(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114422215 A
(43)申请公布日 2022.04.29

(21)申请号 202111675204.1
(22)申请日 2021.12.31
(71)申请人 国网安徽省电力有限公司合肥供电公司
地址 230041 安徽省合肥市宿松路133号
申请人 国网安徽省电力有限公司
国网信息通信产业集团有限公司
天津市普迅电力信息技术有限公司
(72)发明人 陈朔 彭晓武 马俊杰 李周 王海超 胡昊 张照 潘胜 周林
(74)专利代理机构 天津盛理知识产权代理有限公司 12209
代理人 王雨晴
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/10(2022.01)
G06F 21/44(2013.01)

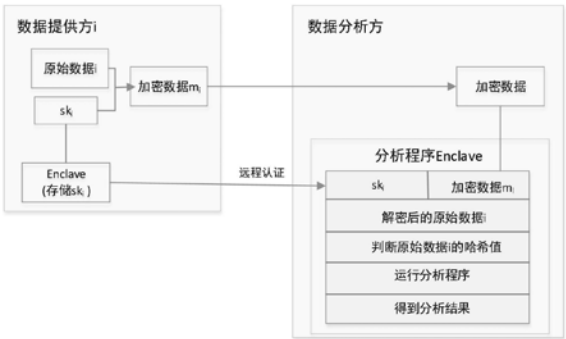
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种基于区块链的跨平台和可信能源数据共享系统及方法

(57)摘要

一种基于区块链的跨平台的可信能源数据共享系统及方法,包括:多个数据提供方、区块链和数据分析方,该多个数据提供方分别通过区块链和数据分析方相连接。本发明能够针对不同能源资源数据掌握在不同能源企业,且数量大的特点,能够解决多方能源数据在聚合和共享过程中的数据可信问题。



CN 114422215 A

1.一种基于区块链的跨平台的可信能源数据共享系统,其特征在于:包括:多个数据提供方、区块链和数据分析方,该多个数据提供方分别通过区块链和数据分析方相连接;

所述多个数据提供方均已各自注册为区块链节点,每个数据提供方i(i=1,2,3……)包含一对私钥sk_i和公钥pk_i,公钥pk_i用于加密原始数据,私钥sk_i用于解密原始数据,并且能够安装enclave,其中,enclave是在Intel的SGX上运行的受信任程序,用于数据安全传输,并保证隐私数据的安全。

该数据提供方使用区块链发布元数据,并给数据分析方传输公钥加密后的原始数据,以及远程认证中对数据分析方身份的验证和传递私钥;

所述数据分析方也注册为区块链节点,并且能够安装enclave分析程序;

该数据分析方用于查看数据提供方的元数据和发送使用数据请求,并接受来自数据提供方已加密的原始数据,以及编写、安装分析程序和使用数据提供方发来的的私钥解密出数据提供方的原数据,然后在enclave内执行分析程序;

所述区块链用于存储数据提供方的元数据以及数据提供方和数据分析方的公钥。

2.一种基于区块链的跨平台的可信能源数据共享方法,其特征在于:包括以下步骤:

步骤1、数据提供方发布元数据,数据分析方发出数据使用需求;

步骤2、数据提供方发送加密的原始数据到数据分析方;

步骤3、数据提供方和数据分析方双方之间进行远程认证;

步骤4、数据分析方接收到数据提供方发来的私钥,然后执行程序,最终实现跨平台的可信能源数据共享。

3.根据权利要求2所述的一种基于区块链的跨平台的可信能源数据共享方法,其特征在于:所述步骤1的具体步骤包括:

(1)数据提供方i在区块链上发布其元数据

所述元数据包括原始数据集的描述和哈希,其中哈希是具有恒定长度输出的抗冲突函数;

(2)数据分析方从区块链上看到多个数据提供方的元数据,获取所有元数据的相关信息,确定哪些数据提供方的原始数据聚合后可得到所需的分析结果,并对相应数据提供方发出使用数据请求。

4.根据权利要求2所述的一种基于区块链的跨平台的可信能源数据共享方法,其特征在于:所述步骤2的具体步骤包括:

(1)相应的数据提供方i生成各自的密钥对(pk_i,sk_i),利用各自公钥pk_i对其原始能源数据m_i进行加密;

(2)相应的数据提供方i将加密后的数据发送至数据分析方。

5.根据权利要求2所述的一种基于区块链的跨平台的可信能源数据共享方法,其特征在于:所述步骤3的具体步骤包括:

(1)数据分析方本地编写并安装分析程序的enclave,然后数据分析方将该enclave的代码公开,其中enclave是在Intel的SGX上运行的受信任程序;

(2)由相应的数据提供方i检查数据分析方已发布enclave的合法性,如果通过,相应的数据提供方i将在本地设置一个存储sk_i的新enclave,并建立对分析程序enclave的远程认证,如果目标enclave的哈希值等于所得的数据分析方分析程序enclave的哈希值,远程认

证通过,然后将sk_i发送到目标enclave。

6.根据权利要求2所述的一种基于区块链的跨平台的可信能源数据共享方法,其特征在于:所述步骤4的具体步骤包括:

(1)数据分析方接受到数据提供方i的私钥sk_i,使用sk_i解密出数据提供方i的原始数据i

(2)判定原始数据i的哈希值与数据提供方i的元数据哈希值是否匹配,如果不匹配则返回信息“来自数据提供方i的数据是无效的”,如果匹配,则运行分析程序,得到多方能源数据提供方聚合和共享数据后的分析结果;

其中数据提供方i的元数据哈希值是硬编码。

一种基于区块链的跨平台和可信能源数据共享系统及方法

技术领域

[0001] 本发明属于数据共享技术领域，涉及一种跨平台和可信能源数据共享系统及方法，尤其是一种基于区块链的跨平台的可信能源数据共享系统及方法。

背景技术

[0002] 区块链是一个分布式的、不可逆的公共分类账，集合了密码学技术、分布式数据库管理、智能合约等技术，其中智能合约是旨在自动执行的确定性程序的一部分，将所有参与的节点数据通过加密算法保存在区块链的链式结构节点上，并共同检验记录上传数据。区块链和智能合约技术通常用于存储/维护信息或以公开和不变的方式执行操作。针对国网链能源数据量巨大，导致的区块链储存能力和计算能力不足的问题已存在各种解决方案，然而，在大范围内的能源大数据聚合和共享也面临着数据不可信等隐私安全问题。不同的能源资源由不同的企业控制，由于隐私泄露、数据安全和数据利益受损等危害的存在，导致能源数据拥有者不愿聚合和共享数据，势必造成“数据孤岛”。虽然各地国网建立能源数据中心取得一定成功，但在更大范围内汇总能源数据仍然存在无法克服的困难。如专利一种数据共享方法及系统，CN202011070405.4介绍了能源数据在联盟链实上共享的方法，尤其联盟链半中心化结构的特点，很容易被恶意玩家所攻击，在有限的节点内，可以假定多个参与者会出现合谋的可能性，不能保证数据可信共享，另外，也缺乏行业统一标准，在解决方案上会有各种障碍。

[0003] 目前，隐私计算中基于硬件设计的方案主要是可信执行环境(TEE)。全球平台组织(GP)在2010年提出TEE的第一个标准，表明其能确保一个任务按照预期执行而保证初始状态、运行时状态的机密性和完整性。即使在OS、BIOS、VMM或者SMM这些系统层存在特权恶意软件的情况下TEE也能保证数据安全，其应用场景可包括云端(服务器)、移动端、边缘设备等。

[0004] 目前有一系列基于硬件的解决方案被称为可信执行环境(TEE)，包括Intel的SGX和AMD，可以确保程序在受保护的环境中运行，实现两个基本目标，即程序代码不能被篡改，中间变量不能由受保护程序本身以外的各方获得。在本发明中，我们使用intel的软件保护扩展(SGX)。其设计原则是在CPU电路层对受保护的内存访问增加一个权限判断。具体来说，TEE保护的内存地址段对外不可访问，包括操作系统和未保护的内存。但是，可以指定外部调用受信任程序的某些方法。

[0005] 在英特尔SGX上运行的受信任程序称为enclave。Intel提供了两enclave之间的安全数据传输功能，称为本地认证和远程认证，实现了从一个enclave到另一个enclave的数据传输，同时将隐私数据保留在安全域之内。前者用于两个enclave位于同一平台上的情况，而后者用于位于不同平台的enclave之间的身份验证和数据传输。(此处的身份验证包括身份确认和检查enclave的哈希值)，例如，在本发明中，数据提供方和数据分析方属于不同的平台，因此将使用远程认证。然而，远程认证的一个缺点是，它既要求Enclave在线，又要求存在可信的第三方。因此，在现实中，使用远程认证传输的数据量和频率是有限的，这

意味着我们无法通过远程认证传输整个数据集。

[0006] 而且,针对数据分析方(国家电网公司数据中心)需要从多个能源数据提供方(能源企业)收集能源数据以执行分析任务的需求,即只需要多种能源数据聚合后的分析结果而不需要原始数据,但存在能源数据量十分庞大且不同能源数据资源由不同能源数据提供方控制的情况,由于数据法律以及隐私泄露、数据安全和数据利益受损等隐私敏感性问题的存在,导致能源数据提供方不愿把所拥有的原始数据跟其他能源数据聚合和共享给数据分析方,这严重影响了政府对能源结构化决策。

[0007] 因此,如何针对不同能源资源数据掌握在不同能源企业,且数量大的特点,提出一种基于区块链的跨平台和可信能源数据共享系统,能够解决多方能源数据在聚合和共享过程中的数据可信问题是本领域技术人员亟待解决的技术难题。

发明内容

[0008] 本发明的目的在于克服现有技术的不足,提出一种基于区块链的跨平台的可信能源数据共享系统及方法,针对不同能源资源数据掌握在不同能源企业,且数量大的特点,能够解决多方能源数据在聚合和共享过程中的数据可信问题。

[0009] 本发明解决其现实问题是采取以下技术方案实现的:

[0010] 一种基于区块链的跨平台的可信能源数据共享系统,包括:多个数据提供方、区块链和数据分析方,该多个数据提供方分别通过区块链和数据分析方相连接;

[0011] 所述多个数据提供方均已各自注册为区块链节点,每个数据提供方i(i=1,2,3……)包含一对私钥sk_i和公钥pk_i,公钥pk_i用于加密原始数据,私钥sk_i用于解密原始数据,并且能够安装enclave,其中,enclave是在Intel的SGX上运行的受信任程序,可看成是一个被保护的内容容器,可以存放应用程序敏感数据和代码,用于数据安全传输,并保证隐私数据的安全。

[0012] 该数据提供方使用区块链发布元数据,并给数据分析方传输公钥加密后的原始数据,以及远程认证中对数据分析方身份的验证和传递私钥;

[0013] 所述数据分析方也注册为区块链节点,并且能够安装enclave分析程序。

[0014] 该数据分析方用于查看数据提供方的元数据和发送使用数据请求,并接受来自数据提供方已加密的原始数据,以及编写、安装分析程序和使用数据提供方发来的的私钥解密出数据提供方的原数据,然后在enclave内执行分析程序。

[0015] 所述区块链用于存储数据提供方的元数据以及数据提供方和数据分析方的公钥。

[0016] 一种基于区块链的跨平台的可信能源数据共享方法,包括以下步骤:

[0017] 步骤1、数据提供方发布元数据,数据分析方发出数据使用需求;

[0018] 步骤2、数据提供方发送加密的原始数据到数据分析方;

[0019] 步骤3、数据提供方和数据分析方双方之间进行远程认证;

[0020] 步骤4、数据分析方接收到数据提供方发来的私钥,然后执行程序,最终实现跨平台的可信能源数据共享。

[0021] 而且,所述步骤1的具体步骤包括:

[0022] (1)数据提供方i在区块链上发布其元数据

[0023] 所述元数据包括原始数据集的描述和哈希,其中哈希是具有恒定长度输出的抗冲

突函数；

[0024] (2)数据分析方从区块链上看到多个数据提供方的元数据，获取所有元数据的相关信息，确定哪些数据提供方的原始数据聚合后可得到所需的分析结果，并对相应数据提供方发出使用数据请求。

[0025] 而且，所述步骤2的具体步骤包括：

[0026] (1)相应的数据提供方i生成各自的密钥对(pk_i, sk_i)，利用各自公钥pk_i对其原始能源数据m_i进行加密；

[0027] (2)相应的数据提供方i将加密后的数据发送至数据分析方；

[0028] 而且，所述步骤3的具体步骤包括：

[0029] (1)数据分析方本地编写并安装分析程序的enclave，然后数据分析方将该enclave的代码公开，其中enclave是在Intel的SGX上运行的受信任程序；

[0030] (2)由相应的数据提供方i检查数据分析方已发布enclave的合法性，如果通过，相应的数据提供方i将在本地设置一个存储sk_i的新enclave，并建立对分析程序enclave的远程认证，如果目标enclave的哈希值等于所得的数据分析方分析程序enclave的哈希值，远程认证通过，然后将sk_i发送到目标enclave；

[0031] 而且，所述步骤4的具体步骤包括：

[0032] (1)数据分析方接受到数据提供方i的私钥sk_i，使用sk_i解密出数据提供方i的原始数据i

[0033] (2)判定原始数据i的哈希值与数据提供方i的元数据哈希值是否匹配，如果不匹配则返回信息“来自数据提供方i的数据是无效的”，如果匹配，则运行分析程序，得到多方能源数据提供方聚合和共享数据后的分析结果；

[0034] 其中数据提供方i的元数据哈希值是硬编码。

[0035] 本发明的优点和有益效果：

[0036] 1、本发明提出了一种基于区块链的跨平台的可信能源数据共享系统，多方能源数据在聚合和共享过程中，原始数据都没有离开安全域，即保证了数据提供者的可靠性，确保了数据隐私安全，保障了数据提供商和数据分析方双方的利益，使大范围内深度挖掘多种能源数据的统计价值成为可能，为政府等部门能源结构优化决策提供重要依据。

[0037] 2、本发明能够解决多个能源数据提供方把能源数据进行聚合和共享给数据分析方过程中隐私泄露、数据安全和数据利益受损的问题，通过密码学技术、可信执行环境(TEE)等技术，使数据在整个过程中不离开安全域，同时保证分析程序执行的可靠性，保护原始数据隐私不泄露、保证数据安全、维护数据提供商的利益，建立多方参与下可信能源数据的共享系统。

[0038] 3、本发明的数据提供方和数据分析方双方都安装可信执行环境TEE，防止数据分析方与原始数据接触，虽然原始数据跨平台，但由数据提供方本身生成密钥对，用其公钥对原始数据加密后传给数据分析方，能保证数据提供方是唯一拥有私钥的一方，而公钥的可信度是不言而喻的，保证了数据提供方的原始数据不出安全域，有效打消数据提供方的顾虑。

[0039] 4、本发明的分析程序在数据分析方的平台上执行，保证了分析结果的正确性，在区块链上实现跨平台、可信的多方能源数据共享系统。

附图说明

[0040] 图1是本发明的一种基于区块链的跨平台的可信能源数据共享系统的组成结构图；

具体实施方式

[0041] 以下对本发明实施例作进一步详述：

[0042] 一种基于区块链的跨平台的可信能源数据共享系统，如图1所示，包括：多个数据提供方、区块链和数据分析方，该多个数据提供方分别通过区块链和数据分析方相连接；

[0043] 所述多个数据提供方均已各自注册为区块链节点，每个数据提供方i(i＝1,2,3……)包含一对私钥sk_i和公钥pk_i，公钥pk_i用于加密原始数据，私钥sk_i用于解密原始数据，并且能够安装enclave，其中，enclave是在Intel的SGX上运行的受信任程序，可看成是一个被保护的内容容器，可以存放应用程序敏感数据和代码，用于数据安全传输，并保证隐私数据的安全；

[0044] 该数据提供方使用区块链发布元数据，并给数据分析方传输公钥加密后的原始数据，以及远程认证中对数据分析方身份的验证和传递私钥；

[0045] 所述数据分析方也注册为区块链节点，并且能够安装enclave分析程序。

[0046] 该数据分析方用于查看数据提供方的元数据和发送使用数据请求，并接受来自数据提供方已加密的原始数据，以及编写、安装分析程序和使用数据提供方发来的的私钥解密出数据提供方的原数据，然后在enclave内执行分析程序。

[0047] 区块链：所述区块链用于存储数据提供方的元数据以及数据提供方和数据分析方的公钥

[0048] 一种基于区块链的跨平台的可信能源数据共享方法，包括以下步骤：

[0049] 步骤1、数据提供方发布元数据，数据分析方发出数据使用需求；

[0050] 所述步骤1的具体步骤包括：

[0051] (1)数据提供方i在区块链上发布其元数据

[0052] 在本实施例中，所述元数据包括原始数据集的描述和哈希，其中哈希是具有恒定长度输出的抗冲突函数。

[0053] 元数据的准确度可参考在区块链上记录的元数据的“信用值”，它是购买相应数据的数据分析人员的反馈。信用值越高，元数据越可靠。

[0054] (2)数据分析方从区块链上看到多个数据提供方的元数据，获取所有元数据的相关信息，确定哪些数据提供方的原始数据聚合后可得到所需的分析结果，并对相应数据提供方发出使用数据请求

[0055] 步骤2、数据提供方发送加密的原始数据到数据分析方

[0056] 所述步骤2的具体步骤包括：

[0057] (1)相应的数据提供方i生成各自的密钥对(pk_i, sk_i)，利用各自公钥pk_i对其原始能源数据m_i进行加密

[0058] (2)相应的数据提供方i将加密后的数据发送至数据分析方；(通过正常传输通道)

[0059] 步骤3、数据提供方和数据分析方双方之间进行远程认证

[0060] 所述步骤3的具体步骤包括：

[0061] (1)数据分析方本地编写并安装分析程序的enclave，然后数据分析方将该enclave的代码公开，其中enclave是在Intel的SGX上运行的受信任程序

[0062] (2)由相应的数据提供方i检查数据分析方已发布enclave的合法性，如果通过，相应的数据提供方i将在本地设置一个存储sk_i的新enclave，并建立对分析程序enclave的远程认证，如果目标enclave的哈希值等于所得的数据分析方分析程序enclave的哈希值，远程认证通过，然后将sk_i发送到目标enclave

[0063] 步骤4、数据分析方接收到数据提供方发来的私钥，然后执行程序，最终实现跨平台的可信能源数据共享；

[0064] 所述步骤4的具体步骤包括：

[0065] (1)数据分析方接受到数据提供方i的私钥sk_i，使用sk_i解密出数据提供方i的原始数据i

[0066] (2)判定原始数据i的哈希值与数据提供方i的元数据哈希值是否匹配，如果不匹配则返回信息“来自数据提供方i的数据是无效的”，如果匹配，则运行分析程序，得到多方能源数据提供方聚合和共享数据后的分析结果；

[0067] 其中数据提供方i的元数据哈希值是硬编码的，硬编码是将数据直接嵌入到程序或其他可执行对象的源代码中的软件开发实践，硬编码数据通常只能通过编辑源代码和重新编译可执行文件来修改，所以硬编码的数据一般表示不容易改变的信息。

[0068] 本发明的工作原理是：

[0069] 多个数据提供方在区块链上发布各自的元数据，数据分析方看到多个元数据后，获取数据的相关信息，如果需要从元数据提供方的原始数据得到分析结果，就对相应的数据提供方发出使用数据的请求。多个数据提供方只需把其原始数据用自己的公钥加密后发送至数据分析方，数据分析方编写并安装分析程序的enclave，把元数据硬编码，然后把enclave代码公开。数据提供方检查数据分析方公布的enclave的合法性，如果通过，就在本地设置一个存储私钥的enclave，然后，建立对分析程序enclave的远程认证，如果是数据分析方发布的enclave的哈希值，则把私钥发送到数据分析方的enclave。数据分析方在本地使用私钥在enclave内执行分析程序，以获得分析结果。

[0070] 需要强调的是，本发明所述实施例是说明性的，而不是限定性的，因此本发明包括并不限于具体实施方式中所述实施例，凡是由本领域技术人员根据本发明的技术方案得出的其他实施方式，同样属于本发明保护的范围。

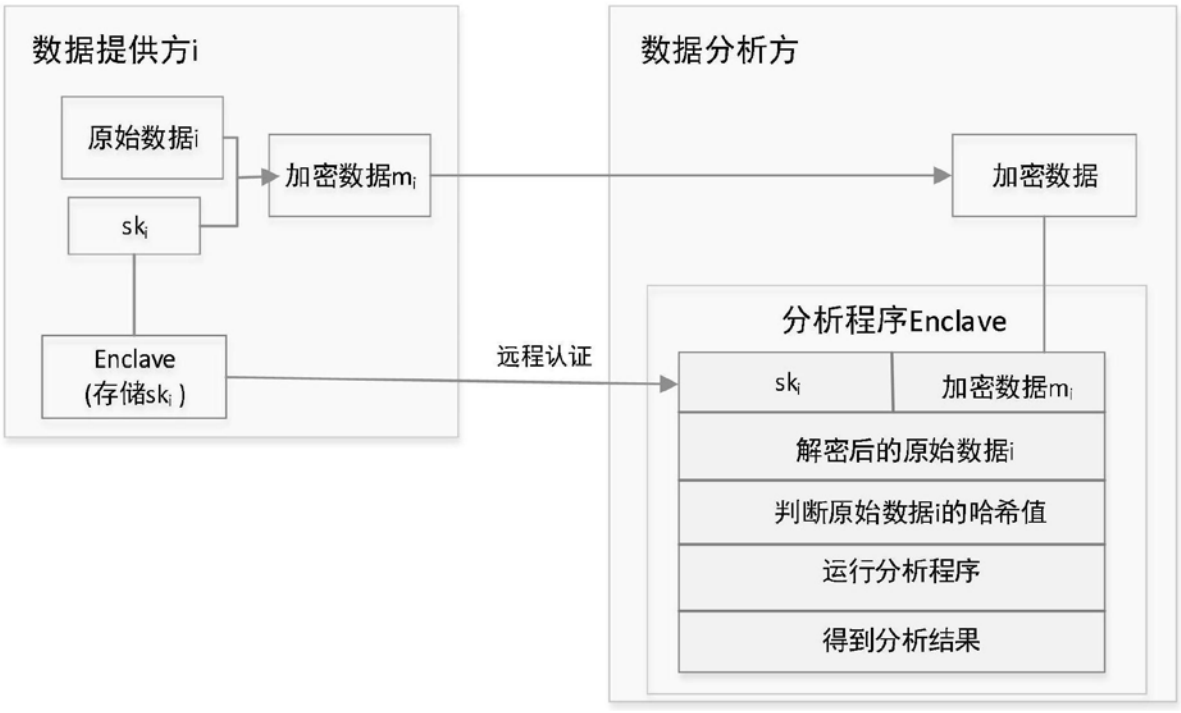

数据提供方i
原始数据i
加密数据m_i
sk_i
Enclave
(存储sk_i)
远程认证
数据分析方
加密数据
分析程序Enclave
sk_i
加密数据m_i
解密后的原始数据i
判断原始数据i的哈希值
运行分析程序
得到分析结果

图1