# 基于区块链的鸿蒙物联网数据可信存储研究与应用

梅常鹏[1],汪显顺[1],林重汕[1],刘秀英[1],张子卉[2]
(1. 东华理工大学 软件学院,江西 南昌 330013;
2. 海口经济学院 腾竞依智网络学院,海南 海口 570100)

**摘　要**:随着当今物联网生态系统的快速发展,鸿蒙物联网已经在智能家居、智能交通、智能医疗和智能制造等领域得到了广泛应用和探索。如何安全可靠地存储设备数据成为了需要解决的一个问题。针对目前传统鸿蒙物联网行业的中心化数据存储模式可能存在的单点故障、存储中心化和设备数据易于泄露等问题,根据区块链技术的去中心化、加密性和不可篡改属性,该文提出了一种基于 Hyperledger Fabric 框架,结合非对称加密算法、智能合约、星际文件系统(IPFS)和开源鸿蒙系统,采用链上链下双路存储的模式,用于大规模数据存储,以实现鸿蒙物联网数据可信存储。通过系统分析和实验测试,该方案能满足鸿蒙物联网数据安全存储和可追溯性的需求,提高了鸿蒙物联网生态系统整体的安全性和可靠性。

**关键词**:鸿蒙物联网;区块链技术;去中心化;密码学;资源存储;信息安全;数据完整性
**中图分类号**:TP311.1　　**文献标识码**:A　　**文章编号**:1673-629X(2025)06-0070-07
doi:10.20165/j.cnki.ISSN1673-629X.2025.0006

# Research and Application of Trusted Storage of HarmonyOS IoT Data Based on Blockchain

MEI Chang-peng[1], WANG Xian-shun[1], LIN Chong-shan[1], LIU Xiu-ying[1], ZHANG Zi-hui[2]
(1. School of Software, EAST China University of Technology, Nanchang 330013, China;
2. Tengjing Yizhi Network College, Haikou University of Economics, Haikou 570100, China)

**Abstract**: With the rapid development of today's IoT ecosystem, HarmonyOS IoT has been widely used and explored in the fields of smart home, smart transportation, smart healthcare, and smart manufacturing. How to store device data safely and reliably has become a problem that needs to be solved. In view of the problems that may exist in the centralized data storage mode of the traditional HarmonyOS IoT industry, such as single point of failure, storage centralization and easy leakage of device data, according to the decentralization, encryption and tamper-proof attributes of blockchain technology, we propose a framework based on Hyperledger Fabric. Combining asymmetric encryption algorithms, smart contracts, interplanetary file systems (IPFS) and open source HarmonyOS systems, the mode of on-chain and off-chain dual-socket storage is used for large-scale data storage to achieve trusted storage of HarmonyOS IoT data. Through system analysis and experimental testing, the proposed solution can meet the needs of secure storage and traceability of HarmonyOS IoT data, and improve the overall security and reliability of the HarmonyOS IoT ecosystem.

**Key words**: HarmonyOS Internet of Things; blockchain technology; decentralization; cryptology; resource storage; information security; data integrity

## 0　引　言

物联网[1](Internet of Things, IoT)是指通过互联网连接各种物理设备,物联网技术已经被广泛应用于各个领域,如智能家居[2]、智能交通[3]、物流[4]、医疗保健等[5]。目前,物联网已经成为了全球范围内一个快速发展的领域,根据预测,到 2025 年物联网设备将超过 1 000 亿台[6],它正在改变着人们的生活和工作方式。鸿蒙物联网(HarmonyOS IoT)是指由华为推出的基于鸿蒙操作系统的物联网生态系统,旨在实现设备之间的无缝连接和协同工作[7]。鸿蒙物联网数据也随着设备的增多和生态系统的扩展,以指数级的速度逐年增长。如何安全可靠地处理数据成为了需要解决

**收稿日期**:2024-10-16　　**修回日期**:2025-02-18
**基金项目**:江西省网络空间安全智能感知重点实验室开放基金(JKLCIP202205)
**作者简介**:梅常鹏(1998-),男,硕士研究生,通讯作者,研究方向为物联网、区块链。

的一个问题,如果这些隐私数据遭受攻击,会给用户带来潜在的安全问题,造成不必要的经济损失[8]。

当面对存储体量大、结构多样化的鸿蒙物联网数据,如何确保它们的数据安全是该文的主要研究目的。该方案采用存储方法中的基于星际文件系统(InterPlanetary File System,IPFS)和区块链分布式存储架构[9]的数据存储方法,提出基于区块链结合 IPFS 的鸿蒙物联网数据可信存储方案。该方案主要解决的问题有两个:第一,如何使用区块链和 IPFS 技术来保证鸿蒙物联网数据的可信存储,防止其被篡改和攻击;第二,去中心化的架构下,数据以何种方式存储在什么地方,才能确保数据的完整性和可用性。

针对以上两个问题,该方案基于 IPFS 技术的分布式存储和基于内容寻址的特性,将原始数据存储至 IPFS 网络中,将返回数据的内容标识符(CID),即数据的哈希值,一旦上传至 IPFS 网络后其哈希值就固定不变,除非所有节点删除该文件,否则无法轻易移除或修改。数据的哈希值作为唯一标识,确保了内容的不可篡改性,从而实现数据的完整性和可用性,并且将原始数据存储在 IPFS 网络中的存储地址使用非对称加密算法进行加密,将加密后的数据存储地址上传至区块链网络中,由于区块链新区块一旦上链确认后将无法修改的特性,进一步保证其安全性。因数据存储地址使用了非对称加密算法和区块链技术,攻击者无法获得解密的私钥和篡改链上内容,使其安全性极高,很难被成为攻击的对象。

## 1　相关技术及现状分析

### 1.1　相关技术

区块链技术[10]最初在比特币应用,随着区块链技术的不断发展和完善,现在它被作为一种信任管理机制广泛应用于非数字货币领域中,来降低不可信环境中的信任成本,提高环境的可信程度。区块链作为一个分布式、协调性高和共享能力强的数据账本,可用于数据完整性保护[11]。区块链的本质是一个去中心化的分布式数据库[12],区块与区块之间通过哈希指针首尾相连从而构成整个区块链。每个区块包括区块头与区块体两部分,区块头主要包括父区块哈希值、版本号和 Merkle 根[13],区块体主要包括 Merkle 树记录的账本信息,即区块中的所有交易记录。

IPFS 是一个由社区开发的对等协议和网络[14],一个完全去中心化的和内容寻址的媒体对象存储和检索平台,采用基于信息的内容技术,而非位置,利用对信息进行定位,实现分布式存储的功能。IPFS 主要对存储的内容进行加密生成哈希地址,使得数据无法被改变。与传统 HTTP 协议相比,IPFS 传输速率更高,网络堵塞的发生情况也更低[15]。

哈希算法(Hash algorithm)是一种用于将任意长度的输入数据通过特定的数学函数转变为固定长度的数据输出的算法,通过散列算法,变换成固定长度的输出,该输出就是散列值。区块链中使用了哈希算法[16],因为区块链块头中使用哈希函数是单向的,只能输入信息得到哈希值,具有唯一性,所以区块链中新区块加入后,便无法更改,实现了区块链不可篡改的特性。

### 1.2　现状分析

当前鸿蒙物联网数据存储主要采用以下两种存储模式:集中式存储模式和分布式存储模式。这两种存储模式虽然方便快捷,但是却存在数据隐私泄露、数据篡改等信任问题,一旦该地点遭受攻击或产生数据泄露,可能会导致重要数据的安全受到威胁。

随着区块链技术的快速发展,区块链技术应用在各个方面,并且现在有越来越多研究工作开始将区块链技术应用在物联网数据存储中,区块链作为一种公用账本技术,具备去中心化、可追溯和难篡改等特性。利用区块链技术可以实现去中心化的数据存储,在没有单一的中心服务器情况下控制所有数据,提高了数据存储的安全性和可靠性。

IPFS 是通过 P2P 网络实现的对等分布式文件系统,IPFS 的核心概念是内容寻址,即根据文件的内容生成唯一的哈希值(IPFS Hash)作为文件的地址。这意味着无论文件在何处存储,只要内容不变,对应的哈希值也不会改变,因此可以确保文件的唯一性和完整性。IPFS 技术有着极为出色的数据存储与共享功能,而且可以和区块链高度融合。

根据当前鸿蒙物联网数据存储面对的问题,结合区块链和 IPFS 技术的特性,可以有效解决当前鸿蒙物联网数据存储中心化、数据篡改和安全性这类问题,结合区块链和 IPFS 两个技术去中心化、不可篡改性和持久性的特点,并且结合非对称加密算法,实现鸿蒙物联网数据的可信存储。

## 2　系统设计

### 2.1　系统架构设计

传统的 IPFS 与区块链结合的模型方案中存在四个部分,包括物联网设备、服务器、IPFS 网络和区块链网络。传统的 IPFS 和区块链结合的方案虽然可以将数据存储至 IPFS 网络中实现分布式存储,解决了数据单点故障和存储效率的问题,并且将文件存储在 IPFS 的地址进行上链操作,保证了数据存储地址的完整性,但是由于存储到区块链网络中的地址是公开透明的,所有人都可以查询,这就导致了数据存在泄露的风险,非

正常的用户可以下载数据存储地址,然后到 IPFS 网络中下载原始数据,数据的安全性就面临了严重的问题。

为了解决此问题,该方案在 IPFS 和区块链存储的基础上,提出了非对称加密技术,使用公私密钥对来对数据存储在 IPFS 网络中的地址进行加密,然后将加密后的数据存储地址进行上链存储。需要下载使用时,从区块链下载加密后的数据存储地址,使用私钥进行解密,这样不仅实现了数据的分布式存储,而且解决了数据泄露的问题,实现了数据的可信存储。

该方案采用的区块链系统为 Hperledger Fabric,主要包含两个模块——系统模块和工具模块。用于构架区块链数据传输网络,用于对鸿蒙物联网数据的传输加密,主要参与的节点有证书服务(CA)、背书节点(endorser peer)、提交节点(committer peer)和排序节点(order peer)。首先使用配置生成工具,生成区块链网络、创建通道和生成对等体,然后将链码进行安装实例化,实现数据的上传。在鸿蒙物联网数据区块链中,主要包含两个身份——用户和管理员,即拥有鸿蒙物联网设备的所有者和鸿蒙物联网生态系统管理员,一个身份在区块链网络中就对应一个对等体,这样就可以利用区块链的特性来对数据的上传和管理进行可信的操作。

该系统在配置完区块链和 IPFS 网络后,最终面向用户的为前端页面,所有交互功能均可在网页实现,可以将其作为模块化,集成至新的系统中,具有较高的兼容性,可应用于各类物联网平台。亦可在原有功能基础上,根据实际环境进一步开发相关配套功能,如基于属性的访问控制和基于角色的访问控制等功能。

基于 IPFS 和区块链的鸿蒙物联网数据可信存储架构主要分为四个层,如图 1 所示。物理层:作为系统架构的最底层,通常有传感器、智能家居和物联网设备等硬件组件,这些设备会产生大量的数据,用户可以进行初步的过滤筛选,将认为重要的数据进行摘出,然后通过网络层上传至存储层,对数据进行进一步处理。网络层:对于物理层传输上来的数据,网络层负责建立物理层和应用层之间的连接,并使用 P2P 网络和智能合约进行传输,从而为整个方案提供可靠的后端支持,智能合约中编写的功能,可以为用户和管理员提供服务,使得用户和管理员可以操作和处理数据。存储层:数据经过网络层的操作后,会将经过智能合约操作后的原始数据存储至 IPFS 网络中,实现原始数据的分布式存储,然后对原始数据存储至 IPFS 网络中的地址加密后存储至区块链中。应用层:主要面向用户和管理员,提供各种功能和服务,用户和管理员可以向服务器申请注册账户信息,用户可以上传数据,管理员可以对上传后的数据进行操作。

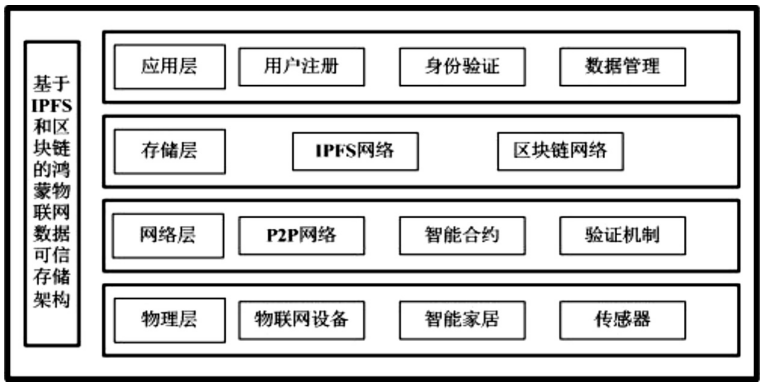


图 1 基于 IPFS 和区块链的鸿蒙物联网数据可信存储架构

### 2.2 链上和链下双路存储

传统区块链系统为了保证安全性而导致效率低下,会出现数据存储的容量低与访问速率慢的问题,导致不能存储大量数据。为了解决此问题,采用区块链结合 IPFS 网络分布式存储的方式解决大规模数据存储的问题,采用链上和链下双路进行数据存储,功能如表 1 所示。基于 IPFS 和区块链的鸿蒙物联网数据可信存储方案中,考虑到鸿蒙物联网数据结构复杂并且体量庞大的问题,并且要保证原始数据的完整性和安全性,采用链上链下双路存储的技术,可以使该方案具备足够的容量可信地存储鸿蒙物联网数据。

表 1 链上存储和链下存储

| 类型 | 功能 | 特点 |
|---|---|---|
| 链上存储 | 将原始数据存储在 IPFS 网络加密后的地址上链,不存储原始数据 | 减轻区块链存储压力<br>提高存储和查询效率 |
| 链下存储 | 将原始数据存储至 IPFS 网络中,并且将返回的数据存储地址加密 | 分布式存储数据<br>存储扩容,提高存储容量 |

### 2.3　系统功能流程图

该系统基于 IPFS 和区块链的架构实现数据的可信存储,系统实现如图 2 所示。首先用户和管理者登入系统管理页面,点击注册按钮申请,向服务器申请注册账户信息。当申请成功后,服务器会调用 usra 库使用 RSA 算法生成 1 024 位的公私密钥对返回账户信息,包含各自的公私密钥对用于管理数据。之后将鸿蒙物联网设备产生的数据上传至服务器中,将鸿蒙物联网数据打包成 zip 格式,然后通过网页发送到服务器。服务器会使用用户的私钥和管理者的公钥对来对原始数据进行数据上传操作,将原始数据后存储至 IPFS 网络中。原始数据存储至 IPFS 网络后会返回一个 IPFS Hash 值,然后使用管理者的公钥对 IPFS Hash 值进行加密,返回一个加密 IPFS Hash 值。最后,将加密 IPFS Hash 值存储至区块链中。当管理员需要下载数据时,输入管理员的私钥来解密加密 IPFS Hash 值,得到原始的 IPFS Hash 值,然后在 IPFS 网络中搜索到原始数据进行下载。

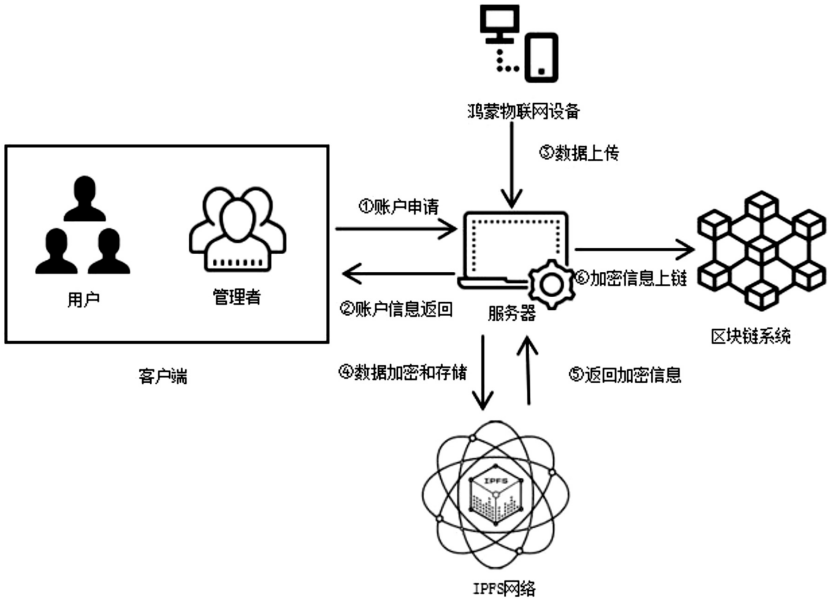


图 2　系统功能实现

### 2.4　系统功能模块设计

该方案的系统功能主要有四个模块:密钥生成、数据上传、数据下载和数据传输记录查询。系统的数据加密和存储等流程涉及相关符号的含义如表 2 所示。

表 2　信息符号的含义

| 符号 | 含义 |
|---|---|
| Data | 数据 |
| PublicKey | 公钥 |
| PrivateKey | 私钥 |
| $User_{SK}$ | 用户私钥 |
| $User_{PK}$ | 用户公钥 |
| $Admin_{SK}$ | 管理员私钥 |
| $Admin_{PK}$ | 管理员公钥 |
| Encrypt | 加密 |
| Decrypt | 解密 |
| IPFS_Hash | IPFS Hash 值 |
| $IPFS\_Hash_{Encrypt}$ | 加密 IPFS Hash 值 |
| Records | 传输记录 |

密钥生成算法:用户或者管理员进入到系统的注册页面,点击注册来获取用于管理数据的公私密钥对,系统会调用 ursa. generatePrivateKey ( )、keys. toPublicPem( ) 和 keys. toPrivatePem( ) 算法生成一对公私密钥对返回给用户或者管理员,需妥善保管好自身的公私密钥对。

数据上传算法:用户在网页上填写用户私钥($User_{SK}$)、管理员公钥($Admin_{PK}$)和鸿蒙物联网数据(Data),并将上传请求提交到服务器。服务器收到用户请求后,调用 ipfs-http-client 库,将鸿蒙物联网数据存储到 IPFS 网络。然后 IPFS 服务器生成 IPFS Hash 值,并使用管理员的公钥对其进行加密,最后返回加密 IPFS Hash 值。

算法 1:用户将鸿蒙物联网数据上传到 IPFS 网络

Input:用户私钥($User_{SK}$),管理员公钥($Admin_{PK}$),数据(Data)

Output:加密 IPFS Hash 值($IPFS\_Hash_{Encrypt}$)

1:BEGIN

2: IPFS. add(Data)　//向 IPFS 网络上传原始数据

3:　　return IPFS_Hash　//返回 IPFS_Hash 值

4: Encrypt($User_{SK}$,$Admin_{PK}$,IPFS_Hash) //使用用户私钥、管理员公钥对 IPFS _Hash 值加密

5:　　return $IPFS\_Hash_{Encrypt}$　//返回加密 IPFS_Hash 值

6:END

数据下载算法,管理员从 IPFS 网络中下载鸿蒙物联网数据。当需要下载鸿蒙物联网数据后,管理员在网页中填写加密 IPFS Hash 值,并将下载请求提交到服务器。服务器收到下载请求后,使用管理员的私钥解密加密 IPFS Hash 值,并调用 ipfs-http-client 库从 IPFS 网络下载原始数据,并返回给管理员,即可下载原始数据。

算法 2:管理员从 IPFS 网络下载鸿蒙物联网数据

Input:管理员公钥($Admin_{PK}$),加密 IPFS Hash 值($IPFS\_Hash_{Encrypt}$)

Output:数据(Data)

1:BEGIN

2: Decrypt($Admin_{SK}$,$IPFS\_Hash_{Encrypt}$) //使用管理员私钥对加密 IPFS_Hash 值解密

3: return IPFS_Hash //返回 IPFS_Hash 值

4: IPFS. down(IPFS_Hash) //调用 IPFS. down 函数下载数据

5: return Data //返回原始数据

6:END

数据传输记录查询算法:管理员在收到鸿蒙物联网数据后,通过服务器上的 ursa 库将私钥转换为公钥,然后用公钥调用智能合约中的查询功能,查看鸿蒙物联网数据的传输记录。

算法 3:数据传输记录查询算法

Input:管理员私钥($Admin_{SK}$)

Output:传输记录(Records)

1:BEGIN

2: Usra. GetPublicKey($Admin_{SK}$) //通过 ursa 库将私钥转换为公钥

3: return $Admin_{PK}$ //获得管理员公钥($Admin_{PK}$)

4: stub. GetState($Admin_{PK}$) //用公钥调用智能合约中的查询功能

5: return (Records) //返回传输记录

6:END

## 3 实验与结果分析

### 3.1 系统部署与功能测试

该文搭建的区块链系统是在基于 Linux 操作系统下开发的,底层框架使用的是 Hyperledger Fabric,虚拟机系统及使用工具配置环境和工具如下:VMware Workstation Pro 17. 5. 1、Ubuntu 20. 04、Hyperledger Fabric 1. 4. 0、Node. js 8. 15. 0、Go 1. 12. 1、Docker 20. 10. 12、Git 2. 25. 1 和 IPFS Kubo v0. 25. 0。

实验环境部署,首先在 Linux 系统上安装 Hyperledger Fabric1. 4. 0 版本,配置基础工具:Node. js、Go、Docker、Docker compose、Git 和 IPFS。接着使用 Hyperledger Fabric 中内置的脚本输入 sudo ./byfn. sh up 启动脚本生成区块链网络,随后将智能合约进行实例化,以支持应用程序发起交易请求,再输入 docker-compose up -d 启动区块链浏览器的数据库容器 PostgreSQL,随后启动 IPFS 网络,输入 ipfs daemon 即可成功生成 IPFS 网络,最后启动前端框架,支持通过浏览器访问系统前端页面,进行交互操作。

账户注册功能:创建密钥对按钮,点击注册按钮,会使用 RSA 算法生成公私密钥对返回给用户。

数据上传存储功能:用户点击上传数据按钮,输入用户的私钥和管理者的公钥以及数据,如图 3 所示。

上传成功后,会返回两个信息,第一个是使用管理员公钥加密后的 IPFS Hash 值,第二个是加密 IPFS Hash 值存储到区块链后作为一个新的交易返回的交易哈希值,如图 4 所示。


图 3 数据加密上传


图 4　数据加密上传后返回结果

数据下载功能,输入数据存储后得到的加密 IPFS Hash 值,然后因为在上传的时候输入了管理员的公钥,所以下载的时候需要输入管理员的私钥对加密 IPFS Hash 值进行解密,然后再从 IPFS 网络中下载原始数据,如图 5 所示。


图 5　加密数据下载

### 3.2　性能评估

测试存储性能,测试方式为:比较传统的集中式存储和该文提出的区块链分布式存储两种存储方案的存储空间使用情况和优缺点分析。测试内容为从 1 到 5 个不同大小数据文件使用两种存储方案的存储空间占用情况,测试结果如图 6 所示。

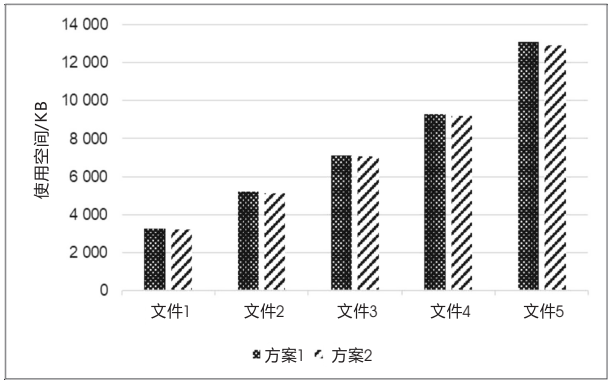


图 6　不同存储方案下的存储空间比较

方案 1:鸿蒙物联网数据利用 AES-256 加密算法压缩加密后存储在本地。

方案 2:采用该文提出的链上链下双路存储方案,将原始数据存储至 IPFS 网络,数据存储地址存储至区块链中。

方案 1 将原始文件通过 AES-256 加密算法加密后存储在本地,虽然实现了数据文件的加密存储,但是这种方式属于集中式存储的一类,如果存储地点出现了故障,数据没有进行冗余备份,会造成数据丢失的问题。方案 2 为该文提出的区块链技术和 IPFS 技术相结合的存储模式,原始文件只存储在 IPFS 分布式存储网络中,实现了分布式存储和数据冗余备份,并且利用区块链不可篡改的特性,将加密后的数据存储地址进行上链操作,实现了可信存储。

从测试结果来看,两个方案使用的存储空间几乎相同,但是该文提出的方案 2 实现了数据的分布式存储和数据的加密存储,并且相比于传统的集中式存储模式,该方案的去中心化模式避免了单点故障的问题,数据的完整性和不可篡改性得到了保证,以及数据存储具有较长的持久性,对数据传输的记录更为公开透明,数据传输可溯源,并且采用链上链下双路存储的模式,提高了数据的存储容量和存储速率。

### 3.3　系统对比

传统的物联网数据存储系统采用集中式存储的模式,无冗余备份,采用分布式存储存在数据存储安全的问题,并且由于采用中心化管理的模型,存在节点故障导致数据泄露等问题,无法满足数据传输的可追溯性和防篡改机制。与其他现有的物联网数据存储系统进行性能对比分析,结果如表 3 所示。

表 3　物联网数据存储系统性能对比分析

| 性能 | 文中方案 | 文献[17] | 文献[18] | 文献[19] | 文献[20] |
|---|---|---|---|---|---|
| 分布式存储 | √ | √ | × | √ | √ |
| 透明可追溯 | √ | √ | √ | √ | × |

续表 3

| 性能 | 文中方案 | 文献[17] | 文献[18] | 文献[19] | 文献[20] |
|---|---|---|---|---|---|
| 去中心化 | √ | √ | √ | √ | × |
| 交易可靠性 | √ | √ | √ | × | × |
| 数据存储地址安全性 | √ | × | × | × | × |

## 4 结束语

针对当前鸿蒙物联网数据主要采用中心化的管理模型带来的数据安全问题,提出了基于区块链和 IPFS 技术的鸿蒙物联网数据可信存储方案。该方案充分利用了区块链技术的不可篡改性、去中心化存储和持久性的特点,结合 IPFS 星际文件系统的分布式存储,使用链上链下双路存储,减轻了区块链的存储压力,提高了存储容量和存储速率,并且结合非对称加密算法来对数据存储地址进行加解密,进一步提高了数据存储的安全性,实现了鸿蒙物联网数据的可信存储。结合仿真实验,验证了方案的可行性和正确性。在未来的工作中,会主要针对存储数据类型做进一步工作,丰富数据存储类型,针对不同应用场景的数据类型进行分类存储,以提高存储效率,并且在不同应用场景增加访问控制功能,提高对数据的管理能力,有效保护用户隐私和数据安全。

**参考文献:**


[1] 毛燕琴,沈苏彬. 物联网信息模型与能力分析[J]. 软件学报,2014,25(8):1685-1695.

[2] FRANCO P,MARTINEZ J M,KIM Y C,et al. IoT based approach for load monitoring and activity recognition in smart homes[J]. IEEE Access,2021,9:45325-45339.

[3] HU J,KAUR K,LIN H,et al. Intelligent a normally detection of trajectories for IoT empowered maritime transportation systems[J]. IEEE Transactions on Intelligent Transportation Systems,2022,24(2):2382-2391.

[4] TANG X. Research on smart logistics model based on internet of things technology[J]. IEEE Access,2020,8:151150-151159.

[5] 杨 震. 物联网发展研究[J]. 南京邮电大学学报:社会科学版,2010,12(2):1-10.

[6] AGIWAL M,SAXENA N,ROY A. Towards connected living:5G enabled internet of things (IoT)[J]. IETE Technical Review,2019,36(2):190-202.

[7] 叶 剑. 面向鸿蒙应用的跨设备隐私泄露方法及检测方法研究[D]. 成都:电子科技大学,2024.

[8] 赵 阔,邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全,2017(5): 1-6.

[9] RAMAN R K,VARSHENY L R. Dynamic distributed storage for blockchains[C]//2018 IEEE international symposium on information theory (ISIT). Vai:IEEE,2018:2619-2623.

[10] XU Xiwei,WEBER I,STAPLES M,et al. A taxonomy of blockchain-based systems for architecture design[C]//2017IEEE international conference on software architecture (ICSA). Gothenburg:IEEE,2017:243-252.

[11] 刘明达,陈左宁,拾以娟,等. 区块链在数据安全领域的研究进展[J]. 计算机学报,2021,44(1):1-27.

[12] 蔡维德,郁 莲,王 荣,等. 基于区块链的应用系统开发方法研究[J]. 软件学报,2017,28(6):1474-1487.

[13] 袁 勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481-494.

[14] 刘文选,赵金东. 基于 Hyperledger Fabri-c 与星际文件系统相结合的数据存储框架[J]. 郑州大学学报:理学版,2023,55(1):28-34.

[15] ZHENG Q,YI L,PING C,et al. An innovative IPFS-based storage model for blockchain[C]//2018 IEEE/WIC/ACM international conference on web intelligence (WI). Santiago:IEEE,2018:704-708.

[16] 樊 凯,周自横,袁望淞,等. 基于区块链的安全多方计算研究现状与展望[J]. 信息对抗技术,2024,3(3):41-62.

[17] 杨久华. 基于区块链的物联网数据安全存储技术研究[D]. 南京:南京邮电大学,2023.

[18] 倪孝泽. 基于区块链的物联网数据存储方法研究[D]. 成都:电子科技大学,2024.

[19] 王 超. 基于区块链的物联网数据存储与共享技术研究[D]. 郑州:中原工学院,2023.

[20] 王鹏然. 智慧城镇物联网数据中台系统设计与实现[D]. 北京:北京邮电大学,2023.