(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 112487470 A
(43)申请公布日 2021.03.12

(21)申请号 201910856247.6

(22)申请日 2019.09.11

(71)申请人 浙江宇视科技有限公司
地址 310000 浙江省杭州市滨江区西兴街道江陵路88号10幢南座1-11层、2幢A区1-3楼、2幢B区2楼

(72)发明人 黄黎滨

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
代理人 张磊

(51)Int.Cl.
G06F 21/62(2013.01)

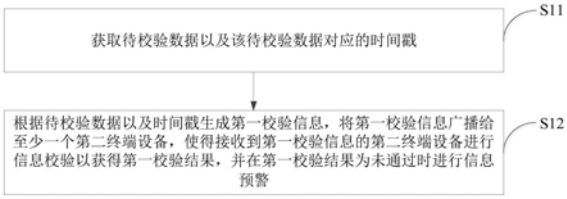
权利要求书3页 说明书13页 附图3页

(54)发明名称

信息校验方法、装置、终端设备和计算机可读存储介质

(57)摘要

本申请实施例提出一种信息校验方法、装置、终端设备和计算机可读存储介质，涉及信息安全技术领域。在本申请实施例中，第一终端设备获取待校验数据以及该待校验数据对应的时间戳；根据待校验数据以及时间戳生成第一校验信息，将第一校验信息广播给至少一个第二终端设备，使得接收到第一校验信息的第二终端设备进行信息校验以获得第一校验结果，并在第一校验结果为未通过时进行信息预警。本申请能够有效降低终端被非法篡改的风险。



CN 112487470 A

1.一种信息校验方法,其特征在于,应用于分布式系统中的第一终端设备,该分布式系统还包括与所述第一终端设备通信连接的第二终端设备,所述方法包括:

获取待校验数据以及该待校验数据对应的时间戳;

根据所述待校验数据以及所述时间戳生成第一校验信息,将所述第一校验信息广播给至少一个所述第二终端设备,使得接收到所述第一校验信息的第二终端设备进行信息校验以获得第一校验结果,并在所述第一校验结果为未通过时进行信息预警。

2.根据权利要求1所述的信息校验方法,其特征在于,所述方法还包括:

接收所述第二终端设备反馈的校验规则,该校验规则用于进行再次信息校验;

按照所述校验规则生成二次校验信息,并将所述二次校验信息发送给反馈所述校验规则的第二终端设备,以使得该第二终端设备根据所述二次校验信息进行再次信息校验以获得二次校验结果,并在所述二次校验结果为校验未通过时进行信息预警。

3.根据权利要求2所述的信息校验方法,其特征在于,所述校验规则中包括加密信息以及该加密信息对应的加密位置,所述按照所述校验规则生成二次校验信息的步骤,包括:

提取所述校验规则中包括的加密信息以及加密位置;

按照所述加密位置在预设的待加密数据中叠加所述加密信息得到所述二次校验信息。

4.根据权利要求3所述的信息校验方法,其特征在于,所述加密信息包括随机数、符号、图片和文字中的至少一种。

5.根据权利要求1所述的信息校验方法,其特征在于,当待校验数据作为待同步数据时,所述方法还包括:

发送携带有所述第一终端设备的终端标识的所述待同步数据给第二终端设备,使得该第二终端设备根据所述终端标识验证所述待同步数据的合法性,并在所述待同步数据为合法时,对所述待同步数据进行哈希运算得到待同步哈希值,将所述待同步哈希值与保存的哈希值进行比对,在比对结果一致时根据所述待同步数据进行数据同步更新。

6.一种信息校验方法,其特征在于,应用于分布式系统中的第二终端设备,该分布式系统还包括与所述第二终端设备通信连接的第一终端设备,所述方法包括:

获取第一终端设备广播的第一校验信息,其中,所述第一校验信息为所述第一终端设备根据获取的待校验数据及该待校验数据对应的时间戳所生成;

对所述第一校验信息进行信息校验,得到第一校验结果,并将所述第一校验结果发送至所述第一终端设备,以在所述第一校验结果为未通过时进行信息预警。

7.根据权利要求6所述的信息校验方法,其特征在于,所述对所述第一校验信息进行信息校验,得到第一校验结果的步骤,包括:

根据所述第一校验信息携带的终端标识确定出设备公钥,根据所述设备公钥验证所述第一校验信息是否为与所述终端标识对应的第一终端设备发送;

当所述第一校验信息不是与所述终端标识对应的第一终端设备发送时,判定校验未通过,并生成所述第一校验结果。

8.根据权利要求7所述的信息校验方法,其特征在于,所述对所述第一校验信息进行信息验证,得到第一校验结果的步骤,还包括:

当所述第一校验信息是与所述终端标识对应的第一终端设备发送时,检测是否保存有与所述终端标识对应的第一终端设备的校验信息;

若保存有与所述终端标识对应的第一终端设备的校验信息，则继续判断保存的校验信息与所述第一校验信息是否一致，若一致，则判定校验通过，并生成所述第一校验结果。

9.根据权利要求8所述的信息校验方法，其特征在于，所述判断保存的校验信息与所述第一校验信息是否一致的步骤，包括：

利用自身的私钥对所述第一校验信息进行解密得到待校验哈希值和待校验时间戳；

判断所述待校验哈希值和待校验时间戳与所述保存的校验信息中的哈希值和时间戳是否一致；

当所述待校验哈希值与所述保存的校验信息中的哈希值一致，且所述待校验时间戳与所述保存的校验信息中的时间戳一致时，判定所述保存的校验信息与所述第一校验信息一致；反之，判定所述保存的校验信息与所述第一校验信息不一致。

10.根据权利要求9所述的信息校验方法，其特征在于，当所述保存的校验信息与所述第一校验信息不一致，所述方法还包括：

若所述待校验哈希值与所述保存的校验信息中的哈希值不一致，且所述待校验时间戳与所述保存的校验信息中的时间戳一致，则进行数据篡改预警；或者

若所述待校验哈希值与所述保存的校验信息中的哈希值不一致，且所述待校验时间戳相对于所述保存的校验信息中的时间戳较新，则生成用于再次进行信息校验的校验规则，该校验规则包括用于进行加密的加密信息以及该加密信息对应的加密位置；

反馈所述校验规则给发送所述第一校验信息的第一终端设备，以使所述第一终端设备根据所述校验规则生成二次校验信息；

接收所述第一终端发送的二次校验信息，对所述二次校验信息进行信息校验，得到二次校验结果，并将所述二次校验结果发送至所述第一终端设备，以在所述二次校验结果为校验未通过时进行信息预警。

11.根据权利要求10所述的信息校验方法，其特征在于，所述对所述二次校验信息进行信息校验，得到二次校验结果的步骤，包括：

从所述二次校验信息中提取加密信息，比对提取到的加密信息与所述校验规则中的加密信息是否一致；

若一致，则判定校验通过，并生成二次校验结果，以及将保存的校验信息中的哈希值更改为所述第一校验信息中的哈希值。

12.一种信息校验装置，其特征在于，应用于分布式系统中的第一终端设备，该分布式系统还包括与所述第一终端设备通信连接的多个第二终端设备，所述装置包括：

第一数据获取模块，用于获取待校验数据以及该待校验数据对应的时间戳；

第一信息校验模块，用于根据所述待校验数据以及所述时间戳生成第一校验信息，将所述第一校验信息广播给至少一个第二终端设备，使得接收到所述第一校验信息的第二终端设备进行信息校验以获得第一校验结果，并在所述第一校验结果为未通过时进行信息预警。

13.一种信息校验装置，其特征在于，应用于分布式系统中的第二终端设备，该分布式系统还包括与所述第二终端设备通信连接的第一终端设备，所述装置包括：

第二信息获取模块，用于获取第一终端设备广播的第一校验信息，其中，所述第一校验信息为所述第一终端设备根据获取的待校验数据及该待校验数据对应的时间戳所生成；

第二信息校验模块，用于对所述第一校验信息进行信息校验，得到第一校验结果，并将所述第一校验结果发送至所述第一终端设备，以在所述第一校验结果为未通过时进行信息预警。

14.一种终端设备，其特征在于，包括处理器和存储器，所述存储器存储有能够被所述处理器执行的机器可执行指令，所述处理器可执行所述机器可执行指令以实现权利要求1-5或权利要求6-11任一所述的信息校验方法。

15.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1-5或权利要求6-11中任一项所述的信息校验方法。

信息校验方法、装置、终端设备和计算机可读存储介质

技术领域

[0001] 本申请涉及信息安全技术领域，具体而言，涉及一种信息校验方法、装置、终端设备和计算机可读存储介质。

背景技术

[0002] 随着如人脸布控等智能业务的广泛应用，终端智能化程度越来越高，终端数据的安全性也变得尤为重要，一旦终端被非法侵入修改，造成的危害是非常巨大的。例如，对于现有的包括数据中心以及多个监控终端的分布式智能监控系统而言，为了提高监控过程中涉及的数据比对等业务的时效性，布控数据一般保存在监控终端中。那么，一旦数据中心被攻击则也会导致所有监控终端上的布控数据都存在被篡改的风险。

发明内容

[0003] 有鉴于此，本申请的目的在于提供一种信息校验方法、装置、终端设备和计算机可读存储介质，能够有效降低终端设备被非法篡改的风险。

[0004] 为了实现上述目的，本申请实施例采用的技术方案如下：

[0005] 第一方面，本申请实施例提供一种信息校验方法，应用于分布式系统中的第一终端设备，该分布式系统还包括与所述第一终端设备通信连接的第二终端设备，所述方法包括：

[0006] 获取待校验数据以及该待校验数据对应的时间戳；

[0007] 根据所述待校验数据以及所述时间戳生成第一校验信息，将所述第一校验信息广播给至少一个所述第二终端设备，使得接收到所述第一校验信息的第二终端设备进行信息校验以获得第一校验结果，并在所述第一校验结果为未通过时进行信息预警。

[0008] 第二方面，本申请实施例提供一种信息校验方法，应用于分布式系统中的第二终端设备，该分布式系统还包括与所述第二终端设备通信连接的第一终端设备，所述方法包括：

[0009] 获取第一终端设备广播的第一校验信息，其中，所述第一校验信息为所述第一终端设备根据获取的校验数据及该校验数据对应的时间戳所生成；

[0010] 对所述第一校验信息进行信息校验，得到第一校验结果，并将所述第一校验结果发送至所述第一终端设备，以在所述第一校验结果为未通过时进行信息预警。

[0011] 第三方面，本申请实施例提供一种信息校验装置，应用于分布式系统中的第一终端设备，该分布式系统还包括与所述第一终端设备通信连接的多个第二终端设备，所述装置包括：

[0012] 第一数据获取模块，用于获取待校验数据以及该待校验数据对应的时间戳；

[0013] 第一信息校验模块，用于根据所述待校验数据以及所述时间戳生成第一校验信息，将所述第一校验信息广播给至少一个第二终端设备，使得接收到所述第一校验信息的第二终端设备进行信息校验以获得第一校验结果，并在所述第一校验结果为未通过时进行

信息预警。

[0014] 第四方面，本申请实施例提供一种信息校验装置，应用于分布式系统中的第二终端设备，该分布式系统还包括与所述第二终端设备通信连接的第一终端设备，所述装置包括：

[0015] 第二数据获取模块，用于获取第一终端设备广播的第一校验信息，其中，所述第一校验信息为所述第一终端设备根据获取的待校验数据及该待校验数据对应的时间戳所生成；

[0016] 第二信息校验模块，用于对所述第一校验信息进行信息校验，得到第一校验结果，并将所述第一校验结果发送至所述第一终端设备，以在所述第一校验结果为未通过时进行信息预警。

[0017] 第五方面，本申请实施例提供一种终端设备，包括处理器和存储器，所述存储器存储有能够被所述处理器执行的机器可执行指令，所述处理器可执行所述机器可执行指令以实现上述任一实施例提供的信息校验方法。

[0018] 第六方面，本申请实施例提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述任一实施例提供的信息校验方法。

[0019] 本申请实施例提供的信息校验方法、装置、终端设备和计算机可读存储介质中，在分布式系统中的第二终端设备的协助下实现对第一终端设备上获取的待校验信息的信息校验，能够有效避免第一终端设备上的数据被非法篡改的问题发生，提高了分布式系统中各终端设备的安全性。

[0020] 为使本申请的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

[0021] 为了更清楚地说明本申请实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，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，还可以根据这些附图获得其他相关的附图。

[0022] 图1示出了本申请实施例提供的分布式系统的方框结构示意图；

[0023] 图2示出了本申请实施例提供的应用于第一终端设备的信息校验方法的流程示意图；

[0024] 图3示出了本申请实施例提供的应用于第一终端设备的信息校验方法的另一流程示意图；

[0025] 图4示出了本申请实施例提供的应用于第二终端设备的信息校验方法的流程示意图；

[0026] 图5示出了本申请实施例提供的终端设备的方框结构示意图；

[0027] 图6示出了本申请实施例提供的应用于第一终端设备的信息校验装置的功能模块示意图；

[0028] 图7示出了本申请实施例提供的应用于第二终端设备的信息校验装置的功能模块示意图。

[0029] 图标:10-分布式系统;20-终端设备;211-第一数据获取模块;212-第一信息校验模块;213-第二数据获取模块;214-第二信息校验模块;22-处理器;23-存储器;24-通信模块;30-客户端。

具体实施方式

[0030] 经研究发现,在现有的分布式系统中,当需要对分布式系统中的终端设备进行配置管理时,一般的配置过程包括:用户通过客户端登录数据中心对需要新增的终端设备进行注册,并在注册完成的终端设备上线后,通过数据中心向该终端设备下发配置数据并根据该配置数据进行终端配置。同时,数据中心会对下发的配置数据进行备份,而终端设备也会保存用于对数据中心的合法性进行校验的校验数据。

[0031] 对于前述基于数据中心实现的中心化的分布式系统,一旦数据中心被攻破、侵占,该数据中心所在的分布式系统中的配置数据等将可能被全部篡改,导致分布式系统中的全部终端设备被攻占、篡改。对于前述基于中心化的分布式系统中存在的设备被篡改的问题,本申请给出一种弱中心化的信息校验方法、装置、终端设备和计算机可读存储介质,将分布式系统中防止设备信息篡改任务分散至该分布式系统中的所有设备(如终端设备、数据中心等),以降低终端设备被非法篡改的风险。下面将结合本申请实施例中附图,对本申请实施例中的技术方案进行清楚、完整地描述。

[0032] 应注意,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。通常在此处附图中描述和示出的本申请实施例的组件可以以各种不同的配置来布置和设计。因此,以下对在附图中提供的本申请的实施例的详细描述并非旨在限制要求保护的本申请的范围,而是仅仅表示本申请的选定实施例。基于本申请的实施例,本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0033] 需要说明的是,术语“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。

[0034] 实施例一

[0035] 请参阅图1,为本申请实施例一提供的分布式系统10的示意图,该分布式系统10包括多个能够互相通信的终端设备20,各终端设备20可具有相同或不同的型号、配置等。在本实施例一中,为了能够清楚的描述应用于分布式系统10的信息校验方法,通过术语“第一”、“第二”对不同场景下扮演不同角色的终端设备20进行区分,如第一终端设备、第二终端设备等。换言之,第一终端设备与第二终端设备为硬件设备相同、功能相同的终端设备,第一终端设备和第二终端设备可以互换角色,以实现不同场景下的信息校验。另外,在一些实现方式中,数据中心可以作为多个终端设备20中的一个,与各终端设备20共同实现信息校验,本实施例在此不做具体限制。

[0036] 实施例二

[0037] 请结合参阅图2,为本申请实施例提供的应用于分布式系统10中的任意一个终端设备20(为便于区分,该终端设备20在以下内容中统称为第一终端设备,其它的终端设备20统称为第二终端设备)的信息校验方法的流程示意图,该信息校验方法可以由信息校验装置来执行,该信息校验装置可以由软件或/和硬件实现,可配置在安装有如安卓(Android)等操作系统的终端设备20中,该终端设备20可以是、但不限于计算机、手机、IPad、服务器、移动上网设备等中。所应说明的是,本实施例一中给出的信息校验方法并不以图2以及以下的具体顺序为限制。下面结合图2对信息校验方法的具体流程进行阐述,内容如下。

[0038] 步骤S11,获取待校验数据以及该待校验数据对应的时间戳。

[0039] 其中,待校验数据可以是,但不限于,客户端30、数据中心、非法终端等向第一终端设备下发的数据,如配置参数、需要修改的配置参数、待同步数据等。时间戳可以是客户端30、数据中心或非法终端向第一终端设备下发待校验数据的时间,还可以是第一终端设备获取到待校验数据的时间等。

[0040] 需要说明的是,在第一终端设备检测到自身的配置参数被修改或接收到需要通过自身同步至分布式系统10中的第二终端设备的待同步数据时,即可将修改后的数据或需要同步的待同步数据作为待校验数据,以用于后续的信息校验,确保自身数据不被非法篡改。

[0041] 步骤S12,根据待校验数据以及时间戳生成第一校验信息,将第一校验信息广播给至少一个第二终端设备,使得接收到第一校验信息的第二终端设备进行信息校验以获得第一校验结果,并在第一校验结果为未通过时进行信息预警。

[0042] 其中,根据实际需求的不同,如不同要求的安全等级等,第一终端设备在对第一校验信息进行广播时,可以将第一校验信息广播给分布式系统10中的全部第二终端设备进行全局校验;为了提高校验效率,也可以将第一校验信息仅广播给分布式系统10中的部分第二终端设备以进行小范围的信息校验等。

[0043] 另外,本实施例中的第一校验信息的生成方式可以有多种,例如,可以利用现有的加密算法对待校验数据和时间戳进行加密,得到第一校验信息;又例如,也可以提取第一校验信息中的部分信息与时间戳一起生成第一校验信息;又例如,还可以是利用公私钥加密以及哈希运算来对待校验信息和时间戳进行处理得到第一校验信息等。

[0044] 作为一种实现方式,下面以利用公私钥加密以及哈希运算为例并结合下述步骤S120至步骤S122对第一校验信息的生成过程进行简单介绍,内容如下。

[0045] 步骤S120,对待校验数据以及第一终端设备的唯一标识信息进行哈希运算得到哈希值。其中,第一终端设备的唯一标识信息可以是,但不限于,第一终端设备的序列号、型号、设备名称、物理地址等。

[0046] 步骤S121,利用至少一个第二终端设备的设备公钥对哈希值和时间戳进行加密,得到与至少一个第二终端设备对应的至少一个加密信息。

[0047] 步骤S122,利用第一终端设备的私钥对至少一个加密信息进行签名得到至少一个第一校验信息。

[0048] 其中,在步骤S120至步骤S122中,第一终端设备在计算得到哈希值后,需要确定是由分布式系统10中的部分第二终端设备进行信息校验还是全部第二终端设备进行信息校验。当完成第二终端设备的确定后,第一终端设备可利用确定后的第二终端设备的设备公钥对哈希值和时间戳进行加密,得到与各第二终端设备对应的一个或多个加密信息。再利

用私钥对每个加密信息进行签名得到至少一个第一校验信息。最后，根据至少一个第一校验信息对应的设备公钥的不同，将各第一校验信息广播给对应的第二终端设备。

[0049] 可以理解的是，第一终端设备中可预先保存有分布式系统10中的各第二终端设备的设备公钥。实际实施时，设备公钥可以由数据中心将各个第二终端设备的设备公钥统一下发给第一终端设备后进行保存，也可以是由各第二终端设备将自身的设备公钥广播给其他终端设备20，如第一终端设备等，本实施例在此不做限制。

[0050] 另外，在本实施例中，步骤S12中所述的接收到第一校验信息的第二终端设备进行信息校验的具体过程(即第一校验结果的获取过程)可以根据实际需求进行设定。例如，在一种实现方式中，假设第一校验信息中携带有发送该第一校验信息的终端设备的终端标识，那么，第二终端设备根据第一校验信息进行信息校验的校验过程可以通过步骤S123至步骤S124实现，内容如下。

[0051] 步骤S123，第二终端设备根据第一校验信息携带的终端标识确定出设备公钥，根据设备公钥验证第一校验信息是否为与终端标识对应的第一终端设备发送。应注意的是，终端标识与前述的唯一标识信息可以相同，也可以不同，本实施例在此不做限制。

[0052] 步骤S124，当第一校验信息不是与终端标识对应的第一终端设备发送时，判定校验未通过，并生成第一校验结果发送给第一终端设备使得该第一终端设备根据校验结果进行信息预警；反之，则判定校验通过，以及生成第一校验结果给第一终端设备。

[0053] 上述步骤S123至步骤S124中给出的信息校验过程中，第二终端设备是利用携带于第一校验信息中的终端标识实现对第一终端设备发过来的信息的合法性的校验。同时，第一终端设备根据接收到的第一校验结果判断是否进行信息预警，能够有效防止终端设备20被非法篡改，提高终端设备20上的信息安全性。

[0054] 此外，作为一种可能的实施方式，在第二终端设备所生成的第一校验结果为校验未通过时，该第二终端设备自身也可在校验未通过时进行信息预警。作为另一种可能的实施方式，在第二终端设备所生成的第一校验结果为校验未通过时，可以将校验未通过的信息发送至数据中心，使得数据中心根据该校验未通过的信息进行信息预警。

[0055] 也即，在第二终端设备所生成的第一校验结果为校验未通过时，第二终端设备、第一终端设备及数据中心中至少一方将进行信息预警，本实施例对此不作具体限制。

[0056] 应注意，除上述步骤S123至步骤S124中给出的校验过程外，为了进一步提高信息校验结果的准确性，防止终端设备20上的信息被非法篡改。作为另一种实现方式，第二终端设备还可以在基于终端标识的信息校验结果为校验通过时，检测自身是否保存有与终端标识对应的终端设备的校验信息；若保存有与终端标识对应的终端设备的校验信息，则继续判断保存的校验信息与第一校验信息是否一致，若一致，则判定校验通过，并生成第一校验结果给第一终端设备。可以理解的是，当信息校验方法还包括如前述判断保存的校验信息与第一校验信息是否一致的步骤时，那么第二终端设备可以不反馈基于终端标识进行信息校验的校验结果给第一终端设备。

[0057] 此外，当第二终端设备未保存有与终端标识对应的终端设备20的校验信息时，第二终端设备将第一校验信息与第一终端设备进行对应保存，用于后续的信息校验。进而使得分布式系统10中的各终端设备20可通过校验信息的相互备份实现对接收到的校验信息的校验，提高终端设备20上的数据的安全性。应注意，若第二终端设备中未保存有与终端标

识对应的终端设备20的校验信息，且基于设备公钥进行信息校验得到的第一校验结果为校验通过时，第一终端设备可以以第一校验结果作为与该第二终端设备对应的校验结果，也可以忽略该第二终端设备，并取消该第二终端设备参与信息校验的资格，本实施例在此不做限制。

[0058] 作为一种可选的实现方式，下面结合步骤S125至步骤S127对第二终端设备判断保存的校验信息与第一校验信息是否一致的判断过程进行介绍。

[0059] 步骤S125，利用自身的私钥对第一校验信息进行解密得到待校验哈希值和待校验时间戳。

[0060] 步骤S126，判断待校验哈希值和待校验时间戳与保存的校验信息中的哈希值和时间戳是否一致。

[0061] 步骤S127，当待校验哈希值与保存的校验信息中的哈希值一致，且待校验时间戳与保存的校验信息中的时间戳一致时，判定保存的校验信息与第一校验信息一致；反之，判定保存的校验信息与第一校验信息不一致。

[0062] 在一些实现方式中，步骤S125至步骤S127中所述的保存的校验信息与第一校验信息不一致的情况可以有：待校验哈希值与保存的校验信息中的哈希值不致，但待校验时间戳与保存的校验信息中的时间戳一致；或者待校验哈希值与保存的校验信息中的哈希值不一致，且待校验时间戳相对于保存的校验信息中的时间戳较新等，本实施例在此不做限制。例如，假设已保存的校验信息中的时间戳为2019年7月5日13时52分，而待校验时间戳为2019年7月8日21时13分，那么，可以判定待校验时间戳相对于保存的校验信息中的时间戳较新。

[0063] 应注意，第一终端设备在根据第二终端设备反馈的第一校验结果确定是否为校验通过时，可以是在全部第二终端设备反馈的第一校验结果为校验通过时，判定校验通过，即第一终端设备未被非法篡改。也可以是当反馈第一校验结果为校验通过的第二终端设备的比例达到预设值(如90％、99％等)时，判定校验通过，即第一终端设备未被非法篡改，本实施例在此不做限制。反之，则根据校验结果进行预警，以告知工作人员等第一终端设备存在非法篡改或攻占风险。

[0064] 为了进一步对本实施例中给出的信息校验方法的实现过程进行说明，假设在分布式系统10中包括发起信息校验的终端设备20为第一终端设备A，协助进行信息校验的终端设备20为第二终端设备B1、B2、B3，那么，由客户端30向第一终端设备A下发待校验数据，该第一终端设备A请求第二终端设备B1、B2、B3协助进行校验的校验过程可以包括：

[0065] (1)客户端30向第一终端设备A下发配置参数。

[0066] (2)第一终端设备A根据接收到的配置参数进行终端配置，以及将该配置参数作为待校验数据，并获取客户端30下发待校验数据的时间戳。

[0067] (3)第一终端设备A对待校验数据以及自身的序列号(唯一标识信息)进行哈希运算得到哈希值。然后，再分别利用第二终端设备B1、B2、B3的设备公钥C1、C2、C3对哈希值和时间戳进行加密，得到与第二终端设备B1、B2、B3分别对应的三个加密信息D1、D2、D3。在本实施例的一种实现方式中，利用自身的私钥A1对加密信息D1、D2、D3进行签名得到第一校验信息E1、E2、E3。最后，第一终端设备A将第一校验信息E1、E2、E3分别按照加密公钥的不同广播给第二终端设备B1、B2、B3。

[0068] (4)在第二终端设备B1、B2、B3接收到对应的第一校验信息后，分别对该第一校验信息进行校验。其中，以第二终端设备B1对接收到第一校验信息E1进行校验的校验过程为例进行说明，第二终端设备B1在接收到的第一校验信息E1后，可根据该第一校验信息E1中携带的终端标识确定设备公钥X，并利用该设备公钥X验证第一校验信息E1是否为与设备公钥X对应的终端设备发送。其中，当第一校验信息E1不是与设备公钥X对应的终端设备发送时，则判定校验未通过，并反馈第一校验结果给第一终端设备A，该第一终端设备A进行数据篡改预警。反之，则判定校验通过。

[0069] 作为又一种实现方式，当第一校验信息E1是与设备公钥X对应的终端设备发送，且第二终端设备B1中保存有与设备公钥X对应的终端设备20的校验信息时，第二终端设备可继续比对已保存的校验信息与第一校验信息E1是否一致，并根据比对结果反馈第一校验结果给第一终端设备以执行对应的处理策略。

[0070] 其中，在第二终端设备B1判断已保存的校验信息与第一校验信息E1是否一致时，首先利用自身的私钥对第一校验信息E1进行解密得到待校验哈希值和待校验时间戳，然后判断待校验哈希值和待校验时间戳与已保存的校验信息中的哈希值和时间戳是否一致，一般可包括以下两种判断结果。

[0071] (a)当待校验哈希值与保存的校验信息中的哈希值一致，且待校验时间戳与保存的校验信息中的时间戳一致时，判定保存的校验信息与第二校验信息一致，则检验通过，并反馈第一校验结果给第一终端设备A。

[0072] (b)当待校验哈希值与保存的校验信息中的哈希值不一致，且待校验时间戳与保存的校验信息中的时间戳一致时，或者，当待校验哈希值与保存的校验信息中的哈希值不一致，且待校验时间戳相对于保存的校验信息中的时间戳较新时，判定保存的校验信息与第一校验信息不一致，校验未通过，反馈第一校验结果给第一终端设备A，同时进行数据篡改预警。

[0073] 综上，与现有技术中基于中心化的分布式系统10相比，本实施例给出的信息校验方法中不依赖于数据中心进行信息校验，而是在第一终端设备获取到客户端30或数据中心下发的待校验数据后，利用分布式系统10中的至少一个第二终端设备对获取到待校验数据进行校验，进而根据参与信息校验的第二终端设备反馈的校验结果判断是否需要进行报警，从而避免第一终端设备被非法篡改，提高分布式系统10中的各终端设备20上的数据的安全性。

[0074] 换言之，本申请通过弱中心化(基于多个第二终端设备)的信息校验方式，有效降低了分布式系统10中的终端设备20或数据中心被非法篡改、侵占的风险，提高了在进行终端设备20上的数据同步或参数修改时的数据安全性。

[0075] 实施例三

[0076] 在上述实施例二的基础上，考虑到第二终端设备反馈的第一校验结果为校验不通过时，可能是由于设备信息被非法篡改或侵入导致的校验不通过(如待校验哈希值与保存的校验信息中的哈希值不一致，且待校验时间戳与保存的校验信息中的时间戳一致)，也有可能是由于进行正常的设备信息修改导致的校验不通过(如待校验哈希值与保存的校验信息中的哈希值不一致，且待校验时间戳相对于保存的校验信息中的时间戳较新时)。因此，本实施例在前述实施例二给出的信息校验方法的基础上增加二次校验过程，以对发送第一

校验信息的第一终端设备的运行状态或身份合法性进行核对，进而有效区分第一终端设备获取的待校验信息是否为正常修改，以避免误判结果的出现，确保能够实现对分布式系统10中的终端设备20上的信息的正常修改。在本实施例中，该二次校验过程可通过如图3所示的步骤S14和步骤S15实现，内容如下。

[0077] 步骤S14，接收第二终端设备反馈的校验规则，该校验规则用于进行再次信息校验。

[0078] 其中，校验规则是由校验不通过的第二终端设备生成并反馈，以用于对发送第一校验信息的第一终端设备的身份的合法性或者第一终端设备是否正常运行进行再次校验，进而判断第一校验信息与已保存的校验信息不一致是否为正常的信息修改导致的。应注意的是，第一终端设备在根据接收到的校验规则生成二次校验信息时，可以是在接收到的第二终端设备反馈的第一校验结果为校验不通过的数量与参与信息校验的全部终端设备20的数量的比值达到预设值(如20％)时即根据校验规则生成二次校验信息；也可以是只要接收到第二终端设备反馈的第一校验结果为校验不通过时即根据校验规则生成二次校验信息，本实施例在此不做限制。

[0079] 可选地，作为一种可选的实现方式，校验规则的生成过程可根据实际需求进行设定，例如，在本实施例中，校验规则中可以包括第一终端设备用于生成二次校验信息的加密信息以及该加密信息对应的加密位置。其中，加密信息可以由第二终端设备根据实际情况随机生成，如加密信息可以包括图片、文字、符号、随机数等中的一种或多种，本实施例在此不做限制。

[0080] 步骤S15，按照校验规则生成二次校验信息，并将二次校验信息发送给反馈校验规则的第二终端设备，以使得该第二终端设备根据二次校验信息进行再次信息校验以获得二次校验结果，并在二次校验结果为校验未通过时进行信息预警。

[0081] 其中，在一些实现方式中，当校验规则中包括加密信息以及该加密信息对应的加密位置时，步骤S15中的按照校验规则生成二次校验信息的过程可以包括：第一终端设备提取校验规则中包括的加密信息以及加密位置，并按照加密位置在预设的待加密数据中叠加加密信息得到二次校验信息。

[0082] 可选地，预设的待加密数据可以是预先保存在第一终端设备中，也可以是由第二终端设备通过校验规则进行实时指定等，本实施例在此不做限制。例如，假设预设的待加密数据为图片，第一终端设备可根据加密位置在图片的对应位置叠加加密信息后得到二次校验信息。

[0083] 应注意的是，当第二终端设备根据二次校验信息进行二次信息校验并生成二次校验结果的过程可以包括：可按照加密位置等从二次校验信息中提取加密信息，比对提取到的加密信息与校验规则中的加密信息是否一致；若一致，则判定校验通过，并生成二次校验结果反馈给第一终端设备，以及将保存的校验信息中的哈希值更改为第一校验信息中的哈希值。反之，若提取到的加密信息与校验规则中的加密信息不一致，则判定第一终端设备无法正常运行，可能存在被侵占或非法篡改的问题，并向数据中心或客户端30等进行信息篡改预警。

[0084] 换言之，当第二终端设备基于第一终端设备发送的二次校验信息判定二次校验通过时，即可判定第一终端设备的身份为合法的，即第一终端设备未出现非法篡改问题或者

未被非法攻占，那么，可进一步根据第一终端设备发送的第一校验信息对已保存的与第一终端设备对应的校验信息进行更改、备份，以用于后续的信息校验。

[0085] 基于上述实施例二给出的信息校验方法的描述，在本实施例中，假设第二终端设备B1、B2、B3在基于第一校验信息进行信息校验时，第二终端设备B1将接收到的第一校验信息与已保存的校验信息进行比对后，比对结果为：待校验哈希值与保存的校验信息中的哈希值不一致，且待校验时间戳相对于保存的校验信息中的时间戳较新，即二者不一致，那么，第二终端设备B1可生成用于再次进行信息校验的校验规则；并利用第一终端设备A的设备公钥对校验规则进行加密后发送给该第一终端设备A。

[0086] 第一终端设备A接收到的校验规则后，根据该校验规则生成二次校验信息并发送给第二终端设备B1进行再次信息校验。第二终端设备B1提取二次校验信息中的加密信息，并将该加密信息与发送的校验规则中的加密信息进行比对，若一致，则将自身已保存的校验信息中的哈希值更改为第一校验信息中的哈希值，若不一致，则进行数据篡改预警，并反馈二次校验结果给第一终端设备。

[0087] 综上，相对于现有技术，本实施例给出的信息校验方法中，第一终端设备根据第二终端设备反馈的校验规则在预设的加密数据的指定位置叠加加密信息，以生成二次校验信息并发送给第二终端设备，该第二终端设备根据二次校验信息来对第一终端设备的身份的合法性进行二次检验，以核对第一终端设备上的程序是否还在正常运行，进而验证第一终端设备是否被非法侵占。如果第二终端设备基于通过前述二次校验信息进行信息校验的校验结果再次为校验通过时，则可判定第一终端设备运行正常，即证明该第一终端设备获取的待校验数据为正常的修改流程对应的数据，从而一方面有效区分了产生待校验数据的方式是否为正常的数据修改流程，另一方面还进一步确保了终端设备20的安全性。

[0088] 此外，一般的侵占篡改数据有两种情况，一种仅仅是入侵后篡改数据，对于这种情况通过定时的海量验证即可有效控制，只要有一台终端设备20验证失败，即可预警该终端设备20不可信。另一种是篡改数据的同时还恶意植入代码，这种情况下会将截取终端设备20所接收到的数据，并且可能模拟发送一些假数据，这种情况通过本申请实施例给出的二次校验的方式可以得到控制。设备状态确认时需要设备程序正常运行，在不破解代码程序的情况下，无法模拟得到合法的验证数据，当然破解代码源程序不在本方案的考虑范围。

[0089] 需要说明的是，在上述实施例二和实施例三中，由于在第一终端设备在执行上述实施例二和实施例三给出的信息校验的过程中，第一终端设备可能存在被侵占或非法篡改的风险。因此，在一些实现方式中，为了进一步提高分布式系统10中各终端设备20的安全性，当分布式系统10中的终端设备20在进行信息校验时，该终端设备20可停止接收其他待校验数据或执行其他数据业务，直至本次校验结束。

[0090] 实施例四

[0091] 当基于上述实施例二或/和实施例三给出的信息校验方法对待校验信息进行校验的校验结果为校验通过，且待校验信息为需要同步给该第二终端设备以使该第二终端设备根据待校验数据执行参数配置或其他操作时，信息校验方法还可包括：第一终端设备发送携带有第一终端设备的终端标识的待同步数据给第二终端设备，使得该第二终端设备根据终端标识验证待同步数据的合法性，并在待同步数据为合法时，对待同步数据进行哈希运算得到待同步哈希值，将待同步哈希值与保存的哈希值进行比对，以及在比对结果一致时

根据待同步数据进行数据同步更新。

[0092] 作为一种实现方式，基于上述实施例二或/实施例三给出的信息校验方法，假设待校验数据为待同步数据，该待同步数据需要同步给第二终端设备B3。那么，当第一终端设备A接收到的第二终端设备B1、B2、B3反馈的第一校验结果或二次校验结果为检验通过时，第一终端设备A可发送携带有自身终端标识的待校验数据给第二终端设备B3进行数据同步。

[0093] 在第二终端设备B3接收到的第一终端设备A发送的待校验数据时，将该待校验数据作为待同步数据，根据待同步数据中携带的终端标识确定用于验证待同步数据的合法性的设备公钥；当基于设备公钥验证待同步数据为合法时，对待同步数据进行哈希运算得到待同步哈希值；将待同步哈希值与保存的哈希值进行比对，若比对结果一致，则根据待同步数据进行数据同步更新，以实现终端配置。

[0094] 综上，相对于现有技术中通过数据中心进行终端设备20的配置方式，本实施例中通过终端设备20之间的数据同步实现终端配置更加方便、高效。此外，第二终端设备通过对接收到的待同步数据的进一步验证，能够进一步降低数据同步过程中的安全风险。

[0095] 实施例五

[0096] 本实施例提供一种信息校验方法，该信息校验方法应用于上述分布式系统中的第二终端设备，即第二终端设备作为第一终端设备的协助方，以协助第一终端设备完成信息校验。由上述可知，第一终端设备和第二终端设备为硬件设备相同、功能相同的终端设备，即上述第一终端设备可以实现该实施例中第二终端设备的功能，而该实施例中的第二终端设备也可以实现上述第一终端设备的功能。

[0097] 结合图4所示对第二终端设备进行信息校验的过程进行详细介绍，内容如下。所应说明的是，本实施例中给出的信息校验方法并不以图4以及以下的具体顺序为限制。

[0098] 步骤S21，获取第一终端设备广播的第一校验信息，其中，所述第一校验信息为所述第一终端设备根据获取的待校验数据及该待校验数据对应的时间戳所生成。

[0099] 步骤S22，对所述第一校验信息进行信息校验，得到第一校验结果，并将所述第一校验结果发送至所述第一终端设备，以在所述第一校验结果为未通过时进行信息预警。

[0100] 本实施例中，第二终端设备可以协助第一终端设备完成信息校验，避免了信息校验过程只能依赖数据中心所导致的信息易被非法篡改、数据安全性易受到威胁的弊端。

[0101] 作为一种可能的实施方式，第二终端设备根据第一校验信息进行信息校验，得到第一校验结果的过程具体可通过以下方式实现：

[0102] 根据所述第一校验信息携带的终端标识确定出设备公钥，根据所述设备公钥验证所述第一校验信息是否为与所述终端标识对应的第一终端设备发送。

[0103] 当所述第一校验信息不是与所述终端标识对应的第一终端设备发送时，判定校验未通过，并生成所述第一校验结果。

[0104] 而当所述第一校验信息是与所述终端标识对应的第一终端设备发送时，检测是否保存有与所述终端标识对应的第一终端设备的校验信息。

[0105] 若保存有与所述终端标识对应的第一终端设备的校验信息，则继续判断保存的校验信息与所述第一校验信息是否一致，若一致，则判定校验通过，并生成所述第一校验结果。

[0106] 作为一种可能的实施方式，第二终端设备可通过以下方式判断保存的校验信息与

第一校验信息是否一致：

[0107] 利用自身的私钥对所述第一校验信息进行解密得到待校验哈希值和待校验时间戳。

[0108] 判断所述待校验哈希值和待校验时间戳与所述保存的校验信息中的哈希值和时间戳是否一致。

[0109] 当所述待校验哈希值与所述保存的校验信息中的哈希值一致，且所述待校验时间戳与所述保存的校验信息中的时间戳一致时，判定所述保存的校验信息与所述第一校验信息一致；反之，判定所述保存的校验信息与所述第一校验信息不一致。

[0110] 而在保存的校验信息与所述第一校验信息不一致时，该信息校验方法还包括以下步骤：

[0111] 若所述待校验哈希值与所述保存的校验信息中的哈希值不一致，且所述待校验时间戳与所述保存的校验信息中的时间戳一致，则进行数据篡改预警；

[0112] 或者，若所述待校验哈希值与所述保存的校验信息中的哈希值不一致，且所述待校验时间戳相对于所述保存的校验信息中的时间戳较新，则生成用于再次进行信息校验的校验规则，该校验规则包括用于进行加密的加密信息以及该加密信息对应的加密位置；

[0113] 反馈所述校验规则给发送所述第一校验信息的第一终端设备，以使所述第一终端设备根据所述校验规则生成二次校验信息；

[0114] 接收所述第一终端发送的二次校验信息，对所述二次校验信息进行信息校验，得到二次校验结果，并将所述二次校验结果发送至所述第一终端设备，以使所述第一终端设备在所述二次校验结果为校验未通过时进行信息预警。

[0115] 具体地，第二终端设备可通过以下方式对二次校验信息进行信息校验，以得到二次校验结果：

[0116] 从所述二次校验信息中提取加密信息，比对提取到的加密信息与所述校验规则中的加密信息是否一致；

[0117] 若一致，则判定校验通过，并生成二次校验结果，以及将保存的校验信息中的哈希值更改为所述第一校验信息中的哈希值。

[0118] 需要说明的是，本实施例中第二终端设备所能实现的各个步骤，与上述实施例二至实施例四中所阐述的第二终端设备实现的各个步骤均一致。本实施例中各个步骤的详细过程可参见上述实施例二至实施例四的对应内容，具体的在本实施例中不作过多阐述。

[0119] 实施例六

[0120] 如图5所示，为本申请实施例提供的一种终端设备20(如第一终端设备、第二终端设备等)的方框结构示意图，该终端设备20可以执行，但不限于，前述实施例二至实施例五中提供的信息校验方法。

[0121] 其中，终端设备20可以包括，但不限于，图5所示的处理器22、存储器23及通信模块24。处理器22、存储器23以及通信模块24各元件相互之间直接或间接地电性连接，以实现数据的传输或交互。例如，这些元件相互之间可通过一条或多条通讯总线或信号线实现电性连接。

[0122] 其中，存储器23用于存储程序或者数据。存储器23可以是，但不限于，随机存取存储器(Random Access Memory，RAM)，只读存储器(Read Only Memory，ROM)，可编程只读存

储器(Programmable Read-Only Memory,PROM),可擦除只读存储器(Erasable Programmable Read-Only Memory,EPROM),电可擦除只读存储器(Electric Erasable Programmable Read-Only Memory,EEPROM)等。

[0123] 处理器22用于读/写存储器23中存储的数据或程序,并执行相应地功能。

[0124] 通信模块24用于通过网络建立终端设备20与分布式系统10中的其它终端设备20之间的通信连接,并用于通过网络收发数据,如第一校验信息的发送、校验规则的接收等。

[0125] 应当理解的是,图5所示的结构仅为终端设备20的结构示意图,终端设备20还可包括比图5中所示更多或者更少的组件,或者具有与图5所示不同的配置。图5中所示的各组件可以采用硬件、软件或其组合实现。

[0126] 实施例七

[0127] 为了执行上述实施例二至实施例四及各个可能的实现方式中的相应步骤,下面给出一种信息校验装置的实现方式,可选地,该信息校验装置可以采用上述图5所示的终端设备20(例如第一终端设备)的器件结构。在一种实现方式中,信息校验装置可以理解为上述终端设备20中的处理器22,也可以理解为独立于上述终端设备20或处理器22之外的在终端设备20控制下实现上述信息校验方法的软件功能模块。

[0128] 需要说明的是,本实施例所提供的信息校验装置,其基本原理及产生的技术效果和上述实施例相同,为简要描述,本实施例部分未提及之处,可参考上述的实施例中相应内容。该信息校验装置可包括如图6所示的第一数据获取模块211、第一信息校验模块212。

[0129] 第一数据获取模块211,用于获取待校验数据以及该待校验数据对应的时间戳;本实施例中,关于第一数据获取模块211的描述具体可参考上述步骤S11的详细描述,也即,步骤S11可以由第一数据获取模块211执行,因而在此不作更多说明。

[0130] 第一信息校验模块212,用于根据待校验数据以及时间戳生成第一校验信息,将第一校验信息广播给至少一个第二终端设备,使得接收到第一校验信息的第二终端设备进行信息校验以获得第一校验结果,并在第一校验结果为未通过时进行信息预警。本实施例中,关于第一信息校验模块212的描述具体可参考上述步骤S12的详细描述,也即,步骤S12可以由第一信息校验模块212执行,因而在此不作更多说明。

[0131] 可选地,上述模块可以软件或固件(Firmware)的形式存储于图5所示的存储器23中或固化于该终端设备20的操作系统(Operating System,OS)中,并可由图5中的处理器22执行。同时,执行上述模块所需的数据、程序的代码等可以存储在存储器23中。

[0132] 实施例八

[0133] 为了执行上述实施例五及各个可能的实现方式中的相应步骤,下面给出一种信息校验装置的实现方式,可选地,该信息校验装置可以采用上述图5所示的终端设备20(例如第二终端设备)的器件结构。在一种实现方式中,信息校验装置可以理解为上述终端设备20中的处理器22,也可以理解为独立于上述终端设备20或处理器22之外的在终端设备20控制下实现上述信息校验方法的软件功能模块。

[0134] 需要说明的是,本实施例所提供的信息校验装置,其基本原理及产生的技术效果和上述实施例相同,为简要描述,本实施例部分未提及之处,可参考上述的实施例中相应内容。该信息校验装置可包括如图7所示的第二数据获取模块213、第二信息校验模块214。

[0135] 第二数据获取模块213,用于获取第一终端设备广播的第一校验信息,其中,所述

第一校验信息为所述第一终端设备根据获取的待校验数据及该待校验数据对应的时间戳所生成。本实施例中，关于第二数据获取模块213的描述具体可参考上述步骤S21的详细描述，也即，步骤S21可以由第二数据获取模块213执行，因而在此不作更多说明。

[0136] 第二信息校验模块214，用于对所述第一校验信息进行信息校验，得到第一校验结果，并将所述第一校验结果发送至所述第一终端设备，以在所述第一校验结果为未通过时进行信息预警。本实施例中，关于第二信息校验模块214的描述具体可参考上述步骤S22的详细描述，也即，步骤S22可以由第二信息校验模块214执行，因而在此不作更多说明。

[0137] 实施例九

[0138] 基于前述实施例二至实施例五中给出的信息校验方法，本实施例还提供一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器22执行时实现上述实施例二至实施例五中的信息校验方法。

[0139] 综上，本申请实施例提供的信息校验方法、装置、终端设备20和计算机可读存储介质中，在分布式系统10中的第二终端设备的协助下实现对第一终端设备上获取的待校验信息的信息校验，能够有效避免第一终端设备上的数据被非法篡改的问题发生，提高了分布式系统10中各终端设备20的安全性。

[0140] 在本申请的一个实施例中，本申请在基于第一校验信息来实现信息校验以防止终端设备20被非法篡改的同时，还能够允许对终端设备20进行的正常的配置数据的修改。其中，为了区分是否是正常的修改流程，本申请中增加了对设备当前运行状况的二次校验，并在二次校验通过后判定该终端设备20获取的待校验数据为正常的修改数据，此时其他终端设备20可根据接收到的第一校验信息同步修改自身保存的校验信息，以便于下次校验时以新的校验信息进行信息校验。

[0141] 以上所述仅为本申请的优选实施例而已，并不用于限制本申请，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

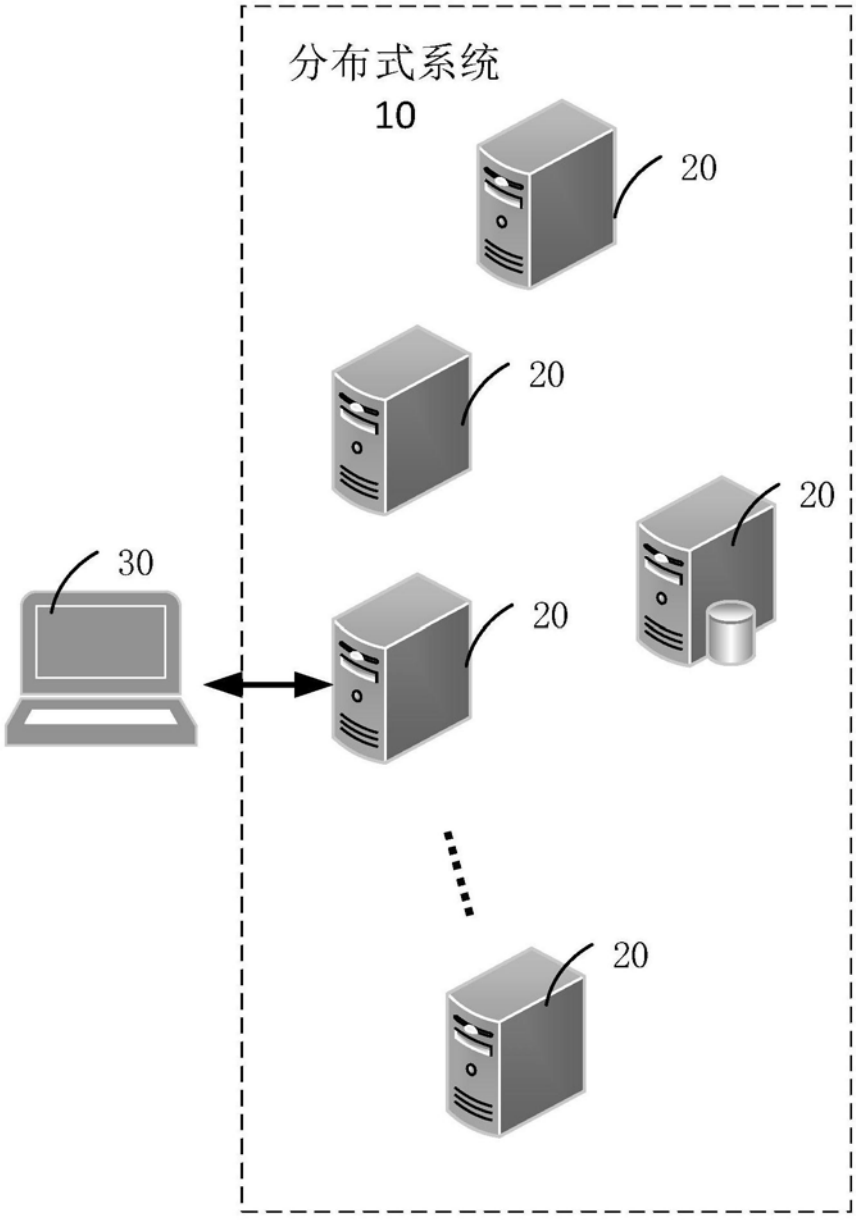


图1

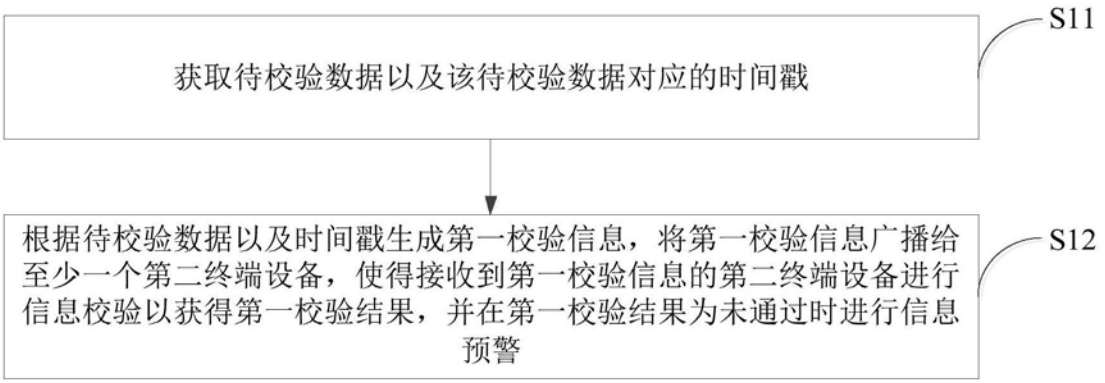

S11
获取待校验数据以及该待校验数据对应的时间戳
S12
根据待校验数据以及时间戳生成第一校验信息，将第一校验信息广播给至少一个第二终端设备，使得接收到第一校验信息的第二终端设备进行信息校验以获得第一校验结果，并在第一校验结果为未通过时进行信息预警

图2

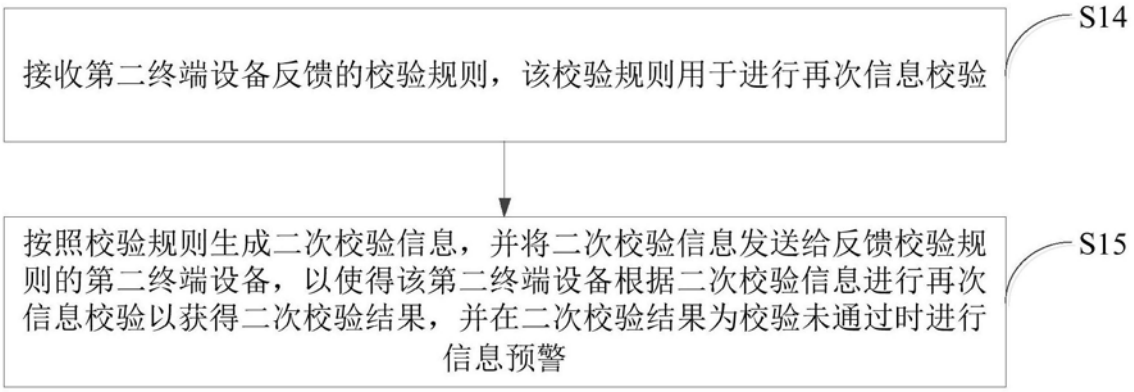

S14
接收第二终端设备反馈的校验规则，该校验规则用于进行再次信息校验
S15
按照校验规则生成二次校验信息，并将二次校验信息发送给反馈校验规则的第二终端设备，以使得该第二终端设备根据二次校验信息进行再次信息校验以获得二次校验结果，并在二次校验结果为校验未通过时进行信息预警

图3

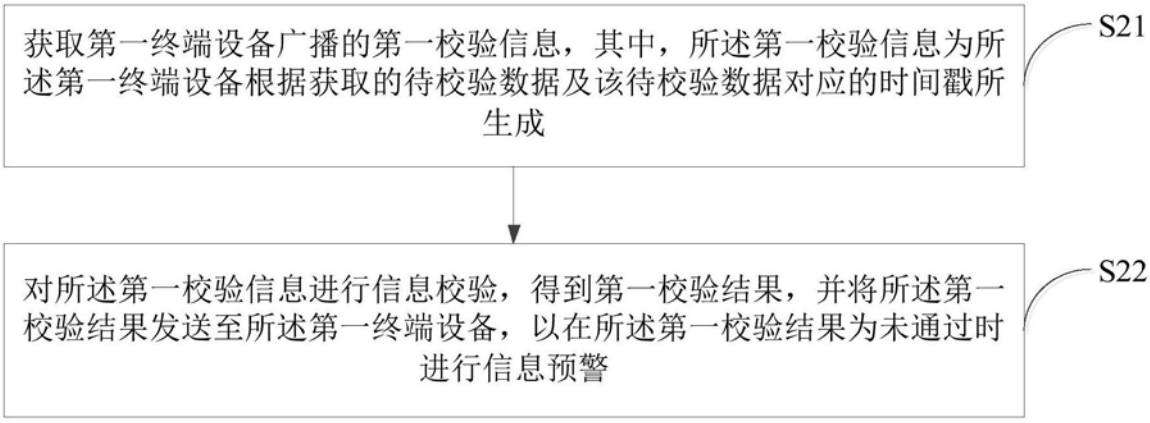

S21
获取第一终端设备广播的第一校验信息，其中，所述第一校验信息为所述第一终端设备根据获取的待校验数据及该待校验数据对应的时间戳所生成
S22
对所述第一校验信息进行信息校验，得到第一校验结果，并将所述第一校验结果发送至所述第一终端设备，以在所述第一校验结果为未通过时进行信息预警

图4

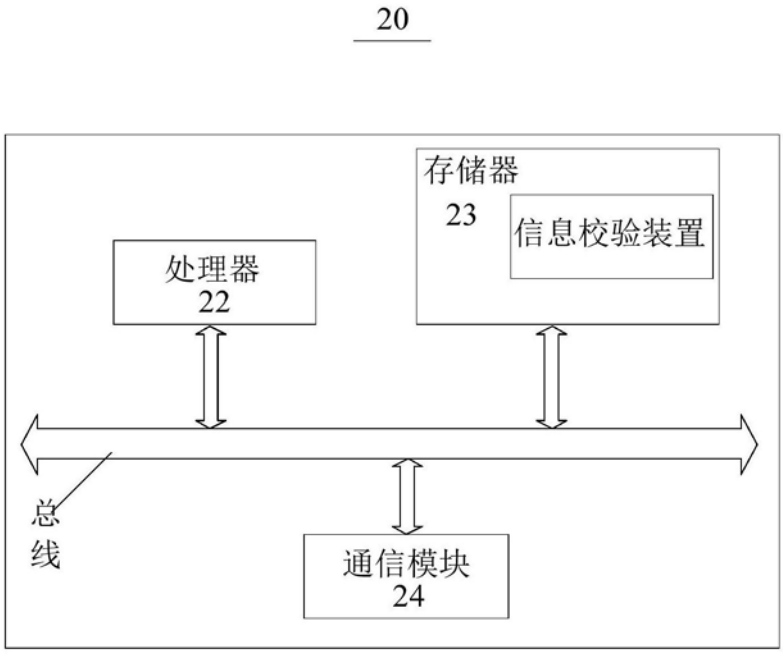

20
存储器
23
信息校验装置
处理器
22
总
线
通信模块
24

图5


信息校验装置
第一数据获取模块
211
第一信息校验模块
212

图6


信息校验装置
第二数据获取模块
213
第二信息校验模块
214

图7