(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 112001730 A
(43)申请公布日 2020.11.27

(21)申请号 202010861053.8

(22)申请日 2020.08.25

(71)申请人 徐鹏飞
地址 650217 云南省昆明市经济技术开发区云大西路105号

(72)发明人 徐鹏飞

(51)Int.Cl.
G06Q 20/38(2012.01)
G06F 21/31(2013.01)
G06F 21/56(2013.01)
G06F 21/64(2013.01)
G06Q 20/06(2012.01)

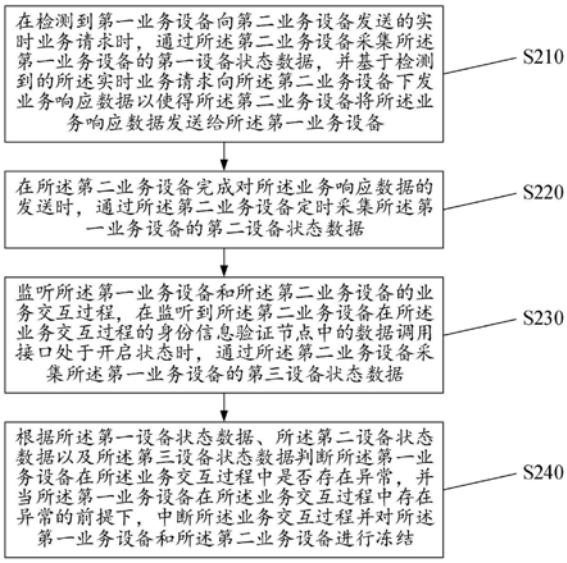
权利要求书3页 说明书12页 附图3页

(54)发明名称

基于区块链和数字货币的数据安全检测方法及云计算中心

(57)摘要

本说明书公开了基于区块链和数字货币的数据安全检测方法及云计算中心，能在检测到实时业务请求时、在第二业务设备完成对业务响应数据的发送时以及在监听到第二业务设备在业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时采集第一业务设备的不同设备状态数据，从而在出判断第一业务设备在业务交互过程中存在异常时冻结第一业务设备和第二业务设备。如此，能够通过部署在云端的云计算中心实现对业务设备进行数字支付交易时的数据安全检测，以准确判断处于交易进程中的业务设备是否携带木马程序，从而在不影响业务设备正常运行的前提下提高木马检测的准确性，避免业务设备的重要数据被木马程序恶意篡改，确保业务设备的安全运行。



CN 112001730 A

1.一种基于区块链和数字货币的数据安全检测方法,其特征在于,应用于与多个业务设备通信的所述云计算中心,所述方法至少包括:

在检测到第一业务设备向第二业务设备发送的实时业务请求时,通过所述第二业务设备采集所述第一业务设备的第一设备状态数据,并基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备;

在所述第二业务设备完成对所述业务响应数据的发送时,通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据;

监听所述第一业务设备和所述第二业务设备的业务交互过程,在监听到所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时,通过所述第二业务设备采集所述第一业务设备的第三设备状态数据;

根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常,并当所述第一业务设备在所述业务交互过程中存在异常的前提下,中断所述业务交互过程并对所述第一业务设备和所述第二业务设备进行冻结。

2.根据权利要求1所述的方法,其特征在于,根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常,包括:

根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据各自对应的时序状态分布判断所述第一业务设备在所述业务交互过程中是否存在异常。

3.根据权利要求2所述的方法,其特征在于,根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据各自对应的时序状态分布判断所述第一业务设备在所述业务交互过程中是否存在异常,包括:

确定出所述第一设备状态数据对应的第一时序状态分布与所述第二设备状态数据对应的第二时序状态分布之间的第一分布差异信息以及所述第二设备状态数据对应的第二时序状态分布与所述第三设备状态数据对应的第三时序状态分布之间的第二分布差异信息;

针对所述第一设备状态数据,以所述第一时序状态分布为参考按照所述第一分布差异信息对所述第一设备状态数据进行特征数据筛选得到第四设备状态数据;针对所述第二设备状态数据,以所述第二时序状态分布为参考按照所述第二分布差异信息对所述第二设备状态数据进行特征数据筛选得到第五设备状态数据;

分别将所述第一设备状态数据和所述第二设备状态数据、所述第一设备状态数据和所述第四设备状态数据、所述第二设备状态数据和所述第三设备状态数据、以及所述第二设备状态数据和所述第五设备状态数据进行时序状态分布映射,得到第一映射结果、第二映射结果、第三映射结果和第四映射结果;

确定出所述第一映射结果和所述第二映射结果之间的第一映射缺损数据以及所述第三映射结果和所述第四映射结果之间的第二映射缺损数据;

判断所述第一映射缺损数据和所述第二映射缺损数据是否均与预设映射基准数据相对应;

若是，根据所述第一映射结果和所述第三映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果；

基于所述安全性检测结果判断所述第一业务设备在所述业务交互过程中是否存在异常，若所述安全性检测结果中存在异常标识，则确定所述第一业务设备在所述业务交互过程中存在异常。

4.根据权利要求3所述的方法，其特征在于，所述方法还包括：

若所述第一映射缺损数据和所述第二映射缺损数据没有均与预设映射基准数据相对应，分别确定出所述第一映射缺损数据和所述第二映射缺损数据与所述预设映射基准数据之间的第一数据相似度和第二数据相似度；

比较所述第一数据相似度和所述第二数据相似度的大小；

在所述第一数据相似度小于所述第二数据相似度时，根据所述第一映射结果和所述第二映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果；

在所述第一数据相似度大于所述第二数据相似度时，根据所述第三映射结果和所述第四映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果。

5.根据权利要求1-4任一项所述的方法，其特征在于，在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，包括：

对所述实时业务请求进行解析以得到所述实时业务请求对应的请求报文序列；提取所述报文序列中记载有所述第一业务设备添加的业务申请队列的多个目标报文字段；根据所述多个目标报文字段生成所述第一业务设备的线程配置参数列表以及所述第一业务设备的业务权限信息列表，并确定出所述线程配置列表中的每个第一列表单元的列表识别权重值以及所述业务权限信息列表中的每个第二列表单元的列表识别权重值；

从所述线程配置列表对应的多个第一列表单元中确定出与所述线程配置列表对应的列表识别权重值的中位数之间的差值位于设定权重区间内的最大值对应的第一列表单元的列表数据，并将所述业务权限信息列表中的具有与所述业务权限信息列表对应的列表识别权重值均值的差值最小的目标列表识别权重值对应的第二列表单元确定为参考单元；将所述列表数据以数据流的形式映射值所述参考单元中并在所述参考单元中得到所述列表数据对应的基准映射数据；

基于所述基准映射数据与所述列表数据的数据相关度确定用于对所述第一业务设备进行设备状态数据提取的提取路径参数，并按照预先获取的与所述第二业务设备相对应的接口格式参数将所述提取路径参数进行封装并下发至所述第二业务设备，以使得所述第二业务设备根据所述提取路径参数确定出从所述第一业务设备中进行设备状态参数提取的多条路径指向信息并基于每条路径指向信息对应的所述第一业务设备的存储地址信息从所述第一业务设备对应的存储区中采集所述第一设备状态数据。

6.根据权利要求1-5任一项所述的方法，其特征在于，基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备，具体包括：

根据所述实时业务请求的身份认证密钥确定所述实时业务请求的可信度数据清单；

将所述可信度数据清单中具有动态标识的数据包进行标记；

确定所标记的数据包在所述可信度数据清单中的位相对位置分布；

基于所述相对位置分布生成状态需求信息并将所述状态需求信息添加到预设认证数据中以得到所述业务响应数据；将所述业务响应数据下发给所述第二业务设备以使得所述第二业务设备缓存所述状态需求信息并将所述预设认证数据发送给所述第一业务设备。

7.根据权利要求1所述的方法，其特征在于，在所述第二业务设备完成对所述业务响应数据的发送时，通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据，包括：

根据所述第二业务设备的设备配置数据建立与所述第二业务设备的数据采集线程之间的同步关系；其中，所述同步关系用于表征建立与所述第二业务设备对应的镜像数据采集线程；

在所述第二业务设备按照设定时间步长和所述状态需求信息周期性地采集所述第一业务设备的第二设备状态数据的过程中，并行地采用所述镜像数据采集线程采集与所述第二设备状态数据对应的镜像状态数据，并在所述镜像状态数据与所述第二设备状态数据在时间周期上一致时通过所述第二业务设备获取所述第二设备状态数据。

8.根据权利要求1所述的方法，其特征在于，监听所述第一业务设备和所述第二业务设备的业务交互过程，包括：

调取所述第一业务设备的第一设备运行日志以及所述第二业务设备的第二设备运行日志，并基于获取到的所述第一业务设备和所述第二业务设备之间的数据传输延迟对所述第一设备运行日志以及所述第二设备运行日志进行同步校正；

在完成对所述第一设备运行日志以及所述第二设备运行日志的同步校正之后，按照所述第一设备运行日志的第一文本分隔信息提取所述第一设备运行日志的多个第一日志记录以及按照所述第二设备运行日志的第二文本分隔信息提取所述第二设备运行日志的多个第二日志记录；

按照时间先后顺序将每个第一日志记录与每个第二日志记录进行遍历比较，若其中一个第一日志记录与其中一个第二日志记录之间存在相同的交互数据时，提取该第二日志记录中的日志脚本文件，解析所述日志脚本文件得到所述数据调用接口的状态标识；在所述状态标识为第一标识时确定所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态；在所述状态标识为第二标识时确定所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于关闭状态。

9.一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，该程序被处理器执行时实现权利要求1-8任一项所述方法的步骤。

10.一种云计算中心，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现权利要求1-8任一项所述方法的步骤。

基于区块链和数字货币的数据安全检测方法及云计算中心

技术领域

[0001] 本申请涉及区块链金融，尤其涉及基于区块链和数字货币的数据安全检测方法及云计算中心。

背景技术

[0002] 数字货币是基于节点网络和数字加密算法的虚拟货币，现如今已逐渐得到应用。随着数字经济的发展，数字货币在社会经济活动中的比重越来越大。结合区块链的支付体系能够确保每一笔线上的数字支付交易不会被篡改，同时区块链支付还能够提高数字支付交易的实时性，减少交易延迟，实现快速到账。

[0003] 然而随着业务设备的数量和类型的与日俱增，不同业务设备在实现数字支付交易时，虽然不能对数字支付交易进行篡改，但是可能会在交易过程中向对手方设备植入木马程序，使得对手方设备的重要数据被恶意篡改，这样可能影响对手方设备的安全运行。

发明内容

[0004] 本说明书提供了一种基于区块链和数字货币的数据安全检测方法及云计算中心，以解决或者部分解决现有技术存在的上述技术问题。

[0005] 本说明书公开了一种基于区块链和数字货币的数据安全检测方法，应用于与多个业务设备通信的云计算中心，所述方法至少包括：

[0006] 在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，并基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备；

[0007] 在所述第二业务设备完成对所述业务响应数据的发送时，通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据；

[0008] 监听所述第一业务设备和所述第二业务设备的业务交互过程，在监听到所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时，通过所述第二业务设备采集所述第一业务设备的第三设备状态数据；

[0009] 根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常，并当所述第一业务设备在所述业务交互过程中存在异常的前提下，中断所述业务交互过程并对所述第一业务设备和所述第二业务设备进行冻结。

[0010] 可选地方式中，根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常，包括：

[0011] 根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据各自对应的时序状态分布判断所述第一业务设备在所述业务交互过程中是否存在异常。

[0012] 可选地方式中，根据所述第一设备状态数据、所述第二设备状态数据以及所述第

三设备状态数据各自对应的时序状态分布判断所述第一业务设备在所述业务交互过程中是否存在异常，包括：

[0013] 确定出所述第一设备状态数据对应的第一时序状态分布与所述第二设备状态数据对应的第二时序状态分布之间的第一分布差异信息以及所述第二设备状态数据对应的第二时序状态分布与所述第三设备状态数据对应的第三时序状态分布之间的第二分布差异信息；

[0014] 针对所述第一设备状态数据，以所述第一时序状态分布为参考按照所述第一分布差异信息对所述第一设备状态数据进行特征数据筛选得到第四设备状态数据；针对所述第二设备状态数据，以所述第二时序状态分布为参考按照所述第二分布差异信息对所述第二设备状态数据进行特征数据筛选得到第五设备状态数据；

[0015] 分别将所述第一设备状态数据和所述第二设备状态数据、所述第一设备状态数据和所述第四设备状态数据、所述第二设备状态数据和所述第三设备状态数据、以及所述第二设备状态数据和所述第五设备状态数据进行时序状态分布映射，得到第一映射结果、第二映射结果、第三映射结果和第四映射结果；

[0016] 确定出所述第一映射结果和所述第二映射结果之间的第一映射缺损数据以及所述第三映射结果和所述第四映射结果之间的第二映射缺损数据；

[0017] 判断所述第一映射缺损数据和所述第二映射缺损数据是否均与预设映射基准数据相对应；

[0018] 若是，根据所述第一映射结果和所述第三映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果；

[0019] 基于所述安全性检测结果判断所述第一业务设备在所述业务交互过程中是否存在异常，若所述安全性检测结果中存在异常标识，则确定所述第一业务设备在所述业务交互过程中存在异常。

[0020] 可选地方式中，所述方法还包括：

[0021] 若所述第一映射缺损数据和所述第二映射缺损数据没有均与预设映射基准数据相对应，分别确定出所述第一映射缺损数据和所述第二映射缺损数据与所述预设映射基准数据之间的第一数据相似度和第二数据相似度；

[0022] 比较所述第一数据相似度和所述第二数据相似度的大小；

[0023] 在所述第一数据相似度小于所述第二数据相似度时，根据所述第一映射结果和所述第二映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果；

[0024] 在所述第一数据相似度大于所述第二数据相似度时，根据所述第三映射结果和所述第四映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果。

[0025] 可选地方式中，在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，包括：

[0026] 对所述实时业务请求进行解析以得到所述实时业务请求对应的请求报文序列;提取所述报文序列中记载有所述第一业务设备添加的业务申请队列的多个目标报文字段;根据所述多个目标报文字段生成所述第一业务设备的线程配置参数列表以及所述第一业务设备的业务权限信息列表,并确定出所述线程配置列表中的每个第一列表单元的列表识别权重值以及所述业务权限信息列表中的每个第二列表单元的列表识别权重值;

[0027] 从所述线程配置列表对应的多个第一列表单元中确定出与所述线程配置列表对应的列表识别权重值的中位数之间的差值位于设定权重区间内的最大值对应的第一列表单元的列表数据,并将所述业务权限信息列表中的具有与所述业务权限信息列表对应的列表识别权重值均值的差值最小的目标列表识别权重值对应的第二列表单元确定为参考单元;将所述列表数据以数据流的形式映射值所述参考单元中并在所述参考单元中得到所述列表数据对应的基准映射数据;

[0028] 基于所述基准映射数据与所述列表数据的数据相关度确定用于对所述第一业务设备进行设备状态数据提取的提取路径参数,并按照预先获取的与所述第二业务设备相对应的接口格式参数将所述提取路径参数进行封装并下发至所述第二业务设备,以使得所述第二业务设备根据所述提取路径参数确定出从所述第一业务设备中进行设备状态参数提取的多条路径指向信息并基于每条路径指向信息对应的所述第一业务设备的存储地址信息从所述第一业务设备对应的存储区中采集所述第一设备状态数据。

[0029] 可选地方式中,基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备,具体包括:

[0030] 根据所述实时业务请求的身份认证密钥确定所述实时业务请求的可信度数据清单;

[0031] 将所述可信度数据清单中具有动态标识的数据包进行标记;

[0032] 确定所标记的数据包在所述可信度数据清单中的位相对位置分布;

[0033] 基于所述相对位置分布生成状态需求信息并将所述状态需求信息添加到预设认证数据中以得到所述业务响应数据;将所述业务响应数据下发给所述第二业务设备以使得所述第二业务设备缓存所述状态需求信息并将所述预设认证数据发送给所述第一业务设备。

[0034] 可选地方式中,在所述第二业务设备完成对所述业务响应数据的发送时,通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据,包括:

[0035] 根据所述第二业务设备的设备配置数据建立与所述第二业务设备的数据采集线程之间的同步关系;其中,所述同步关系用于表征建立与所述第二业务设备对应的镜像数据采集线程;

[0036] 在所述第二业务设备按照设定时间步长和所述状态需求信息周期性地采集所述第一业务设备的第二设备状态数据的过程中,并行地采用所述镜像数据采集线程采集与所述第二设备状态数据对应的镜像状态数据,并在所述镜像状态数据与所述第二设备状态数据在时间周期上一致时通过所述第二业务设备获取所述第二设备状态数据。

[0037] 可选地方式中,监听所述第一业务设备和所述第二业务设备的业务交互过程,包括:

[0038] 调取所述第一业务设备的第一设备运行日志以及所述第二业务设备的第二设备运行日志，并基于获取到的所述第一业务设备和所述第二业务设备之间的数据传输延迟对所述第一设备运行日志以及所述第二设备运行日志进行同步校正；

[0039] 在完成对所述第一设备运行日志以及所述第二设备运行日志的同步校正之后，按照所述第一设备运行日志的第一文本分隔信息提取所述第一设备运行日志的多个第一日志记录以及按照所述第二设备运行日志的第二文本分隔信息提取所述第二设备运行日志的多个第二日志记录；

[0040] 按照时间先后顺序将每个第一日志记录与每个第二日志记录进行遍历比较，若其中一个第一日志记录与其中一个第二日志记录之间存在相同的交互数据时，提取该第二日志记录中的日志脚本文件，解析所述日志脚本文件得到所述数据调用接口的状态标识；在所述状态标识为第一标识时确定所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态；在所述状态标识为第二标识时确定所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于关闭状态。

[0041] 本说明书公开了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述方法的步骤。

[0042] 本说明书公开了一种云计算中心，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述方法的步骤。

[0043] 通过本说明书的一个或者多个技术方案，本说明书具有以下有益效果或者优点：

[0044] 能在检测到第一业务设备向第二业务设备发送的实时业务请求时采集第一业务设备的第一设备状态数据、在第二业务设备完成对业务响应数据的发送时采集第一业务设备的第二设备状态数据以及在监听到第二业务设备在业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时采集第一业务设备的第三设备状态数据，从而根据第一设备状态数据、第二设备状态数据以及第三设备状态数据在出判断第一业务设备在业务交互过程中存在异常时冻结第一业务设备和第二业务设备。

[0045] 如此，能够通过部署在云端的云计算中心实现对业务设备进行数字支付交易时的数据安全检测，以准确判断处于交易进程中的业务设备是否携带木马程序，从而在不影响业务设备正常运行的前提下提高木马检测的准确性，避免业务设备的重要数据被木马程序恶意篡改，确保业务设备的安全运行。

[0046] 上述说明仅是本说明书技术方案的概述，为了能够更清楚了解本说明书的技术手段，而可依照说明书的内容予以实施，并且为了让本说明书的上述和其它目的、特征和优点能够更明显易懂，以下特举本说明书的具体实施方式。

附图说明

[0047] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本说明书的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0048] 图1示出了根据本说明书一个实施例的基于区块链和数字货币的数据安全检测系统的结构示意图；

[0049] 图2示出了根据本说明书一个实施例的基于区块链和数字货币的数据安全检测方

法的流程图；

[0050] 图3示出了根据本说明书一个实施例的基于区块链和数字货币的数据安全检测装置的功能模块框图；

[0051] 图4示出了根据本说明书一个实施例的一种云计算中心的示意图。

具体实施方式

[0052] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0053] 发明人在研究时发现，现有技术对这些木马程序进行检测时，大多基于共识机制的验证算法实现检测验证，这样难以确保验证的准确性，并且在业务设备侧部署验证线程会增加业务设备的运行负荷，降低业务设备的运行效率。

[0054] 为改善上述技术问题，本发明实施例提供了基于区块链和数字货币的数据安全检测方法及云计算中心，能够通过部署在云端的云计算中心实现对业务设备进行数字支付交易时的数据安全检测，以准确判断处于交易进程中的业务设备是否携带木马程序，从而在不影响业务设备正常运行的前提下提高木马检测的准确性，避免业务设备的重要数据被木马程序恶意篡改，确保业务设备的安全运行。

[0055] 为详细阐述本实施例，请首先参阅图1，为基于区块链和数字货币的数据安全检测系统100的通信架构示意图，所述数据安全检测系统100可以包括云计算中心200和多个业务设备400。其中，云计算中心200和多个业务设备400互相之间通信连接。在本实施例中，业务设备400可以是区块链节点设备。

[0056] 进一步地，请结合参阅图2，提供了基于区块链和数字货币的数据安全检测方法的流程图，所述方法可以应用于图1中的云计算中心200，具体可以包括以下步骤S210-步骤S240所描述的内容。

[0057] 步骤S210，在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，并基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备。

[0058] 例如，实时业务请求可以是数字交易请求或在线支付请求，在此不作限定，设备状态数据可以是第一业务设备在运行时的资源配置分布和设备安全状态，其中，资源配置分布可以是内存资源的配置情况，设备安全状态可以是第一业务设备的数据调用函数的执行轨迹。响应数据用于表征第二业务设备对实时业务请求进行批准。

[0059] 步骤S220，在所述第二业务设备完成对所述业务响应数据的发送时，通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据。

[0060] 例如，第二设备状态数据和第一设备状态数据处于不同时段。

[0061] 步骤S230，监听所述第一业务设备和所述第二业务设备的业务交互过程，在监听到所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时，通过所述第二业务设备采集所述第一业务设备的第三设备状态数据。

[0062] 例如，业务交互过程为第一业务设备和第二业务设备进行数字支付交易的过程，身份信息验证节点用于对第二业务设备和第一业务设备的身份信息进行校验，数据调用接口连接第二业务设备的身份数据库，在数据调用接口处于开启状态时，身份数据库处于可访问状态。

[0063] 步骤S240，根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常，并当所述第一业务设备在所述业务交互过程中存在异常的前提下，中断所述业务交互过程并对所述第一业务设备和所述第二业务设备进行冻结。

[0064] 例如，第一业务设备存在异常可以理解为第一业务设备携带用于篡改第二业务设备的身份数据库的木马程序。冻结第一业务设备和第二业务设备可以理解为拦截第一业务设备和第二业务设备的所有业务行为。

[0065] 在应用上述步骤S210-步骤S240所描述的内容时，能在检测到第一业务设备向第二业务设备发送的实时业务请求时采集第一业务设备的第一设备状态数据、在第二业务设备完成对业务响应数据的发送时采集第一业务设备的第二设备状态数据以及在监听到第二业务设备在业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时采集第一业务设备的第三设备状态数据，从而根据第一设备状态数据、第二设备状态数据以及第三设备状态数据在出判断第一业务设备在业务交互过程中存在异常时冻结第一业务设备和第二业务设备。

[0066] 如此，能够通过部署在云端的云计算中心实现对业务设备进行数字支付交易时的数据安全检测，以准确判断处于交易进程中的业务设备是否携带木马程序，从而在不影响业务设备正常运行的前提下提高木马检测的准确性，避免业务设备的重要数据被木马程序恶意篡改，确保业务设备的安全运行。

[0067] 在具体实施过程中发明人发现，为了准确判断第一业务设备是否存在异常，需要考虑第一业务设备在不同时段的设备状态数据的差异情况，从而避免误判或漏判。为实现这一目的，步骤S240所描述的根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常，具体可以包括以下步骤所描述的内容：根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据各自对应的时序状态分布判断所述第一业务设备在所述业务交互过程中是否存在异常。这样以来，能够考虑第一业务设备在不同时段的设备状态数据的差异情况，从而准确判断第一业务设备是否存在异常。

[0068] 详细地，根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据各自对应的时序状态分布判断所述第一业务设备在所述业务交互过程中是否存在异常，进一步可以包括以下步骤S241-步骤S248所描述的内容。

[0069] 步骤S241，确定出所述第一设备状态数据对应的第一时序状态分布与所述第二设备状态数据对应的第二时序状态分布之间的第一分布差异信息以及所述第二设备状态数据对应的第二时序状态分布与所述第三设备状态数据对应的第三时序状态分布之间的第二分布差异信息。

[0070] 步骤S242，针对所述第一设备状态数据，以所述第一时序状态分布为参考按照所述第一分布差异信息对所述第一设备状态数据进行特征数据筛选得到第四设备状态数据；

针对所述第二设备状态数据，以所述第二时序状态分布为参考按照所述第二分布差异信息对所述第二设备状态数据进行特征数据筛选得到第五设备状态数据。

[0071] 步骤S243，分别将所述第一设备状态数据和所述第二设备状态数据、所述第一设备状态数据和所述第四设备状态数据、所述第二设备状态数据和所述第三设备状态数据、以及所述第二设备状态数据和所述第五设备状态数据进行时序状态分布映射，得到第一映射结果、第二映射结果、第三映射结果和第四映射结果。

[0072] 步骤S244，确定出所述第一映射结果和所述第二映射结果之间的第一映射缺损数据以及所述第三映射结果和所述第四映射结果之间的第二映射缺损数据。

[0073] 步骤S245，判断所述第一映射缺损数据和所述第二映射缺损数据是否均与预设映射基准数据相对应。

[0074] 步骤S246，若是，根据所述第一映射结果和所述第三映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果。

[0075] 步骤S247，若否，分别确定出所述第一映射缺损数据和所述第二映射缺损数据与所述预设映射基准数据之间的第一数据相似度和第二数据相似度；比较所述第一数据相似度和所述第二数据相似度的大小；在所述第一数据相似度小于所述第二数据相似度时，根据所述第一映射结果和所述第二映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果；在所述第一数据相似度大于所述第二数据相似度时，根据所述第三映射结果和所述第四映射结果确定出所述第一业务设备的状态评估信息并按照所述状态评估信息对所述第一设备状态数据、所述第二设备状态数据和所述第三设备状态数据进行状态安全性检测得到安全性检测结果。

[0076] 步骤S248，基于所述安全性检测结果判断所述第一业务设备在所述业务交互过程中是否存在异常，若所述安全性检测结果中存在异常标识，则确定所述第一业务设备在所述业务交互过程中存在异常。

[0077] 如此，依据上述步骤S241-步骤S248，能够准确判断第一业务设备在所述业务交互过程中是否存在异常。

[0078] 在具体实施过程中，为了确保采集到的第一设备状态数据的完整性，步骤S210所描述的在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，示例性地可以包括以下步骤S2111-步骤S2113所描述的内容。

[0079] 步骤S2111，对所述实时业务请求进行解析以得到所述实时业务请求对应的请求报文序列；提取所述报文序列中记载有所述第一业务设备添加的业务申请队列的多个目标报文字段；根据所述多个目标报文字段生成所述第一业务设备的线程配置参数列表以及所述第一业务设备的业务权限信息列表，并确定出所述线程配置列表中的每个第一列表单元的列表识别权重值以及所述业务权限信息列表中的每个第二列表单元的列表识别权重值。

[0080] 步骤S2112，从所述线程配置列表对应的多个第一列表单元中确定出与所述线程配置列表对应的列表识别权重值的中位数之间的差值位于设定权重区间内的最大值对应的第一列表单元的列表数据，并将所述业务权限信息列表中的具有与所述业务权限信息列

表对应的列表识别权重值均值的差值最小的目标列表识别权重值对应的第二列表单元确定为参考单元;将所述列表数据以数据流的形式映射值所述参考单元中并在所述参考单元中得到所述列表数据对应的基准映射数据。

[0081] 步骤S2113,基于所述基准映射数据与所述列表数据的数据相关度确定用于对所述第一业务设备进行设备状态数据提取的提取路径参数,并按照预先获取的与所述第二业务设备相对应的接口格式参数将所述提取路径参数进行封装并下发至所述第二业务设备,以使得所述第二业务设备根据所述提取路径参数确定出从所述第一业务设备中进行设备状态参数提取的多条路径指向信息并基于每条路径指向信息对应的所述第一业务设备的存储地址信息从所述第一业务设备对应的存储区中采集所述第一设备状态数据。

[0082] 可以理解,通过以上步骤S2111-步骤S2113,能够对实时业务请求进行解析确定出用于对第一业务设备进行设备状态数据提取的提取路径参数,并将所述提取路径参数发送给第二业务设备以使得第二业务设备从第一业务设备对应的存储区中采集第一设备状态数据,,这样能够确保采集到的第一设备状态数据的完整性。

[0083] 在一个可能的实施方式中,为了对第一业务设备进行全方位的设备状态数据采集,以实现准确的异常检测,在步骤S210中,基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备,具体可以通过以下步骤S2121-步骤S2124所描述的内容。

[0084] 步骤S2121,根据所述实时业务请求的身份认证密钥确定所述实时业务请求的可信度数据清单。

[0085] 步骤S2122,将所述可信度数据清单中具有动态标识的数据包进行标记。

[0086] 步骤S2123,确定所标记的数据包在所述可信度数据清单中的位相对位置分布。

[0087] 步骤S2124,基于所述相对位置分布生成状态需求信息并将所述状态需求信息添加到预设认证数据中以得到所述业务响应数据;将所述业务响应数据下发给所述第二业务设备以使得所述第二业务设备缓存所述状态需求信息并将所述预设认证数据发送给所述第一业务设备。

[0088] 这样以来,第二业务设备能够根据缓存的状态需求信息在后续采集中对第一业务设备进行全方位的设备状态数据采集,从而确保后续的异常检测的准确性。

[0089] 在上述步骤S2121-步骤S2124的基础上,为了对第一业务设备进行全方位的设备状态数据采集,在步骤S220中,在所述第二业务设备完成对所述业务响应数据的发送时,通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据,具体可以包括以下步骤S221和步骤S222所描述的内容。

[0090] 步骤S221,根据所述第二业务设备的设备配置数据建立与所述第二业务设备的数据采集线程之间的同步关系;其中,所述同步关系用于表征建立与所述第二业务设备对应的镜像数据采集线程。

[0091] 步骤S222,在所述第二业务设备按照设定时间步长和所述状态需求信息周期性地采集所述第一业务设备的第二设备状态数据的过程中,并行地采用所述镜像数据采集线程采集与所述第二设备状态数据对应的镜像状态数据,并在所述镜像状态数据与所述第二设备状态数据在时间周期上一致时通过所述第二业务设备获取所述第二设备状态数据。

[0092] 这样以来,基于上述步骤S221和步骤S222,能够通过将镜像状态数据与第二设备

状态数据进行比较，从而实现对第一业务设备进行全方位的设备状态数据采集。

[0093] 在一个可以实现的实施例中，为了对第二业务设备对应的数据调用接口进行准确监听，步骤S230所描述的监听所述第一业务设备和所述第二业务设备的业务交互过程，具体可以包括以下步骤S2311-步骤S2313所描述的内容。

[0094] 步骤S2311，调取所述第一业务设备的第一设备运行日志以及所述第二业务设备的第二设备运行日志，并基于获取到的所述第一业务设备和所述第二业务设备之间的数据传输延迟对所述第一设备运行日志以及所述第二设备运行日志进行同步校正。

[0095] 步骤S2312，在完成对所述第一设备运行日志以及所述第二设备运行日志的同步校正之后，按照所述第一设备运行日志的第一文本分隔信息提取所述第一设备运行日志的多个第一日志记录以及按照所述第二设备运行日志的第二文本分隔信息提取所述第二设备运行日志的多个第二日志记录。

[0096] 步骤S2313，按照时间先后顺序将每个第一日志记录与每个第二日志记录进行遍历比较，若其中一个第一日志记录与其中一个第二日志记录之间存在相同的交互数据时，提取该第二日志记录中的日志脚本文件，解析所述日志脚本文件得到所述数据调用接口的状态标识；在所述状态标识为第一标识时确定所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态；在所述状态标识为第二标识时确定所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于关闭状态。

[0097] 可以理解，基于上述步骤S2311-步骤S2313所描述的内容，能够实现对第二业务设备对应的数据调用接口的准确监听。

[0098] 在一个可替换的实施方式中，步骤S230所描述的通过所述第二业务设备采集所述第一业务设备的第三设备状态数据，具体可以包括以下步骤S2321和步骤S2322所描述的内容。

[0099] 步骤S2321，向所述第二业务设备发送用于调整所述第二业务设备的数据采集线程的线程逻辑参数的修改指令。

[0100] 步骤S2322，使所述第二业务设备根据所述修改指令对所述数据采集线程的线程逻辑参数进行修改并基于修改之后的数据采集线程采集所述第一业务设备中与所述数据调用接口存在关联的第三设备状态数据。

[0101] 如此以来，可以通过上述步骤S2321和步骤S2322针对性地采集第一业务设备中与数据调用接口存在关联的第三设备状态数据。

[0102] 在一个可以实现的实施方式中，步骤S240所描述的中断所述业务交互过程并对所述第一业务设备和所述第二业务设备进行冻结，进一步可以包括以下步骤(1)-步骤(4)所描述的内容。

[0103] (1)根据所述业务交互过程对应的协议层信息确定所述第二业务设备的权限列表。

[0104] (2)根据所述第二权限列表生成与所述与所述第二业务设备对应得第二控制指令。

[0105] (3)将所述第二控制指令下发给所述第二业务设备，以指示所述第二业务设备关闭与所述第一业务设备的交互。

[0106] (4)拦截所述第一业务设备和所述第二业务设备的所有业务报文。

[0107] 这样以来，通过上述步骤(1)-(4)所描述的内容，能够确保第一业务设备、第二业务设备以及其他业务设备的数据信息安全性。

[0108] 基于与前述实施例中同样的发明构思，请结合参阅图3，提供了一种基于区块链和数字货币的数据安全检测装置300，应用于与多个业务设备通信的云计算中心，所述装置至少包括以下功能模块：

[0109] 数据下发模块310，用于在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，并基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备；

[0110] 数据采集模块320，用于在所述第二业务设备完成对所述业务响应数据的发送时，通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据；

[0111] 业务监听模块330，用于监听所述第一业务设备和所述第二业务设备的业务交互过程，在监听到所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时，通过所述第二业务设备采集所述第一业务设备的第三设备状态数据；

[0112] 异常判断模块340，用于根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常，并当所述第一业务设备在所述业务交互过程中存在异常的前提下，中断所述业务交互过程并对所述第一业务设备和所述第二业务设备进行冻结。

[0113] 关于上述功能模块的描述请参阅对图2所示的方法的描述，在此不作更多说明。

[0114] 基于与前述实施例中同样的发明构思，提供一种基于区块链和数字货币的数据安全检测系统，包括云计算中心以及与所述云计算中心通信的多个业务设备；

[0115] 所述云计算中心具体用于：

[0116] 在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，并基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备；

[0117] 在所述第二业务设备完成对所述业务响应数据的发送时，通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据；

[0118] 监听所述第一业务设备和所述第二业务设备的业务交互过程，在监听到所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时，通过所述第二业务设备采集所述第一业务设备的第三设备状态数据；

[0119] 根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常，并当所述第一业务设备在所述业务交互过程中存在异常的前提下，中断所述业务交互过程并对所述第一业务设备和所述第二业务设备进行冻结。

[0120] 基于与前述实施例中同样的发明构思，本说明书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，该程序被处理器执行时实现前文任一所述方法的步骤。

[0121] 基于与前述实施例中同样的发明构思，本说明书的实施例还提供一种云计算中心

200，如图4所示，包括存储器204、处理器202及存储在存储器204上并可在处理器202上运行的计算机程序，所述处理器202执行所述程序时实现前文任一所述方法的步骤。

[0122] 通过本说明书的一个或者多个实施例，本说明书具有以下有益效果或者优点：

[0123] 能在检测到第一业务设备向第二业务设备发送的实时业务请求时采集第一业务设备的第一设备状态数据、在第二业务设备完成对业务响应数据的发送时采集第一业务设备的第二设备状态数据以及在监听到第二业务设备在业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时采集第一业务设备的第三设备状态数据，从而根据第一设备状态数据、第二设备状态数据以及第三设备状态数据在出判断第一业务设备在业务交互过程中存在异常时冻结第一业务设备和第二业务设备。

[0124] 如此，能够通过部署在云端的云计算中心实现对业务设备进行数字支付交易时的数据安全检测，以准确判断处于交易进程中的业务设备是否携带木马程序，从而在不影响业务设备正常运行的前提下提高木马检测的准确性，避免业务设备的重要数据被木马程序恶意篡改，确保业务设备的安全运行。

[0125] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本说明书也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本说明书的内容，并且上面对特定语言所做的描述是为了披露本说明书的最佳实施方式。

[0126] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本说明书的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0127] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本说明书的示例性实施例的描述中，本说明书的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本说明书要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本说明书的单独实施例。

[0128] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0129] 此外，本领域的技术人员能够理解，尽管在此的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本说明书的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意

之一都可以以任意的组合方式来使用。

[0130] 本说明书的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本说明书实施例的网关、代理服务器、系统中的一些或者全部部件的一些或者全部功能。本说明书还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本说明书的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0131] 应该注意的是上述实施例对本说明书进行说明而不是对本说明书进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本说明书可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

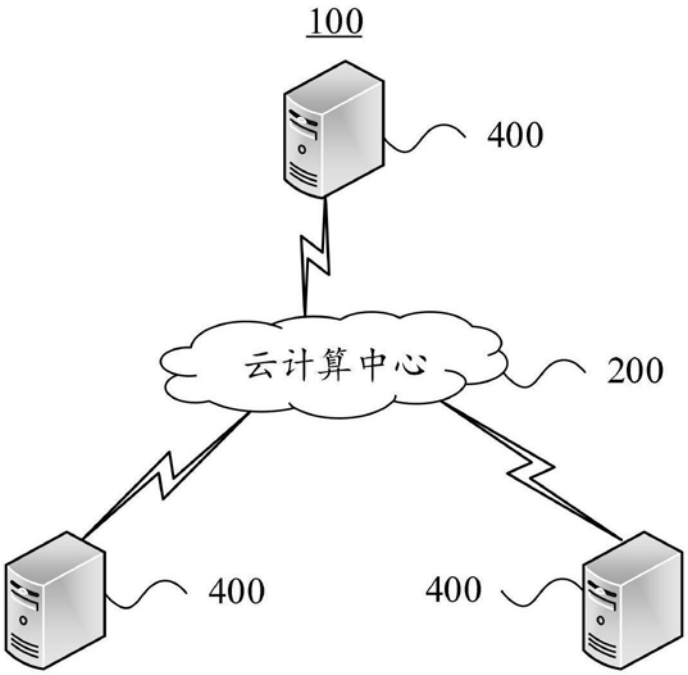


图1

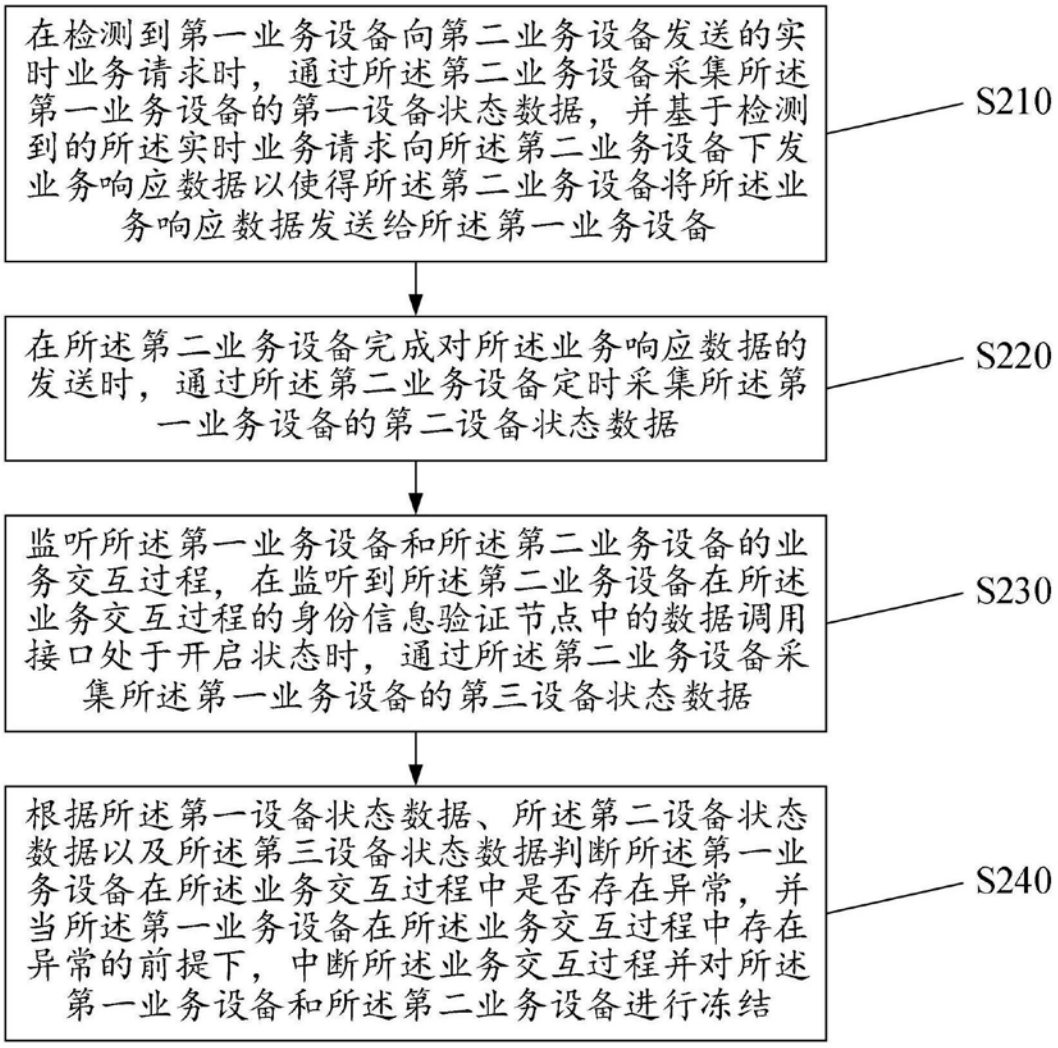

在检测到第一业务设备向第二业务设备发送的实时业务请求时，通过所述第二业务设备采集所述第一业务设备的第一设备状态数据，并基于检测到的所述实时业务请求向所述第二业务设备下发业务响应数据以使得所述第二业务设备将所述业务响应数据发送给所述第一业务设备
S210
在所述第二业务设备完成对所述业务响应数据的发送时，通过所述第二业务设备定时采集所述第一业务设备的第二设备状态数据
S220
监听所述第一业务设备和所述第二业务设备的业务交互过程，在监听到所述第二业务设备在所述业务交互过程的身份信息验证节点中的数据调用接口处于开启状态时，通过所述第二业务设备采集所述第一业务设备的第三设备状态数据
S230
根据所述第一设备状态数据、所述第二设备状态数据以及所述第三设备状态数据判断所述第一业务设备在所述业务交互过程中是否存在异常，并当所述第一业务设备在所述业务交互过程中存在异常的前提下，中断所述业务交互过程并对所述第一业务设备和所述第二业务设备进行冻结
S240

图2

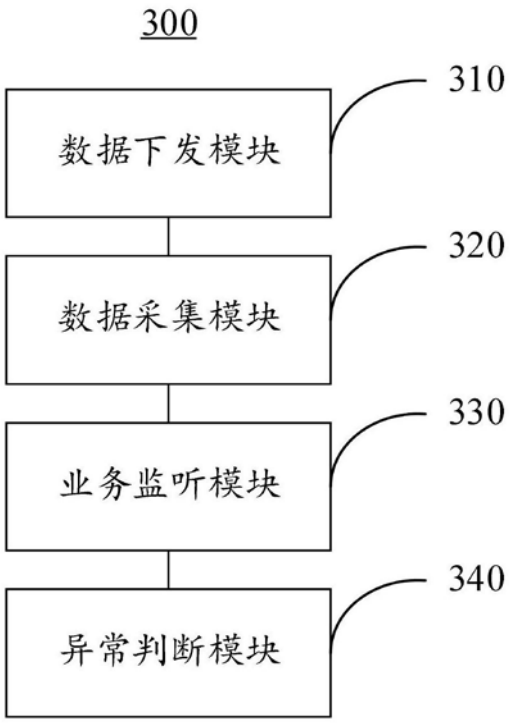

300
310
数据下发模块
320
数据采集模块
330
业务监听模块
340
异常判断模块

图3

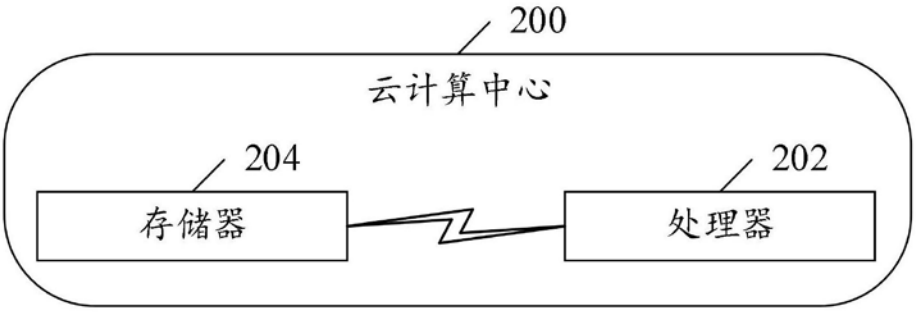

200
云计算中心
204
存储器
202
处理器

图4