

[区块链]

基于区块链技术的仪表自动化数据安全与可信传输

文/敬芃辉

国家管网集团天津液化天然气有限责任公司

区块链技术以其独特的去中心化、不可篡改和加密性质，提供了一种新特性来保障数据在传输和存储过程中的安全性与可信度。探讨区块链技术在仪表自动化数据可信传输中的应用，包括可信传输机制的设计原理、数据加密和访问控制机制，通过数据测试来验证技术在实际中的应用效果和性能。

数据的安全性和可信度直接关联到整个自动化系统的可靠性和效率，然而，传统的数据保护机制面临着种种挑战。区块链技术作为一种创新的分布式账本技术，以其天然的不可篡改性、去中心化特性及通过密码学手段实现的数据安全与隐私保护，为解决上述问题提供了全新的视角和方法。它通过在网络的每个节点上维护数据的共享且不断更新的副本，使得数据一旦被验证并添加到区块链上，就无法被更改或删除，从而确保了数据的完整性与透明度。

区块链技术概述

区块链是一种分布式账本技术，其通过网络中的多个节点共同维护公开透明的数据链，每个数据块中不仅包含了一定数量的交易记录，还包括了前一块的加密散列，确保了整个链的不可逆性与连续性。通过这种方式，区块链技术有效地解决了“双重支付”问题，同时也为数据的安全性、可靠性和不可篡改性提供了坚实保障^[1]。智能合约的概念进一步拓展了区块链技术的应用范围，使得在无须中心化信任机构的前提下，能够在区块链上自动执行预先编写的合约条款，这不仅大幅度提高了交易的效率，也为各类应用提供了无限可能。

区块链在仪表自动化数据可信传输中的应用

1. 可信传输机制的设计原理

区块链作为一种分布式账本技术，通过去中心化、不可篡改的记录和智能合约等特性，为解决传统数据传输中的信任问题提供了创新方案。可信传输机制依托于区块链的去中心化特点，摒弃了传统中心化信任实体的需求，转而通过网络中多个节点之间的共识算法达成数据的一致性和可信度。每个数据事务在被加入区块链之前，需经过一系列的验证过程，此过程包括事务的来源验证、数据完整性校验以及合法性审查，确保了数据在传输过程中的真实性和未经篡改性。其机制不仅提高了数据传输过程的安全性和可信度，而且通过智能合约的应用，提高了数据处理的自动化水平，为仪表自动化系统中的数据安全与可信传输提供了一种全新的解决方案，如图1所示。该机制还具有良好的适应性和扩展性，能够支撑仪表自动化系统在各种不同环境下的安全可信数据传输需求，为仪表自动化领域的发展打开了全新的形式^[2]。

2. 数据加密

在区块链技术应用用于仪表自动化数据加密的研究中，数据的安全性和保密性至关重要。本部分旨在深入探讨加密算法及其在区块链中的实现，尤其

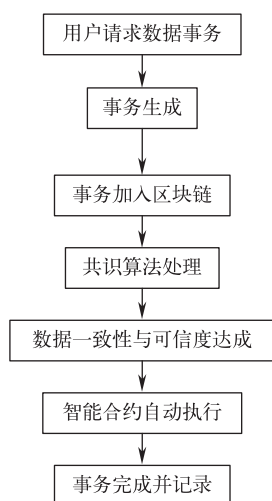


图1 可信传输机制的设计原理

是采用对称加密和非对称加密技术以确保数据在传输过程中的安全性和完整性。引入先进的加密算法，如椭圆曲线加密（ECC）算法，以及其在实时监测系统中的应用，本文将详细阐述加密过程及其在确保仪表自动化数据安全中的作用。考虑到区块链环境下数据加密的需求，ECC由于较高的安全性和较低的计算复杂度而被选为本研究的加密算法。ECC的基本公式为

$$y^2 = x^3 + ax + b \quad (1)$$

式中， a 和 b 是曲线方程的参数，确保了曲线的形状。

ECC的安全性基于椭圆曲线离散对数问题的计算困难性。在区块链应用中，公钥和私钥的生成是基于椭圆曲线上点的乘法运算，计算公式为

$$Q = kP \quad (2)$$

式中， P 是椭圆曲线上的点； k 是私钥； Q 是相应的公钥。

加密过程涉及将明文消息映射到椭圆曲线上的点，然后使用公钥进行加密。解密过程则需要使用私钥。

在仪表自动化系统中，实时监测数据的安全传输尤为关键。采用ECC算法，实现数据的加密和解密。考虑到实时数据的敏感性和传输效率的要求，ECC提供了一种既安全又高效的解决方案。对于每个数据点 D ，加密过程表示为

$$E_D = D \cdot \text{PubKey} \quad (3)$$

式中， E_D 是加密后的数据； D 是原始数据点； PubKey 是接收方的公钥。

解密过程为

$$D = E_D \cdot \text{PrivKey}^{-1} \quad (4)$$

式中， PrivKey^{-1} 是发送方私钥的逆元，用于解密接收到的数据。

ECC算法还结合区块链技术中的智能合约来自动化数据的加密和解密过程，进一步增强仪表自动化系统中数据的安全性。智能合约编程以确保只有授权用户才能访问加密数据，同时还自动验证数据的完整性和来源，确保数据在整个传输过程中未被篡改^[3]。

在实现ECC加密算法时，还需考虑到计算效率和密钥管理。由于仪表自动化系统通常涉及大量数据的收集和传输，因此加密算法的计算效率尤为重要。ECC算法由于其较小的密钥尺寸相比于其他加密算法如RSA，在保持同等安全级别的同时，显著减少计算资源的消耗，使其成为实时监测数据加密的理想选择。

3. 访问控制机制

在区块链技术应用与仪表自动化数据可信传输中的访问控制机制方面，重点在于确保只有授权用户能够访问和操作数据。本部分将引入基于属性的加密（Attribute-Based Encryption, ABE）算法，这是一种高度灵活的加密方式，允许加密的数据根据用户的属性（角色、身份和权限等）来进行访问控制。ABE算法的核心思想是通过对数据进行加密，使得只有满足特定属性集合的用户才能解密。这一机制非常适合区块链环境，因为它利用区块链的不可篡改性和透明性来存储和验证用户属性，进而实现细粒度的访问控制^[4]。

ABE算法分为两种主要形式：密钥策略ABE（Key-Policy ABE, KP-ABE）和密文策略ABE（Ciphertext-Policy ABE, CP-ABE）。本文将主要讨论CP-ABE算法，因为它允许加密者定义哪些用户属性解密数据，这与区块链环境中的访问控制需求高度吻合。

CP-ABE的加密过程表示为

$$E_{\text{data}} = \text{Encrypt}_{\text{CP-ABE}}(\text{data}, A) \quad (5)$$

式中， E_{data} 为加密后的数据； data 是原始数据； A 是访问策略，定义了哪些属性集合解密数据。

解密过程则需要用户的私钥，该私钥是根据用户的属性生成的

$$\text{data} = \text{Decrypt}_{\text{CP-ABE}}(E_{\text{data}}, SK_{\text{user}}) \quad (6)$$

式中, SK_{user} 是基于用户属性生成的私钥。

只有当用户的属性满足 A 时, 解密函数才能成功恢复原始数据。

CP-ABE 的关键在于访问策略 A 的定义和实施。访问策略用访问控制树 (Access Control Tree, ACT) 来表示, 其中每个节点代表属性或属性组合的逻辑运算 (如 AND、OR、NOT), 叶节点代表具体的属性。简单的访问策略为

$$A = (\text{Role} = ?\text{Engineer} \text{ AND } \text{Department} = \text{"Maintenance"}) \text{ OR } (\text{Role} = \text{"Manager"}) \quad (7)$$

只有角色为“工程师”且部门为“维护”的用户, 或者角色为“经理”的用户, 才能解密数据。

在仪表自动化系统中, 这种细粒度的访问控制机制允许系统管理员精确地定义哪些数据由哪些用户访问, 从而既保护了数据的安全性, 也确保了数据的可用性。实时监测数据仅对维护部门的工程师和管理层开放, 而财务报告数据则仅对管理层和财务部门的员工开放。

通过结合 ABE 算法和区块链技术, 实现去中心化的访问控制系统, 其中用户的属性和访问权限安全地存储在区块链上, 而且由于区块链的不可篡改性, 属性和权限信息是可信的^[5]。使用 ABE 算法进行加密数据的安全不再依赖于传统的访问控制列表 (Access Control List, ACL) 或角色基础访问控制 (Role-Based Access Control, RBAC) 系统, 从而减少了中心化权限管理系统的需要, 降低了系统复杂性和管理成本。

数据测试

在进行基于区块链技术的仪表自动化数据安全与可信传输系统的功能测试中, 选取的数据集是专门为此次测试设计并模拟生成的, 目的在于确保测试环境的控制性和数据的适用性。这种方法允许测试的精确度和结果的可靠性得到保证。数据集由模拟脚本产生, 旨在模拟仪表自动化系统中生成的实时数据, 如温度、压力和流量等参数, 确保测试覆盖了系统中各类数据的处理需求, 见表 1。模拟数据的生成, 既考虑到了数据的多样性, 也保证了测试的全面性和深入性。

测试指标包括响应时间、吞吐量、数据传输安

全性、系统稳定性和用户满意度。响应时间指系统处理请求和返回结果所需的时间; 吞吐量是指系统在单位时间内处理事务的数量; 数据传输安全性评估系统在数据传输过程中的安全性能; 系统稳定性评价系统运行的连续性和无故障时间; 用户满意度是基于模拟用户对系统易用性和性能的评分。

表1 数据集

测试编号	响应时间/s	吞吐量/TPS	数据传输安全性	系统稳定性	用户满意度
1	0.56	25.34	通过	通过	4.32
2	0.48	30.12	通过	通过	4.78
3	0.63	20.98	通过	通过	4.56
4	0.52	27.45	通过	通过	4.89
5	0.59	22.67	通过	通过	4.67

结束语

综上所述, 通过综合运用密码学、分布式系统理论和自动化技术等多学科知识, 探索建立在区块链技术基础上的仪表自动化数据安全与可信传输模型, 旨在实现仪表自动化数据在采集、存储和传输过程中的高度安全性和可信度, 同时也为相关领域的研究者和实践者提供理论基础和技术指导。这一研究不仅能够促进区块链技术与仪表自动化领域的交叉融合和创新发展, 更能够为实现更加安全、高效的自动化系统运行提供坚实的技术支撑, 从而为社会经济的发展贡献力量。EA

(收稿日期: 2024-05-11)

参考文献

- [1] 权刚, 董飞宇. 煤化工企业仪表自动化设备的故障预防与维护[J]. 化工管理, 2023(35): 110-112.
- [2] 鲁霄. 论石油化工企业仪表自动化设备的故障维护[J]. 石化技术, 2023, 30(11): 258-260.
- [3] 林芹芹. 自动化仪表在电力系统的应用[J]. 中国设备工程, 2023(15): 210-212.
- [4] 张明杰, 邵旭, 王越. 仪表自动化在化工工业中的应用[J]. 现代工业经济和信息化, 2023, 13(4): 145-147.
- [5] 夏维军. 试析石油化工企业仪表自动化设备的故障维护措施[J]. 中国石油和化工标准与质量, 2023, 43(2): 36-38.