计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(8):75−85 [doi: 10.15888/j.cnki.csa.009188]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链的物联网设备自主管控方案①

邓　艳[1], 叶新荣[1], 余　斌[2,3], 罗慧宁[1]

[1](安徽师范大学 物理与电子信息学院, 芜湖 241002)
[2](中国科学院 合肥物质科学研究院, 合肥 230031)
[3](中国科学技术大学, 合肥 230026)
通信作者: 叶新荣, E-mail: shuchong@ahnu.edu.cn; 余　斌, E-mail: yub@hfcas.ac.cn

摘　要: 传统物联网设备管理系统可能存在隐私数据易泄露、设备运行情况难掌握、异常事件难追溯等痛点, 给个人、企业乃至社会层面都带来了不利影响. 针对以上问题, 本文设计了一种基于区块链的物联网设备自主管控及管控行为审计方案, 通过区块链存证技术将接入系统的设备信息锚定至区块链, 对设备全生命周期进行管理; 基于智能合约技术实现对物联网设备的数据采集、分析及远程管控的一体化自主管控流程; 最后, 结合区块链不可篡改和可追溯的特性对用户行为进行安全审计. 分析结果表明, 本方案具备安全性高、扩展性强等特点, 为构建物联网系统安全管理架构提供了思路.

关键词: 物联网; 区块链; 设备管理; 智能合约; 行为审计

引用格式: 邓艳,叶新荣,余斌,罗慧宁.基于区块链的物联网设备自主管控方案.计算机系统应用,2023,32(8):75–85. http://www.c-s-a.org.cn/1003-3254/9188.html

Blockchain-based Autonomous Management Scheme for IoT Device

DENG Yan[1], YE Xin-Rong[1], YU Bin[2,3], LUO Hui-Ning[1]

[1](School of Physical and Electronic Information, Anhui Normal University, Wuhu 241002, China)
[2](Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, China)
[3](University of Science and Technology of China, Hefei 230026, China)

Abstract: The traditional IoT device management system may have drawbacks such as easy leakage of privacy data and difficulty in grasping the device operation conditions and tracing abnormal events, which poses adverse effects on individuals, enterprises, and even society. Given these problems, the study proposed a blockchain-based IoT device autonomous control and behavior audit scheme. Through blockchain deposition technology, the device information connected to the system is anchored to the blockchain to manage the whole life cycle of the device. Moreover, based on smart contract technology, the integrated autonomous control process including data collection, analysis, and remote control of IoT devices is realized. Finally, the scheme explores the untamperable and traceable features of blockchain to audit the users' behavior. The analysis results show that the proposed scheme has high security and strong scalability, which has the ability to build a security management architecture for the IoT systems.

Key words: Internet of Things (IoT); blockchain; equipment management; smart contract; behavior audit

近年来, 随着新一代物联网信息技术的深入发展和广泛应用, 国家加快推进智慧城市建设和数字化转型, 物联网安全建设已成为新型基础设施规划、建设、管理领域关注的重点. 目前, 对于物联网设备的管

① 基金项目: 国家自然科学基金 (62072005); 安徽省自然科学基金 (2108085Y22)
收稿时间: 2023-01-17; 修改时间: 2023-02-23; 采用时间: 2023-03-08; csa 在线出版时间: 2023-06-09
CNKI 网络首发时间: 2023-06-12

理, 存在诸多问题: 1) 存在大量的设备弱口令及密码共享现象, 系统缺乏完备的安全防护手段. 2) 物联网系统各种设备产生的大量安全信息使管理员难以快速响应. 3) 系统在用户授权管理上存在漏洞, 容易出现越权访问的现象. 4) 系统的日志数据分散[1]. 以上问题导致在物联网系统中终端设备安全无法得到保障.

区块链技术是一种通过自身分布式节点进行网络数据的存储、验证、传递和交流的去中心化的分布式技术, 其底层技术框架具有普适性, 应用于物联网领域, 在横向上能够优化产业链结构、纵向上链接物联网设备与互联网技术设备, 基于其弱中心化、分布式存储、多方共识等特性加强物联网网络的安全性和扩展性[2–7].

针对物联网安全的管理, 有学者提出基于区块链的物联网管理系统方案. Huh 等人[8] 提出了一种基于以太坊进行物联网设备管理的方案, 基于智能合约构建密钥管理系统, 通过智能合约保存来自终端设备的数据. Novo[9] 设计了一种基于区块链的分布式物联网访问控制系统架构, 该方案在单个智能合约中运行, 减少了节点间的通信开销. Loukil 等人[10] 提出一种基于区块链的隐私保护物联网设备管理方法, 利用智能合约加强对数据所有者的隐私保护. Soewito 等人[11] 提出一种利用加密算法和零知识证明加强物联网数据安全传输的方法, 保障系统安全的同时降低数据传输的延迟. Kandah 等人[12] 提出一种基于区块链的信任管理机制, 通过构建可信物联网环境来保障节点安全. Hwang 等人[13] 提出一种动态的物联网设备访问控制方法, 通过区块链技术实现系统的高可靠性和可扩展性. Alblooshi 等人[14] 提出一种基于智能合约的医疗设备管理方法, 实现对医疗设备数据的可信管理和对患者的隐私保护. 赵明慧等人[15] 提出了一种基于区块链的社会物联网可信服务管理框架, 基于区块链去中心化的特性建立信任关系. 任彦冰等人[16] 提出一种分布式的物联网信任数据管理方法, 利用区块链与风险理论实现对分布式物联网内实体的信任管理. 王继业等人[17] 设计了一种基于区块链的数据安全共享体系, 为企业搭建安全可信的数据共享网络环境.

以上基于区块链的物联网设备管理方案, 利用智能合约对物联网设备进行管理, 在一定程度上提高了对物联网设备的访问控制安全性, 加强了对系统数据的隐私保护, 但针对物联网设备从出厂、入网到维护、撤销等流程的全生命周期管理未提出有效的解决方案. 基于以上问题, 本文设计并实现了一种基于区块链的物联网设备自主管控及管控行为审计方案. 通过将接入系统的物联网设备信息上链, 并将系统用户对接入设备的操作权限写入智能合约, 实现对设备的统一管理; 并且利用智能合约技术实现对设备的远程运维管理, 运维人员可远程对设备进行运维操作, 有效提高设备的安全性; 最后将对设备的管控行为上链存证, 对操作过程中的不规范或篡改等异常行为进行告警, 完善因系统人员操作不当触发的追责环节.

1 总体方案

1.1 系统架构

如图 1 所示, 本文设计的物联网设备自主管控系统主要由设备层、数据层、核心链层、业务服务层和用户层构成.

用户层为系统内不同角色用户提供相应服务, 其中用户角色包括设备所属者、设备使用者、设备生产商、管理运维人员及其他用户, 系统提供多终端的访问方式, 包括移动终端、PC 端等; 同时向用户提供数据可视化功能, 用户通过信息显示屏、电视大屏等数据可视化平台对资产设备的运行情况进行实时监控.

业务服务层主要向系统管理人员和运维人员提供设备的全生命周期管理服务, 包括设备信息存证、设备自主管控、身份权限管理、日志分布存储和行为安全审计功能. 其中, 设备信息存证是将接入系统的设备关键信息上链管理, 包括设备出厂后的设备静态信息、安装位置、使用参数、维修和配件更新信息等; 设备自主管控包括对设备的可信数据采集与传输以及设备的远程控制和运维; 身份权限管理基于区块链的分布式身份管理和权限控制策略针对系统内不同的角色进行权限的分配, 避免用户因权限控制的缺失而出现操作不当、数据泄露问题; 日志分布存储服务对系统日志及设备日志进行集中采集后存储至分布式存储系统中, 在统一管理的基础上对数据整合分析; 行为审计功能提供对日志数据的安全分析, 对用户的异常行为进行追溯追责, 同时针对用户操作及设备运行情况进行合规性审计. 另外服务层提供对区块链和数据层的数据存取的交互, 数据接口服务对接应用层发送的服务请求, 并对传输的数据进行核验与封装, 通过接口与区块链交互; 共享交换服务实现了系统数据的实时

更新, 保证系统中数据与设备实时信息的一致性和同步性; 分布式存储备份服务为系统数据提供多节点的备份存储, 提高数据存储效率的同时也加强了系统的数据安全和隐私保护.

核心链层作为底层技术核心, 包括分布式数据存储、P2P 网络、智能合约、共识算法、加密算法等关键技术, 系统核心业务通过区块链智能合约执行, 并广播全网共识. 利用区块链的验证和共识机制识别非合法节点, 避免恶意设备的接入, 同时基于加密算法与数字签名保证重要数据的数据安全.

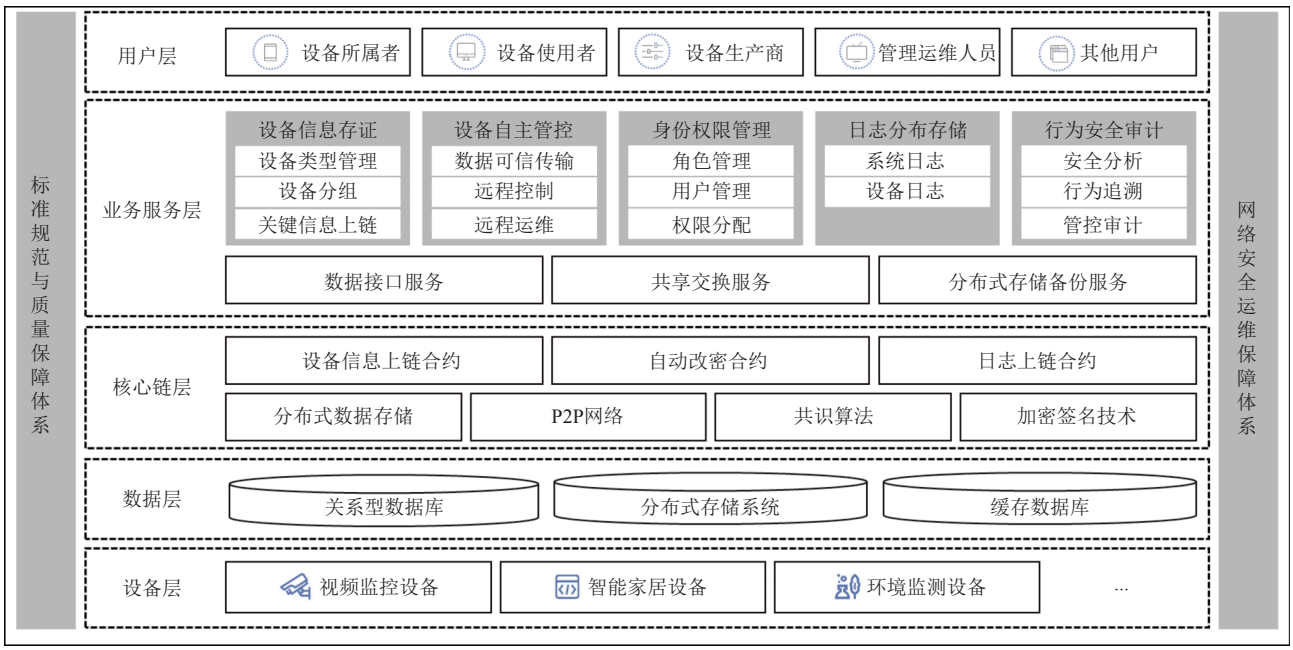

图 1 物联网设备自主管控系统架构

数据层主要为系统数据提供存储功能. 其中, 关系型数据库与分布式存储系统相结合存储系统数据, 并对重要数据存储上链, 本方案中分布式存储系统采用星际文件系统 (interplanetary file system, IPFS). 设备层包括视频监控设备、智能家居设备和环境监测设备等智能物联设备, 如网络摄像机 (IP camera, IPC)、电子锁、智能电视等智能物联网设备皆可接入系统进行统一的设备管理.

1.2 网络拓扑

系统的网络拓扑图如图 2 所示.

数据采集层将从智能物联设备采集到的数据传输至数据采集控制器, 控制器通过现有的互联网、专网或局域网基础网络设施将数据上传至数据库, 并上链存证. 区块链节点服务器部署区块链节点程序, 并组建 P2P 网络, 完成联盟链的搭建. 其中区块链节点包括区块链轻节点与区块链全节点, 区块链轻节点数量较多, 但其只存储最小量的状态数据, 即只存储某一设备的部分数据, 且不会保持随时在线; 而区块链全节点同步所有的区块链数据, 即使部分节点出现问题, 也不会影响整个区块链网络的安全性. 用户可通过移动端或 PC 电脑端访问部署在应用服务器的基于区块链的物联网设备自主管控系统.

2 核心业务设计

本方案主要为实现物联网设备的全生命周期智能化管理, 具体包括前期管理模块、自主管控模块和行为审计模块. 设备全生命周期管理示意图如图 3 所示.

图 3 中, 入网管理模块包括设备静态信息上链、安装调试、维修及配件更新和操作权限设置功能; 自主管控模块包括数据采集、设备控制和运维管理功能; 行为审计模块包括操作行为上链和异常行为预警功能. 通过以上 3 个模块形成从设备管理、管控到行为审计的闭环.

2.1 设备入网管理

设备入网管理模块是将设备的静态信息写入区块链的过程, 物联网设备的产品序列号 (serial number,

SN) 与物联网平台设备证书之间存在一对一的映射关系, 本方案使用 SN 码为认证信息, 由系统管理员使用智能合约将设备的静态信息写入区块链. 并且在将设备信息上链的同时, 将用户对设备的操作权限设置也写入智能合约, 实现用户操作权限的精确分配. 设备信息上链的流程图如图 4 所示.

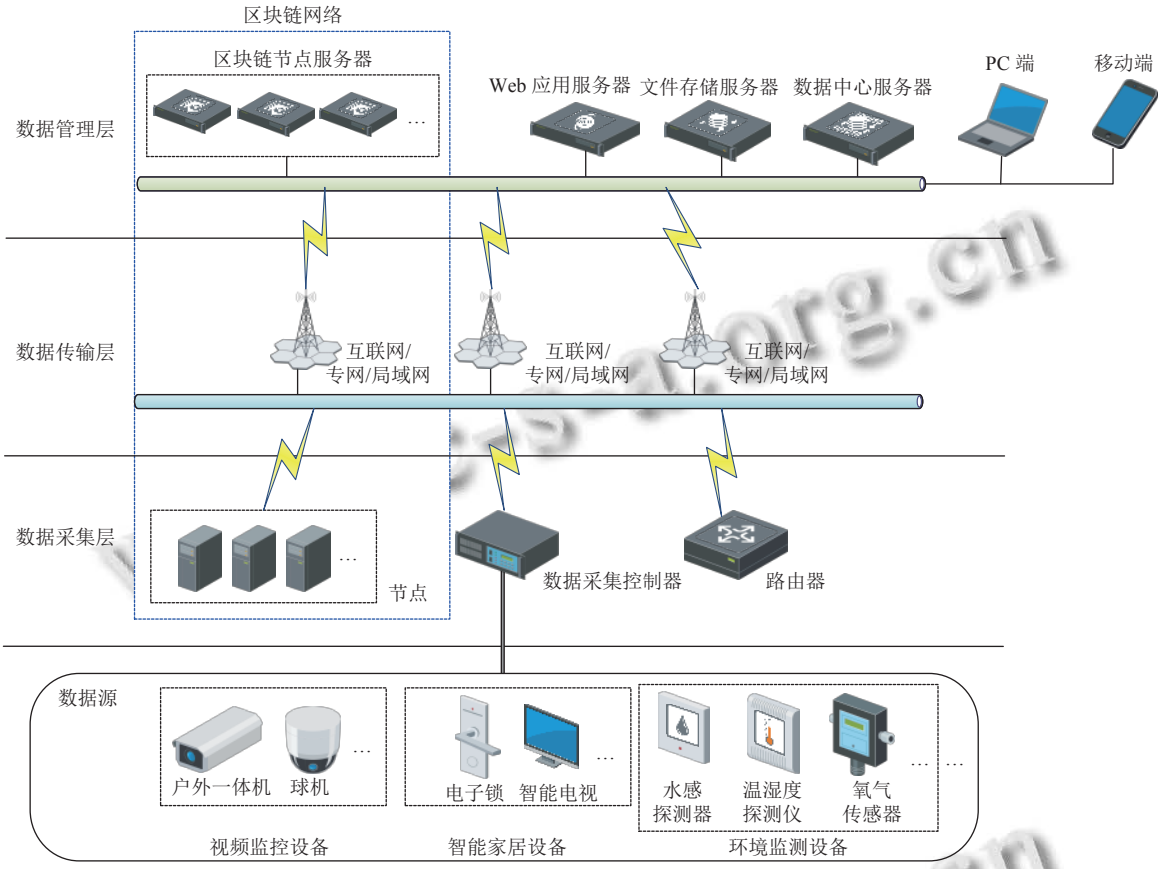

图 2 系统网络拓扑图

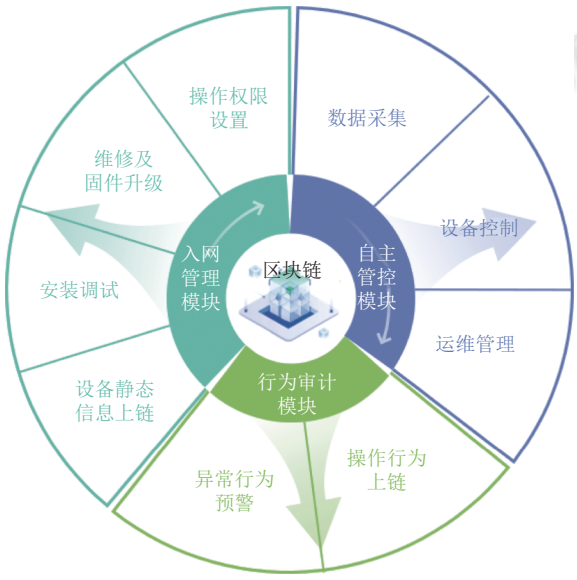

图 3 设备全生命周期管理示意图

如图 4 所示, 管理员将设备的 SN 码与静态信息上传, 传输至数据接口服务, 服务首先将设备信息写入文件并存储至 IPFS, IPFS 返回文件哈希后, 数据接口服务摘取设备信息数据中的关键信息, 调用设备信息上链合约将此关键信息与 IPFS 返回的文件哈希一同上传至区块链, 信息成功上链后数据接口服务将文件哈希与静态信息存储至数据库. 此流程的具体过程如算法 1 所示.

如算法 1 所示, 设备 SN 码 *SNnumber* 和设备静态信息 *StaticInfo* 发送到数据接口服务中, 数据接口服务将 *SNnumber* 和 *StaticInfo* 制成文件 *InfoEntity*, 存储至 IPFS 并获得其文件哈希 $Hash_e$. 另外从设备静态信息 *StaticInfo* 中摘取部分关键信息 *KeyInfo*, 如设备名称、设备类型、IP 地址等信息, 将文件哈希 $Hash_e$ 与关键信息 *KeyInfo* 一同上链存储, 同时将 $Hash_e$ 与设备静态信息 *StaticInfo* 存入数据库.

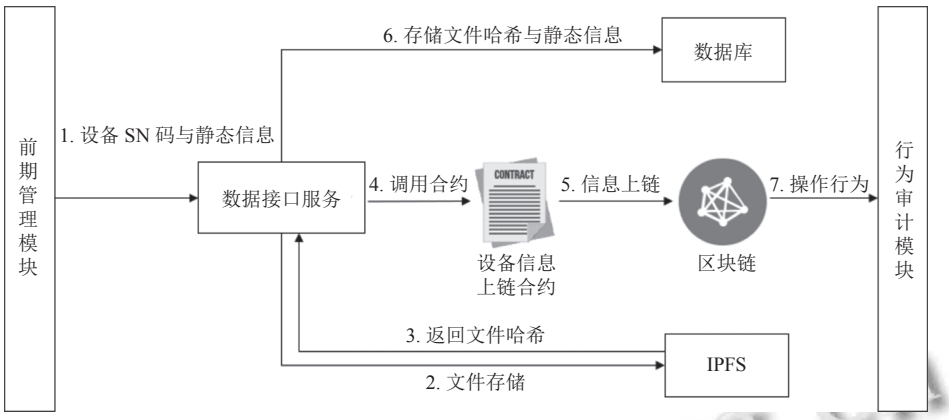

图 4 设备信息上链示意图

算法 1. 设备信息上链算法

输入: *SNnumber* (设备 SN 码), *StaticInfo* (设备静态信息)
输出: $Hash_e$ (文件哈希)

```
1. Procedure ManageEquipment(SNnumber, StaticInfo)
   //将设备信息写入文件
2. InfoEntity = MakeFile(SNnumber, StaticInfo)
   //将文件写入 IPFS 并返回其地址信息
3. FileAddr = SaveToIPFS(InfoEntity)
   //计算文件哈希
4. Hash_e = SHA256(InfoEntity, FileAddr)
   //从设备静态信息中摘取关键信息
5. KeyInfo = ConstructKeyInfo(StaticInfo)
   //将文件哈希与关键信息存储上链
6. Result = UpdataToBlockChain(Hash_e, KeyInfo)
   //将文件哈希和设备静态信息存储至数据库
7. if Check(Result) = true then
      StoreToDataBase(Hash_e, StaticInfo)
      //返回文件哈希
8.    return Hash_e
9. end if
10. end procedure
```

2.2 一体化自主管控

设备一体化自主管控是围绕设备的数据采集、远程控制和远程运维, 实现一体化的设备管控, 具体过程如图 5 所示.

(1) 全域可信数据采集

管理员按照设备实际工作情况制定数据采集策略和规范, 包括数据采集周期及数据的采集类型、采集方式和采集范围, 由系统数据采集层的数据采集控制器通过数据接口与在线设备的通信接口连接, 实时采集在线设备的使用数据和设备状态, 最后将采集到的数据传输到数据中心进行分析处理, 并对序列化处理后的数据进行分布式存储, 实现对设备实时运行状态数据的记录存储.

(2) 设备远程控制

基于知识库对设备当前的状态数据进行数据分析, 分析需要进行的设备控制动作, 将远程控制命令发送到数据采集控制器中的控制单元, 由控制单元执行命令, 控制在线设备完成相应指定动作, 同时将该控制命令与操作记录同步至区块链, 即时保存整个操作过程.

(3) 设备远程运维

将设备各部件运行的状态数据与设备正常运行参数进行对比, 分析设备当前的运行状态是否存在异常, 并预判设备可能发生的故障, 提前介入维护. 为规范运维操作、实现有据可依, 系统以屏幕录像的形式对运维人员的运维操作过程进行全面追踪和记录, 当远程操控完成, 视频录制结束后, 屏幕录像文件将自动保存并同步计算已保全视频的哈希值, 形成一个包含视频文件及相关操作日志信息的证据包上传至 IPFS 进行存证.

2.3 设备管控行为审计

设备管控行为审计是通过对各类日志信息进行统一采集后进行安全分析、行为追溯和行为合规性审计等操作, 如图 6 所示. 系统采集安全设备的运行日志和系统用户的操作日志, 并将采集到的原始日志数据文件上传至 IPFS 保存, 同时对采集到的不同类型的用户行为数据进行分类并解析形成统一格式的标准化数据, 在将其写入关系型数据库的同时与 IPFS 返回的文件哈希一同通过日志上链合约上传至区块链.

(1) 安全分析

安全分析是通过对日志信息进行关联分析判断是

否存在安全问题. 经过预处理后的日志数据进入分析模块, 依据分析策略和关联分析算法对解析后的标准化数据进行关联分析, 辨别其中的危险信息, 划分为安全事件. 对具有安全风险的的安全事件依据不同的危险等级生成告警信息, 通过多种通知方式向用户发出告警, 及时规避安全风险.

(2) 行为追溯

行为审计可以近实时地记录并存储系统的操作日志, 并使用图表、数据列表等方式进行直观展示, 超级管理员可以对平台中所有资产设备产生的日志进行实时查看和对其他用户的操作行为进行实时查看和监控, 当发现异常事件时, 能够通过查询区块链上的操作记录快速定位问题.

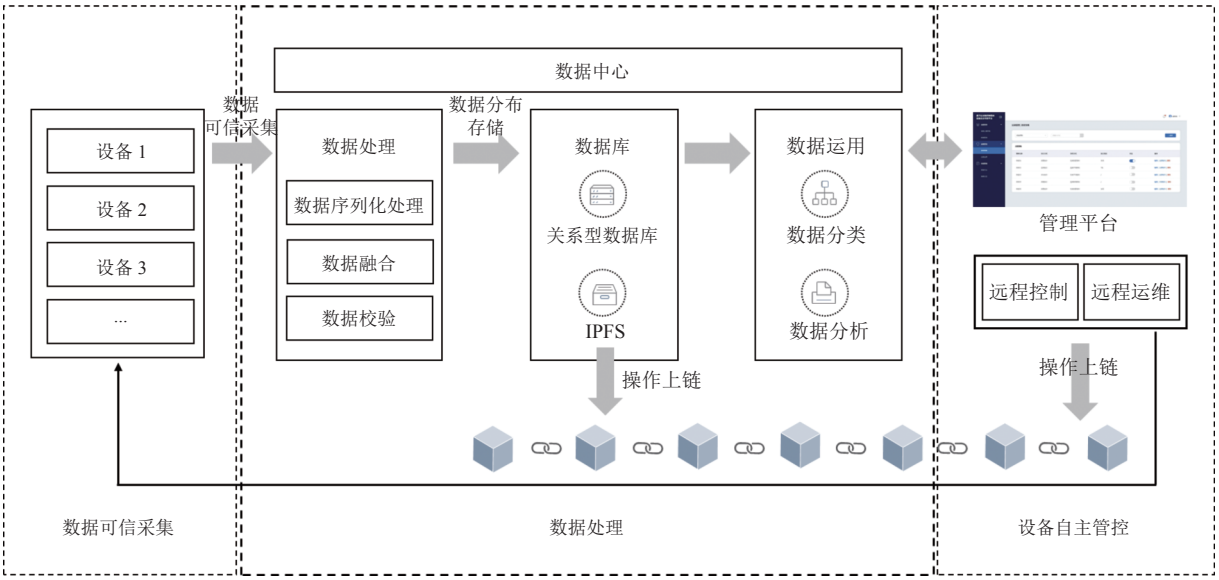

图 5 设备一体化自主管控示意图

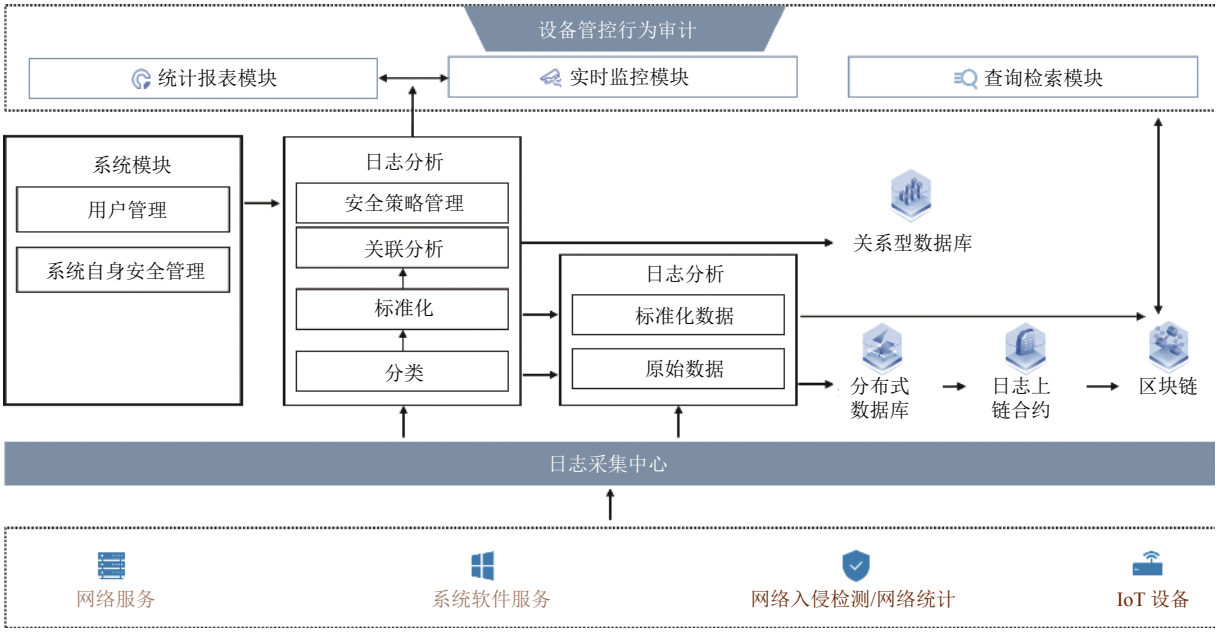

图 6 设备管控行为审计示意图

(3) 管控审计

基于日志服务提供查询、分析、告警、报表等下游计算能力. 根据审计管理员设置的安全审计策略, 对用户的操作行为、用户在不同设备上花费的时间和工

作量以及不同设备的使用情况等进行分析, 审计用户操作行为的合规性并评估设备的运行状况, 同时统计设备运行过程中故障发生时间、故障发生次数、有效的工作时间等关键参数, 以便运维人员制定改进措施, 提升设备整体的稳定性与安全性.

3 实现与分析

3.1 原型系统实现

基于本文提出的物联网设备自主管控及管控行为审计方案, 以 IPC 设备为例, 研发了基于区块链的 IPC 管理平台, 其中, 数据存储层采用 MySQL 和 Redis, 涉及 IPC 设备的具体信息及设备管控行为原始数据则存放在 IPFS 私有集群中; 区块链方面采用以太坊搭建联盟链, 指定联盟链节点共识为 POA (proof of authority); 服务层方面, 以 Node.js 为基础, 使用 Web3.js library 提供的 Web3 对象, 完成对智能合约的调用, 并使用 ipfs-api 调用 IPFS 私有集群.

(1) 设备上链管理

管理员输入设备的静态信息, 调用设备信息上链合约, 实现设备的上链管理, 如图 7 所示. 物联网设备上链信息如图 8 所示, 用户可通过设备名称、SN 码对设备信息进行精确查询.

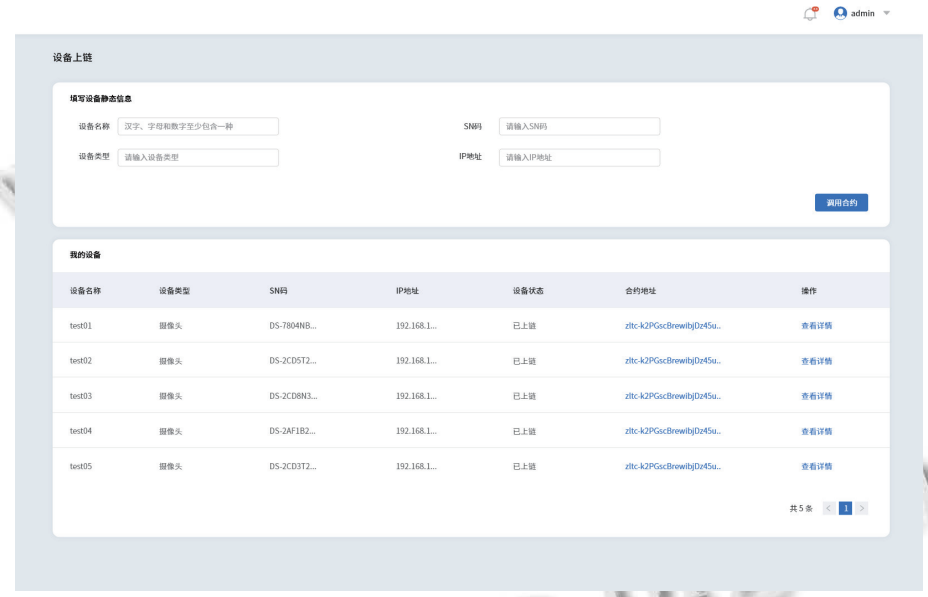

图 7 设备上链示意图

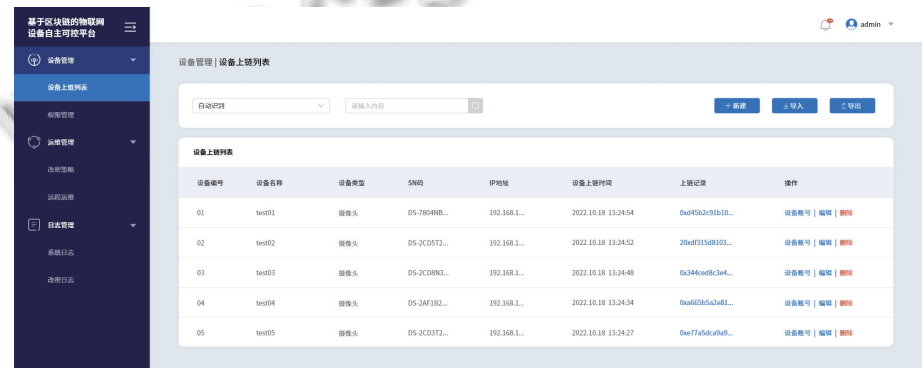

图 8 设备上链管理系统界面图

通过将物联网设备终端可信上链, 使实体设备完成云链化升级, 获得链上的可信身份标识, 设备资产相关数据同步传输到区块链上, 管理方能够对实物资产进行实时监控、分析和协同.

(2) 改密策略

运维人员可远程对设备进行管控, 以远程改密为例, 系统改密策略管理如图 9 所示, 可以通过打开已创建的策略, 或新建改密策略对进行设备密码管理.

利用智能合约技术, 在设备运行过程中实现无干预的自动改密, 同时对改密策略中的密码长度、复杂度进行多维度定义, 提高设备安全性.

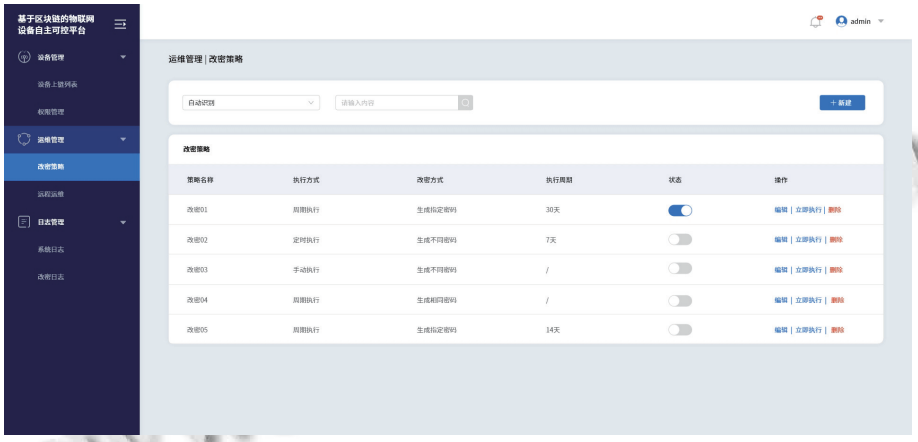

图 9 改密策略管理系统界面

(3) 日志管理

日志管理模块是系统的核心模块之一, 用于审计和管理用户对主机的访问操作的全部日志, 包括系统日志和改密日志. 系统日志功能可以查看系统运行的日志, 包括登录日志和操作日志, 如图 10 所示; 改密日志用于查看改密操作日志, 如图 11 所示.

改密日志为改密策略执行后产生的日志, 在搜索框中输入关键字, 可根据策略名称快速查询改密日志、查看改密详情, 日志内容包括基本信息、改密结果、上链记录等信息.

(4) 异常告警

当系统中出现异常事件时, 会触发异常告警功能, 告警方式包含: 消息、邮件、短信这 3 类告警方式; 告警等级分为: 高、中、低这 3 个不同等级, 如图 12 所示; 告警信息包括异常事件的发生时间、报警类型、设定值和报警值等, 如图 13 所示.

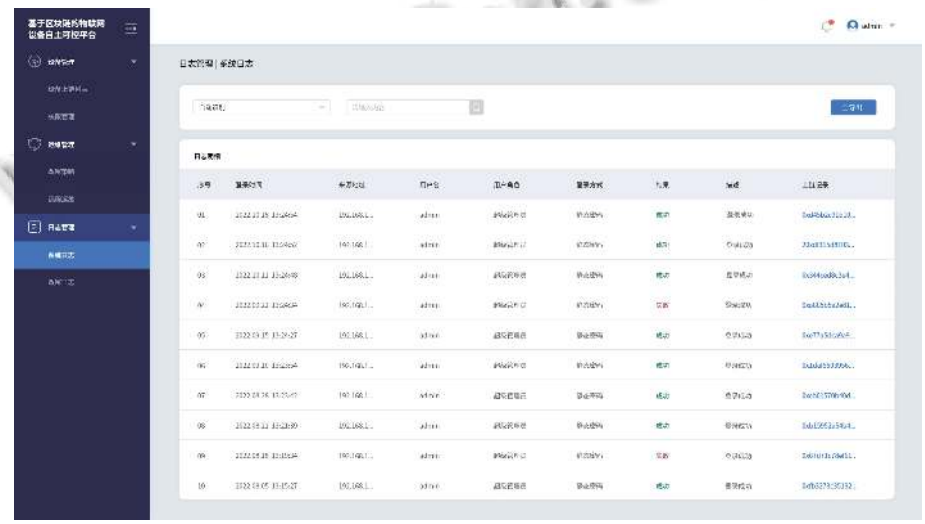

图 10 系统日志界面

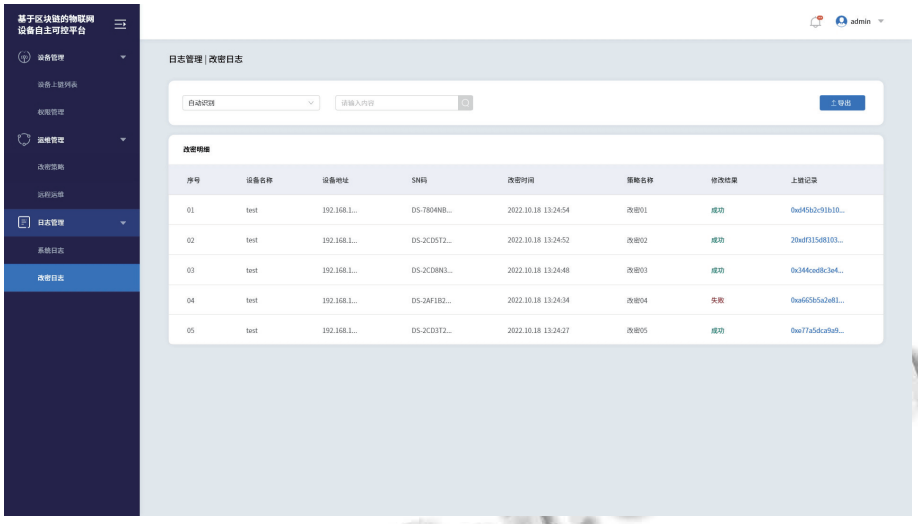

图 11 改密日志界面

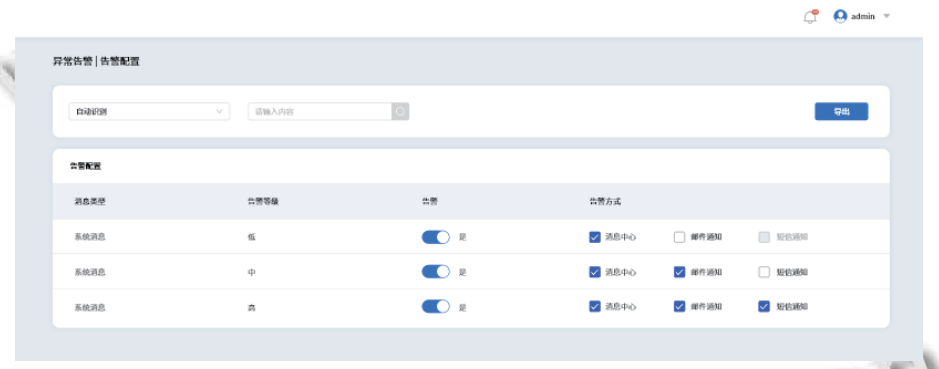

图 12 告警配置界面

图 13 告警信息界面

3.2 扩展性分析

本方案采用开放的系统架构, 在后期的系统设备扩展及数据存储方面都具有良好的可扩展性.

(1) 设备扩展

区块链能够快速处理交易并协调大量连接设备, 随着互联设备数量的增加, 分布式账本技术提供可行的解决方案, 支持物联网海量设备扩展, 助力构建高效、安全的分布式物联网网络[18]. 同时系统支持通过多种协议对不同设备进行监控, 并提供设备类型扩展功能, 通过配置可继续增加可管控的设备类型. 本方案

原型系统的实现以 IPC 设备为例, 在实际应用中具备互联能力的物联网设备皆可上链管理.

(2) 数据存储扩展

本方案采用链上链下协同存储方式, 将非结构化数据由区块链网络节点本地存储空间转移存储至链下分布式存储系统 IPFS 中, 节点本地存储空间仅存储 IPFS 所返回的文件哈希, 此哈希值作为访问文件的索引, 同时可以检验文件内容是否被篡改; 对于结构化数据, 正常数据仍采用哈希上链的方式, 异常数据则直接全部上链, 便于后续的异常事件溯源.

通过结合区块链技术与链下分布式存储系统各自的优势, 在保证数据安全性的同时, 减少了区块链网络中数据所占内存, 减轻系统的存储压力, 有效提高数据存储的扩展性.

3.3 安全性分析

(1) 设备使用的安全性

通过将区块链技术引入物联网设备管理领域, 对物联网设备全生命周期的使用进行管控, 实现对物联网设备的数据安全保护和对用户的隐私保护, 为用户提供更安全的物联网服务; 通过将管理及运维人员的管控行为进行可信审计, 对于异常事件可一键追溯, 快速定位追责, 提高系统的安全性和可信性.

(2) 数据安全性

系统数据存储在分布式的链式结构中, 确保了数据的多重备份, 提高数据库的容错性和安全性. 同时运用非对称加密、哈希算法等技术也加大了试图篡改、删除数据或者恶意攻击数据库等行为的难度和成本, 从而保证链上数据的真实性、完整性、隐私性和安全性.

(3) 数据全域可信

对于设备运行过程中产生的结构化数据、非结构化数据及日志数据等皆在链上进行管理, 基于区块链去中心化、分布式记账、加密可溯源等特点, 保证数据的真实性和完整性, 实现数据的全域可信.

3.4 对比分析

基于对物联网设备管理的安全性需求, 应选择具备去中心化、可溯源的高安全性术, 目前主流的设备管理方案包括软件即服务 (software as a service, SaaS) 系统架构及单机系统架构. 其中, SaaS 系统是一种由第三方服务提供商集中化托管软件应用程序的软件应用程序交付方式; 单机系统指所有业务集成在一台服务器上的系统. 将本方案与 SaaS 平台及单机系统进行比较, 从能否自主管控、系统的管理方式、存储方式、行为溯源以及扩展性和安全性几个方面进行了对比分析, 结果如表 1 所示.

表 1 设备管理方案对比分析

特性	SaaS系统架构	单机系统架构	本方案
自主管控	×	√	√
去中心化管理	×	×	√
分布存储	×	×	√
行为溯源	×	×	√
扩展性	√	×	√
安全性	×	×	√

SaaS 系统采用中心化的管理架构, 用户可操作的自定义控制权有限, 数据皆存放在第三方服务商的服务器上, 中心化存储随之带来的数据安全问题仍需考虑; 单机管理架构的所有服务由一台服务器提供, 其处理能力有限, 当业务增长到一定程度, 单机的硬件资源将无法满足业务需求, 系统扩展性差, 且任何一个模块的错误均可造成整个系统的崩溃; 对比以上两种系统架构, 本方案基于区块链技术设计的分布式管理架构, 为用户打造设备全生命周期的自主管控服务, 能够兼顾安全性、扩展性及行为溯源需求, 具有优势性.

4 结语

本文设计并实现了一种基于区块链的物联网设备自主管控及管控审计方案. 首先, 提出物联网设备一体化自主管控、审计模型, 实现对入网设备的全生命周期管理; 其次, 实现设备拥有者对设备的自主可控, 并对多个物联网统一入口进行管控; 另外, 基于智能合约与 IFPS 等技术对管控行为进行上链存证, 实现对用户管控行为的追溯与审计. 分析结果表明, 本方案基于区块链技术实现了设备的安全自主管控, 保障了设备管控过程中数据安全性和隐私性, 有效提高了设备的安全性.

参考文献

1 吕建富, 赖英旭, 刘静. 基于链上链下相结合的日志安全存储与检索. 计算机科学, 2020, 47(3): 298–303. [doi: 10.11896/jsjkx.190200298]

2 Liu BQ. Overview of the basic principles of blockchain. Proceedings of the 2021 International Conference on Intelligent Computing, Automation and Applications

(ICAA). Nanjing: IEEE, 2021. 588–593. [doi: 10.1109/ICAA53760.2021.00108]
3 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展. 计算机学报, 2018, 41(5): 969–988. [doi: 10.11897/SP.J.1016.2018.00969]
4 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]
5 代闯闯, 栾海晶, 杨雪莹, 等. 区块链技术研究综述. 计算机科学, 2021, 48(S2): 500–508. [doi: 10.11896/jsjkx.201200163]
6 白翔, 许从方, 柳兴, 等. 区块链物联网安全技术综述及关键技术分析. 信息技术, 2022, 46(10): 24–30, 40. [doi: 10.13274/j.cnki.hdzj.2022.10.005]
7 张杰, 许姗姗, 袁凌云. 基于区块链与边缘计算的物联网访问控制模型. 计算机应用, 2022, 42(7): 2104–2111. [doi: 10.11772/j.issn.1001-9081.2021040626]
8 Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform. Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT). PyeongChang: IEEE, 2017. 464–467. [doi: 10.23919/ICACT.2017.7890132]
9 Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 2018, 5(2): 1184–1195. [doi: 10.1109/JIOT.2018.2812239]
10 Loukil F, Ghedira-Guegan C, Boukadi K, *et al*. Data privacy based on IoT device behavior control using blockchain. ACM Transactions on Internet Technology, 2021, 21(1): 23.
11 Soewito B, Marcellinus Y. IoT security system with modified zero knowledge proof algorithm for authentication. Egyptian Informatics Journal, 2021, 22(3): 269–276. [doi: 10.1016/j.eij.2020.10.001]
12 Kandah F, Huber B, Skjellum A, *et al*. A blockchain-based trust management approach for connected autonomous vehicles in smart cities. Proceedings of the 9th IEEE Annual Computing and Communication Workshop and Conference (CCWC). Las Vegas: IEEE, 2019. 544–549. [doi: 10.1109/CCWC.2019.8666505]
13 Hwang D, Choi J, Kim KH. Dynamic access control scheme for IoT devices using blockchain. Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC). Jeju: IEEE, 2018. 713–715. [doi: 10.1109/ICTC.2018.8539659]
14 Alblooshi M, Salah K, Alhammadi Y. Blockchain-based ownership management for medical IoT (MIoT) devices. Proceedings of the 2018 International Conference on Innovations in Information Technology (IIT). Al Ain: IEEE, 2018. 151–156. [doi: 10.1109/INNOVATIONS.2018.8606032]
15 赵明慧, 张琭, 亓晋. 基于区块链的社会物联网可信服务管理框架. 电信科学, 2017, 33(10): 19–25. [doi: 10.11959/j.issn.1000-0801.2017274]
16 任彦冰, 李兴华, 刘海, 等. 基于区块链的分布式物联网信任管理方法研究. 计算机研究与发展, 2018, 55(7): 1462–1478. [doi: 10.7544/issn1000-1239.2018.20180073]
17 王继业, 高灵超, 董爱强, 等. 基于区块链的数据安全共享网络体系研究. 计算机研究与发展, 2017, 54(4): 742–749. [doi: 10.7544/issn1000-1239.2017.20160991]
18 陈要伟. 区块链在物联网安全中的应用研究. 产业与科技论坛, 2020, 19(22): 57–58. [doi: 10.3969/j.issn.1673-5641.2020.22.026]

(校对责编: 牛欣悦)