算机应用。

（收稿日期：2024-07-11）