



(21) 申请号 202410936647.9

(22) 申请日 2024.07.12

(71) 申请人 浪潮云洲工业互联网有限公司

地址 250101 山东省济南市高新区浪潮路
1036号浪潮科技园S02号楼19层(72) 发明人 王小明 齐光鹏 商广勇 陈赛
马振

(74) 专利代理机构 北京集佳知识产权代理有限公司 11227

专利代理师 王欢

(51) Int. Cl.

H04L 9/40 (2022.01)

H04L 9/00 (2022.01)

H04L 67/12 (2022.01)

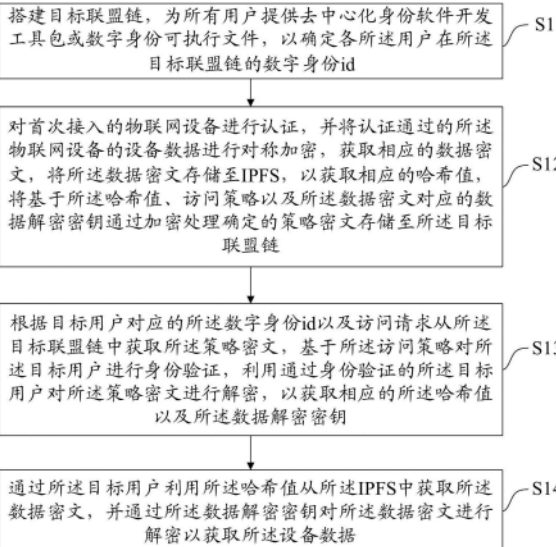
权利要求书2页 说明书9页 附图2页

(54) 发明名称

一种物联网可信数据共享方法、系统、设备
及存储介质

(57) 摘要

本申请公开了一种物联网可信数据共享方法、系统、设备及存储介质,涉及区块链技术领域,包括:搭建目标联盟链,为用户提供去中心化身份软件开发工具包或数字身份可执行文件,确定各用户的数字身份id;将认证通过的设备数据进行加密,获取数据密文,将数据密文存储至IPFS,获取哈希值,将基于哈希值、访问策略及数据密文的数据解密密钥确定的策略密文存储至目标联盟链;根据所述数字身份id及访问请求获取策略密文,对目标用户进行身份验证,利用通过验证的目标用户对策略密文进行解密,获取哈希值及数据解密密钥;利用哈希值获取数据密文,通过数据解密密钥对数据密文进行解密以获取设备数据。实现了物联网数据存储安全以及安全访问。



1. 一种物联网可信数据共享方法,其特征在于,包括:

搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id;

对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;

根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;

通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。

2. 根据权利要求1所述的物联网可信数据共享方法,其特征在于,还包括:

若所述用户为首次登录,则对所述用户进行实名认证,为通过实名认证的所述用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定所述用户在所述目标联盟链的数字身份id,并将所述数字身份id写入所述目标联盟链。

3. 根据权利要求1所述的物联网可信数据共享方法,其特征在于,还包括:

将所述去中心化身份软件开发工具包或数字身份可执行文件安装至所述物联网设备进行运行,以获取所述物联网设备的设备id、目标公钥以及目标私钥,并将所述设备id、所述目标公钥以及所述目标私钥存储至所述目标联盟链。

4. 根据权利要求3所述的物联网可信数据共享方法,其特征在于,所述对首次接入的物联网设备进行认证,包括:

通过所述物联网设备加密目标明文,获取加密后明文,利用所述目标联盟链中的所述目标公钥对所述加密后明文进行解密,确定解密后明文;

基于对所述解密后明文与所述目标明文是否一致的判断完成对所述物联网设备的身份验证;

根据所述物联网设备的设备名称判断所述物联网设备是否为目标企业设备,以便基于相应的判断结果完成对所述物联网设备的信息验证;

通过所述身份验证和所述信息验证完成对首次接入的所述物联网设备的认证。

5. 根据权利要求1所述的物联网可信数据共享方法,其特征在于,所述对首次接入的物联网设备进行认证之后,还包括:

将认证通过的所述物联网设备的设备id、设备名称、所属企业、认证状态以及接入时间写入所述目标联盟链。

6. 根据权利要求1所述的物联网可信数据共享方法,其特征在于,还包括:

若所述访问策略更新,则对所述策略密文进行解密,以便于通过新的访问策略、重新加密后数据密文的数据解密密钥和所述重新加密后数据密文对应的哈希值确定新策略密文,并将所述策略密文上传至所述目标联盟链中;所述重新加密后数据密文为解密所述策略密文后对所述数据密文进行重新加密后的数据密文;

通过所述目标联盟链上的目标智能合约对比所述新策略密文与更新前的所述策略密

文的不同,以完成相应的数据替换。

7.根据权利要求1至6任一项所述的物联网可信数据共享方法,其特征在于,所述根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,包括:

将所述目标用户对应的所述数字身份id与所述目标联盟链中的身份信息进行匹配,根据相应的匹配结果确定所述目标用户的身份是否符合预设身份验证条件;

若否,则禁止获取所述策略密文;

若是,则根据所述访问请求从所述目标联盟链中获取所述策略密文,并将所述目标用户的用户属性与所述访问策略进行对比,以便基于相应的对比结果确定所述目标用户是否通过身份验证;

若通过所述身份验证,则对所述策略密文进行解密;

若未通过所述身份验证,则禁止对所述策略密文进行解密。

8.一种物联网可信数据共享系统,其特征在于,包括:

数字身份id确定模块,用于搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id;

策略密文存储模块,用于对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;

策略密文解密模块,用于根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;

设备数据获取模块,用于通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。

9.一种电子设备,其特征在于,包括:

存储器,用于保存计算机程序;

处理器,用于执行所述计算机程序以实现如权利要求1至7任一项所述的物联网可信数据共享方法。

10.一种计算机可读存储介质,其特征在于,用于保存计算机程序,所述计算机程序被处理器执行时实现如权利要求1至7任一项所述的物联网可信数据共享方法。

一种物联网可信数据共享方法、系统、设备及存储介质

技术领域

[0001] 本发明涉及区块链技术领域,特别涉及一种物联网可信数据共享方法、系统、设备及存储介质。

背景技术

[0002] 随着物联网以及新一代信息技术的融合发展,越来越多设备接入网络,物联网数据呈现出爆炸性增长的趋势,大量的数据被产生和传输,这给设备和数据安全、隐私带来了挑战。基于区块链技术,本发明旨在通过对接入设备认证、数据安全存储以及访问权限控制,提供一种可信的物联网数据共享方法,实现物联网数据安全流通和可信利用。

[0003] 传统的区块链数据存储,元数据往往以明文/密文形式存储到IPFS(InterPlanetary File System,星际文件系统),密文存储解密时需要传输数据所有者的私钥,容易受到网络攻击导致数据泄露;同时物联网可信数据共享包括设备数据采集、存储、传输、处理等流程,发明者往往针对具体场景解决具体问题,难以形成可复制推广的方案;设备的真实可靠也是数据可信共享前必须核验的。

发明内容

[0004] 有鉴于此,本发明的目的在于提供一种物联网可信数据共享方法、系统、设备及存储介质,能够解决物联网设备可信接入、物联网数据存储安全以及安全访问的问题。其具体方案如下:

[0005] 第一方面,本申请公开了一种物联网可信数据共享方法,包括:

[0006] 搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id;

[0007] 对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;

[0008] 根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;

[0009] 通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。

[0010] 可选的,所述方法,还包括:

[0011] 若所述用户为首次登录,则对所述用户进行实名认证,为通过实名认证的所述用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定所述用户在所述目标联盟链的数字身份id,并将所述数字身份id写入所述目标联盟链。

[0012] 可选的,所述方法,还包括:

[0013] 将所述去中心化身份软件开发工具包或数字身份可执行文件安装至所述物联网设备进行运行,以获取所述物联网设备的设备id、目标公钥以及目标私钥,并将所述设备id、所述目标公钥以及所述目标私钥存储至所述目标联盟链。

[0014] 可选的,所述对首次接入的物联网设备进行认证,包括:

[0015] 通过所述物联网设备加密目标明文,获取加密后明文,利用所述目标联盟链中的所述目标公钥对所述加密后明文进行解密,确定解密后明文;

[0016] 基于对所述解密后明文与所述目标明文是否一致的判断完成对所述物联网设备的身份验证;

[0017] 根据所述物联网设备的设备名称判断所述物联网设备是否为目标企业设备,以便基于相应的判断结果完成对所述物联网设备的信息验证;

[0018] 通过所述身份验证和所述信息验证完成对首次接入的所述物联网设备的认证。

[0019] 可选的,所述对首次接入的物联网设备进行认证之后,还包括:

[0020] 将认证通过的所述物联网设备的设备id、设备名称、所属企业、认证状态以及接入时间写入所述目标联盟链。

[0021] 可选的,所述方法,还包括:

[0022] 若所述访问策略更新,则对所述策略密文进行解密,以便于通过新的访问策略、重新加密后数据密文的数据解密密钥和所述重新加密后数据密文对应的哈希值确定新策略密文,并将所述策略密文上传至所述目标联盟链中;所述重新加密后数据密文为解密所述策略密文后对所述数据密文进行重新加密后的数据密文;

[0023] 通过所述目标联盟链上的目标智能合约对比所述新策略密文与更新前的所述策略密文的不同,以完成相应的数据替换。

[0024] 可选的,所述根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,包括:

[0025] 将所述目标用户对应的所述数字身份id与所述目标联盟链中的身份信息进行匹配,根据相应的匹配结果确定所述目标用户的身份是否符合预设身份验证条件;

[0026] 若否,则禁止获取所述策略密文;

[0027] 若是,则根据所述访问请求从所述目标联盟链中获取所述策略密文,并将所述目标用户的用户属性与所述访问策略进行对比,以便基于相应的对比结果确定所述目标用户是否通过身份验证;

[0028] 若通过所述身份验证,则对所述策略密文进行解密;

[0029] 若未通过所述身份验证,则禁止对所述策略密文进行解密。

[0030] 第二方面,本申请公开了一种物联网可信数据共享系统,包括:

[0031] 数字身份id确定模块,用于搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id;

[0032] 策略密文存储模块,用于对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;

[0033] 策略密文解密模块,用于根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;

[0034] 设备数据获取模块,用于通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。

[0035] 第三方面,本申请公开了一种电子设备,包括:

[0036] 存储器,用于保存计算机程序;

[0037] 处理器,用于执行所述计算机程序以实现如前述的物联网可信数据共享方法。

[0038] 第四方面,本申请公开了一种计算机可读存储介质,用于保存计算机程序,所述计算机程序被处理器执行时实现如前述的物联网可信数据共享方法。

[0039] 本申请在共享物联网可信数据时,首先搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id;然后对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;最后通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。可见本申请通过分布式数字身份和访问控制策略为物联网设备生成可信数字身份并进行确权和流转,实现设备的可信数字身份管理,以及对设备的可信访问控制。并且通过区块链和IPFS实现去中心化的数据存储,数据可以分片并存储在IPFS网络中,分布在多个节点上,实现了数据的存储安全,解决了物联网设备可信接入、物联网数据存储安全以及安全访问的问题。

附图说明

[0040] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据提供的附图获得其他的附图。

[0041] 图1为本申请公开的一种物联网可信数据共享方法流程图;

[0042] 图2为本申请公开的一种物联网可信数据共享系统结构示意图;

[0043] 图3为本申请公开的一种电子设备结构图。

具体实施方式

[0044] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于

本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0045] 传统的区块链数据存储,元数据往往以明文/密文形式存储到IPFS,密文存储解密时需要传输数据所有者的私钥,容易受到网络攻击导致数据泄露;同时物联网可信数据共享包括设备数据采集、存储、传输、处理等流程,发明者往往针对具体场景解决具体问题,难以形成可复制推广的方案;设备的真实可靠也是数据可信共享前必须核验的。为了解决上述技术问题,本申请公开了一种物联网可信数据共享方法,能够解决物联网设备可信接入、物联网数据存储安全以及安全访问的问题。

[0046] 参见图1所示,本发明实施例公开了一种物联网可信数据共享方法,包括:

[0047] 步骤S11、搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id。

[0048] 本实施例中,首先根据业务实际,搭建物联网可信联盟链;为所有用户提供分布式数字身份生成和验证工具包DID SDK(Decentralized Identity Software Development Kit,去中心化身份软件开发工具包)/数字身份可执行文件,赋予用户和物联网设备唯一自主可信的链上数字身份id(Identity document,身份标识),公私钥保存在本地。具体来说,用户通过安装DID SDK/数字身份可执行文件自主获取数字身份id及公私钥;通过将DID SDK/数字身份可执行文件安装到智能设备并运行,获得设备身份id机器公私钥,并进行存储并妥善保管;对首次登录系统的用户进行实名认证,将通过认证用户的身份id和公钥写入物联网可信联盟链中。同时,将所述去中心化身份软件开发工具包或数字身份可执行文件安装至所述物联网设备进行运行,以获取所述物联网设备的设备id、目标公钥以及目标私钥,并将所述设备id、所述目标公钥以及所述目标私钥存储至所述目标联盟链。

[0049] 步骤S12、对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链。

[0050] 本实施例中,对首次接入的物联网设备进行认证管理,认证通过的设备id、基本信息以及设备所产生的数据写入到物联网可信联盟链中;其中设备数据的元数据通过对称加密存储在IPFS上,并将访问策略、IPFS返回的哈希值和数据解密密钥形成的策略密文加密存储到物联网可信联盟链中。在对首次接入的物联网设备进行认证时,通过所述物联网设备加密目标明文,获取加密后明文,利用所述目标联盟链中的所述目标公钥对所述加密后明文进行解密,确定解密后明文;基于对所述解密后明文与所述目标明文是否一致的判断完成对所述物联网设备的身份验证;根据所述物联网设备的设备名称判断所述物联网设备是否为目标企业设备,以便基于相应的判断结果完成对所述物联网设备的信息验证;通过所述身份验证和所述信息验证完成对首次接入的所述物联网设备的认证。通俗来说,物联网设备首次接入系统需进行双重校验,首先进行身份校验,由用户/物联网设备加密一段明文并通过联盟链中对应公钥去解密来校验解密后内容是否与加密前明文是否匹配实现身份校验;然后由系统中已完成认证的用户通过设备名称等信息核验是否为所属企业设备。双重认证通过后设备相关信息设备id、设备名、所属企业、认证状态、接入时间等写入物联网可信联盟链中;认证通过后的设备方可接入系统进行数据传输。

[0051] 设备接入后,设备数据通过对称加密存储到物联网可信联盟链,为实现数据快速高效存储,元数据加密存储到IPFS上,存储后会返回一个哈希值,通过该哈希值可查找对应的元数据;数据所有者将IPFS返回的哈希值、数据密文的解密密钥、以及访问控制策略加密形成策略密文存储到物联网可信联盟链上。若所述访问策略更新,则对所述策略密文进行解密,以便于通过新的访问策略、重新加密后数据密文的数据解密密钥和所述重新加密后数据密文对应的哈希值确定新策略密文,并将所述策略密文上传至所述目标联盟链中;所述重新加密后数据密文为解密所述策略密文后对所述数据密文进行重新加密后的数据密文;通过所述目标联盟链上的目标智能合约对比所述新策略密文与更新前的所述策略密文的不同,以完成相应的数据替换。也就是说,链上存证智能合约通过比上传的数据信息摘要实现数据替换,并将历史信息存在历史信息库。传统区块链并不是为大规模数据存储而设计的,这样一来,通过区块链和IPFS融合,将实际数据通过加密存储在IPFS上,相应的访问策略的加密哈希存储到区块链中,提供安全、可靠、去中心化的数据存储方案。并且,通过采用“物联网技术+区块链技术”赋予物联网设备一个真实可信的链上身份,物理网设备可通过物联网芯片自动上传产品动态信息到链端,降低动态溯源信息获取成本的同时,实现端侧到链侧的数据的安全采集,提供安全、可信的数据。

[0052] 步骤S13、根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥。

[0053] 本实施例中数据使用者请求访问数据,首先通过用户自有数字身份id与物联网可信联盟链中的身份信息进行匹配来验证身份真实性;身份验证通过后获取链上对应策略密文,并进行解密,比对用户属性是否满足策略密文中的访问控制策略,满足则可以对策略密文进行解密,不满足不能解密;满足访问控制策略的用户获取数据密文的 IPFS 哈希值和数据密文的解密密钥。具体来说,将所述目标用户对应的所述数字身份id与所述目标联盟链中的身份信息进行匹配,根据相应的匹配结果确定所述目标用户的身份是否符合预设身份验证条件;若否,则禁止获取所述策略密文;若是,则根据所述访问请求从所述目标联盟链中获取所述策略密文,并将所述目标用户的用户属性与所述访问策略进行对比,以便基于相应的对比结果确定所述目标用户是否通过身份验证;若通过所述身份验证,则对所述策略密文进行解密;若未通过所述身份验证,则禁止对所述策略密文进行解密。最后获取相应的所述哈希值以及所述数据解密密钥。

[0054] 步骤S14、通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。

[0055] 本实施例中,最后利用所述哈希值从IPFS中下载相应数据密文并用解密密钥进行解密得到访问数据。并通过数据hash比对来验证数据的一致性和完整性,保证数据未发生丢失。这样一来,当需要访问数据时,数据使用者发起访问请求,由区块链智能合约验证用户属性是否符合访问策略,验证通过后经由区块链获取数据的哈希值,从IPFS网络中检索加密数据块,解密后获取元数据,实现数据的细粒度共享及用户隐私保护。

[0056] 综上所述,本申请在共享物联网可信数据时,首先搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联

盟链的数字身份id;然后对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;最后通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。可见本申请通过分布式数字身份和访问控制策略为物联网设备生成可信数字身份并进行确权和流转,实现设备的可信数字身份管理,以及对设备的可信访问控制。并且通过区块链和IPFS实现去中心化的数据存储,数据可以分片并存储在IPFS网络中,分布在多个节点上,实现了数据的存储安全,解决了物联网设备可信接入、物联网数据存储安全以及安全访问的问题。

[0057] 本申请公开了一种具体的物联网可信数据共享方法,总的来说,首先根据业务实际,搭建物联网可信联盟链;为所有用户提供分布式数字身份生成和验证工具包DID SDK/数字身份可执行文件,赋予用户和物联网设备唯一自主可信的链上数字身份id,公私钥保存在本地;然后对首次接入的物联网设备进行认证管理,认证通过的设备id、基本信息以及设备所产生的数据写入到物联网可信联盟链中;其中,设备数据的元数据通过对称加密存储在IPFS上,并将访问策略、IPFS返回的哈希值和数据解密密钥形成的策略密文加密存储到物联网可信联盟链中。

[0058] 最后数据使用者请求访问数据,首先通过用户自有数字身份id与物联网可信联盟链中的身份信息进行匹配来验证身份真实性;身份验证通过后获取链上对应策略密文,并进行解密,比对用户属性是否满足策略密文中的访问控制策略,满足则可以对策略密文进行解密,不满足不能解密;满足访问控制策略的用户获取数据密文的IPFS哈希值和数据密文的解密密钥;然后从IPFS 中下载相应数据密文并用解密密钥进行解密得到访问数据。并通过数据hash比对来验证数据的一致性和完整性。

[0059] 由此,本申请通过分布式数字身份和访问控制策略为物联网设备生成可信数字身份并进行确权和流转,实现设备的可信数字身份管理,以及对设备的可信访问控制;同时,区块链和IPFS,可以实现去中心化的数据存储。数据可以分片并存储在IPFS网络中,分布在多个节点上。每个数据块都有一个唯一的哈希值作为其标识符。然后,数据的哈希值或元数据可以存储在区块链上,形成数据的标识,区块链记录了数据的存储位置和访问权限等信息;另一方面,访问策略由数据所有者设定并与密文绑定,属性和用户的密钥绑定,同时支持访问策略灵活更新,从而实现数据细粒度安全访问。

[0060] 参见图2所示,本发明实施例公开了一种物联网可信数据共享系统,包括:

[0061] 数字身份id确定模块11,用于搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id;

[0062] 策略密文存储模块12,用于对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至

IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;

[0063] 策略密文解密模块13,用于根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;

[0064] 设备数据获取模块14,用于通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。

[0065] 综上所述,本申请在共享物联网可信数据时,首先搭建目标联盟链,为所有用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定各所述用户在所述目标联盟链的数字身份id;然后对首次接入的物联网设备进行认证,并将认证通过的所述物联网设备的设备数据进行对称加密,获取相应的数据密文,将所述数据密文存储至IPFS,以获取相应的哈希值,将基于所述哈希值、访问策略以及所述数据密文对应的数据解密密钥通过加密处理确定的策略密文存储至所述目标联盟链;根据目标用户对应的所述数字身份id以及访问请求从所述目标联盟链中获取所述策略密文,基于所述访问策略对所述目标用户进行身份验证,利用通过身份验证的所述目标用户对所述策略密文进行解密,以获取相应的所述哈希值以及所述数据解密密钥;最后通过所述目标用户利用所述哈希值从所述IPFS中获取所述数据密文,并通过所述数据解密密钥对所述数据密文进行解密以获取所述设备数据。可见本申请通过分布式数字身份和访问控制策略为物联网设备生成可信数字身份并进行确权和流转,实现设备的可信数字身份管理,以及对设备的可信访问控制。并且通过区块链和IPFS实现去中心化的数据存储,数据可以分片并存储在IPFS网络中,分布在多个节点上,实现了数据的存储安全,解决了物联网设备可信接入、物联网数据存储安全以及安全访问的问题。

[0066] 在一些具体的实施例中,所述系统,还可以包括:

[0067] 实名认证模块,用于若所述用户为首次登录,则对所述用户进行实名认证,为通过实名认证的所述用户提供去中心化身份软件开发工具包或数字身份可执行文件,以确定所述用户在所述目标联盟链的数字身份id,并将所述数字身份id写入所述目标联盟链。

[0068] 在一些具体的实施例中,所述系统,还可以包括:

[0069] 存储模块,用于将所述去中心化身份软件开发工具包或数字身份可执行文件安装至所述物联网设备进行运行,以获取所述物联网设备的设备id、目标公钥以及目标私钥,并将所述设备id、所述目标公钥以及所述目标私钥存储至所述目标联盟链。

[0070] 在一些具体的实施例中,所述策略密文存储模块12,具体可以包括:

[0071] 明文解密单元,用于通过所述物联网设备加密目标明文,获取加密后明文,利用所述目标联盟链中的所述目标公钥对所述加密后明文进行解密,确定解密后明文;

[0072] 身份验证单元,用于基于对所述解密后明文与所述目标明文是否一致的判断完成对所述物联网设备的身份验证;

[0073] 信息验证单元,用于根据所述物联网设备的设备名称判断所述物联网设备是否为目标企业设备,以便基于相应的判断结果完成对所述物联网设备的信息验证;

[0074] 物联网设备认证单元,用于通过所述身份验证和所述信息验证完成对首次接入的

所述物联网设备的认证。

[0075] 在一些具体的实施例中,所述系统,还可以用于将认证通过的所述物联网设备的设备id、设备名称、所属企业、认证状态以及接入时间写入所述目标联盟链。

[0076] 在一些具体的实施例中,所述系统,还可以用于若所述访问策略更新,则对所述策略密文进行解密,以便于通过新的访问策略、重新加密后数据密文的数据解密密钥和所述重新加密后数据密文对应的哈希值确定新策略密文,并将所述策略密文上传至所述目标联盟链中;所述重新加密后数据密文为解密所述策略密文后对所述数据密文进行重新加密后的数据密文;通过所述目标联盟链上的目标智能合约对比所述新策略密文与更新前的所述策略密文的不同,以完成相应的数据替换。

[0077] 在一些具体的实施例中,所述策略密文解密模块13,具体可以用于将所述目标用户对应的所述数字身份id与所述目标联盟链中的身份信息进行匹配,根据相应的匹配结果确定所述目标用户的身份是否符合预设身份验证条件;若否,则禁止获取所述策略密文;若是,则根据所述访问请求从所述目标联盟链中获取所述策略密文,并将所述目标用户的用户属性与所述访问策略进行对比,以便基于相应的对比结果确定所述目标用户是否通过身份验证;若通过所述身份验证,则对所述策略密文进行解密;若未通过所述身份验证,则禁止对所述策略密文进行解密。

[0078] 进一步的,本申请实施例还公开了一种电子设备,图3是根据一示例性实施例示出的电子设备20结构图,图中的内容不能认为是对本申请的使用范围的任何限制。

[0079] 图3为本申请实施例提供的一种电子设备20的结构示意图。该电子设备 20,具体可以包括:至少一个处理器21、至少一个存储器22、电源23、通信接口24、输入输出接口25和通信总线26。其中,所述存储器22用于存储计算机程序,所述计算机程序由所述处理器21加载并执行,以实现前述任一实施例公开的物联网可信数据共享方法中的相关步骤。另外,本实施例中的电子设备20具体可以为电子计算机。

[0080] 本实施例中,电源23用于为电子设备20上的各硬件设备提供工作电压;通信接口24能够为电子设备20创建与外界设备之间的数据传输通道,其所遵循的通信协议是能够适用于本申请技术方案的任意通信协议,在此不对其进行具体限定;输入输出接口25,用于获取外界输入数据或向外界输出数据,其具体的接口类型可以根据具体应用需要进行选取,在此不进行具体限定。

[0081] 另外,存储器22作为资源存储的载体,可以是只读存储器、随机存储器、磁盘或者光盘等,其上所存储的资源可以包括操作系统221、计算机程序222 等,存储方式可以是短暂存储或者永久存储。

[0082] 其中,操作系统221用于管理与控制电子设备20上的各硬件设备以及计算机程序222,其可以是Windows Server、Netware、Unix、Linux等。计算机程序222除了包括能够用于完成前述任一实施例公开的由电子设备20执行的物联网可信数据共享方法的计算机程序之外,还可以进一步包括能够用于完成其他特定工作的计算机程序。

[0083] 进一步的,本申请还公开了一种计算机可读存储介质,用于存储计算机程序;其中,所述计算机程序被处理器执行时实现前述公开的物联网可信数据共享方法。关于该方法的具体步骤可以参考前述实施例中公开的相应内容,在此不再进行赘述。

[0084] 本说明书中各个实施例采用递进的方式描述,每个实施例重点说明的都是与其它

实施例的不同之处,各个实施例之间相同或相似部分互相参见即可。对于实施例公开的装置而言,由于其与实施例公开的方法相对应,所以描述的比较简单,相关之处参见方法部分说明即可。

[0085] 专业人员还可以进一步意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、计算机软件或者二者的结合来实现,为了清楚地说明硬件和软件的可互换性,在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0086] 结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块,或者二者的结合来实施。软件模块可以置于随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

[0087] 最后,还需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0088] 以上对本申请所提供的技术方案进行了详细介绍,本文中应用了具体个例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本申请的限制。

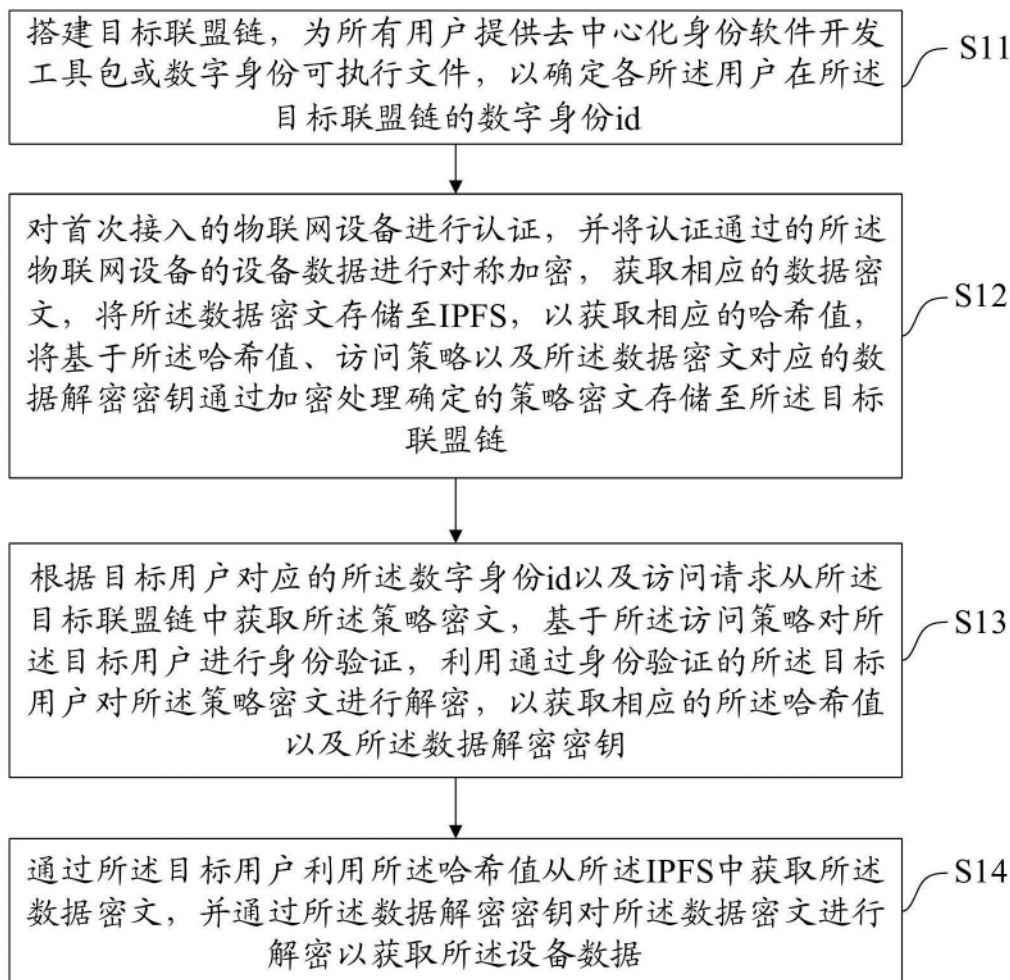


图1

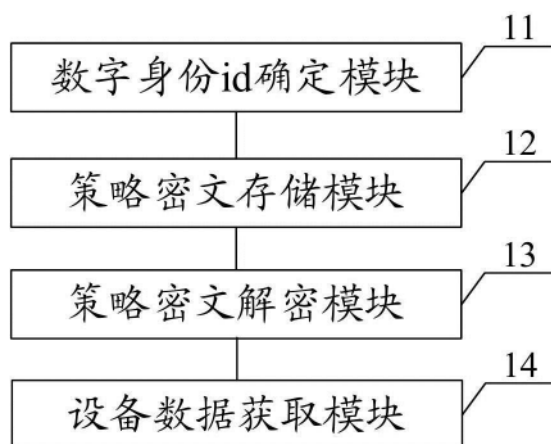


图2

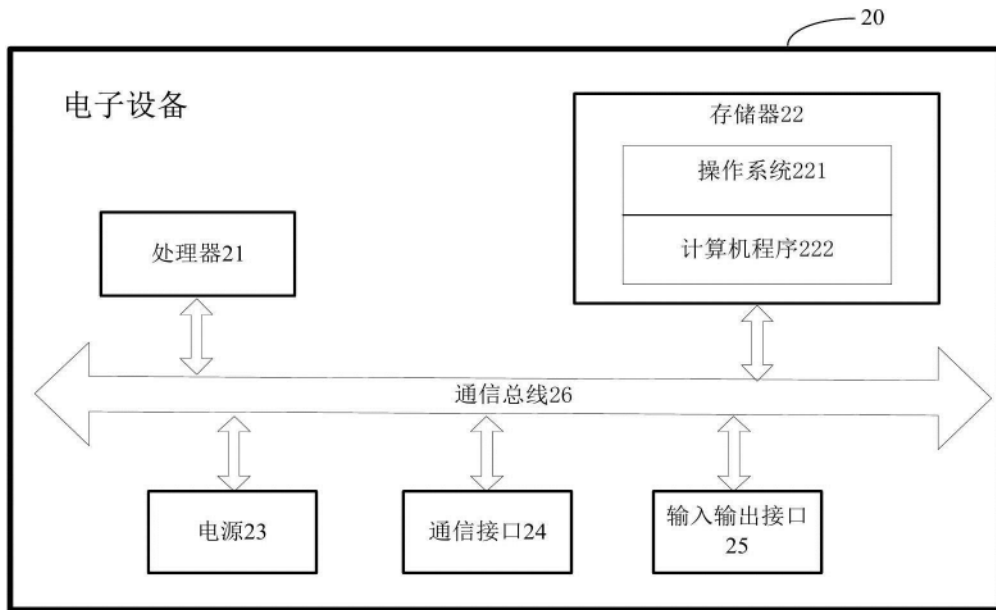


图3