(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 114254286 A
(43)申请公布日 2022.03.29

(21)申请号 202111349232.4

(22)申请日 2021.11.15

(71)申请人 阿里巴巴(中国)有限公司
地址 310000 浙江省杭州市滨江区长河街道网商路699号4号楼5楼508室

(72)发明人 章佳 金天龙 黄旭灵 许可 樊静 张铭

(74)专利代理机构 北京众达德权知识产权代理有限公司 11570
代理人 南海燕

(51)Int.Cl.
G06F 21/32(2013.01)
G06Q 10/06(2012.01)
G06T 19/00(2011.01)
G06V 20/10(2022.01)

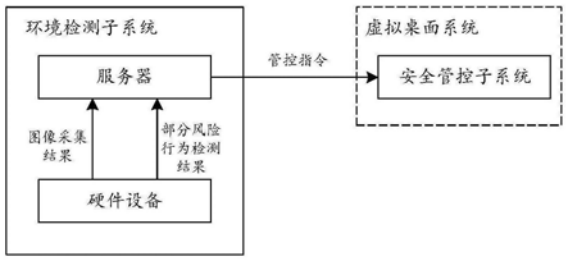
权利要求书2页 说明书14页 附图4页

(54)发明名称

数据安全防控方法、系统及AR眼镜

(57)摘要

本申请实施例公开了数据安全防控方法、系统及AR眼镜，所述系统包括：环境检测子系统，用于对用户办公所在的物理工作环境进行图像采集及风险行为检测，如果检测到的风险行为触发预置的管控方案，则向安全管控子系统发出安全管控指令；安全管控子系统，用于为所述用户的终端设备提供用于办公的软件工作环境，并在接收到所述安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。通过本申请实施例，能够在远程办公场景下，更全面地进行数据安全风险控制。



CN 114254286 A

1.一种数据安全防控系统,其特征在于,包括:

环境检测子系统,用于对用户办公所在的物理工作环境进行图像采集及风险行为检测,如果检测到的风险行为触发预置的管控方案,则向安全管控子系统发出安全管控指令;

安全管控子系统,用于为所述用户的终端设备提供用于办公的软件工作环境,并在接收到所述安全管控指令后,通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

2.根据权利要求1所述的系统,其特征在于,

所述环境检测子系统包括硬件设备以及检测服务器;

所述硬件设备用于对所述物理工作环境进行图像采集;

所述硬件设备和/或所述检测服务器用于通过对采集到的图像进行分析,判断所述物理工作环境中是否存在风险行为,以及对应的风险类型。

3.根据权利要求2所述的系统,其特征在于,

所述硬件设备包括具有图像采集模块的智能音箱设备;

或者,

具有多个图像采集模块的穿戴式设备,所述多个图像采集模块用于以所述用户为中心,对所述物理工作环境进行多角度的图像采集。

4.根据权利要求3所述的系统,其特征在于,

所述穿戴式设备还用于,在触发所述管控方案时,向所述用户提供单模态或多模态的提醒消息。

5.根据权利要求1所述的系统,其特征在于,

不同的管控方案对应不同的管控动作,所述管控动作包括:通过弹出窗口的方式提供提醒消息,对所述终端设备当前页面中展示的内容进行模糊化处理,和/或对所述终端设备进行锁屏处理。

6.一种数据安全防控方法,其特征在于,包括:

获取用户办公所在的物理工作环境中的图像信息;

根据所述图像信息对所述物理工作环境进行风险行为检测;

如果检测到的风险行为触发预置的管控方案,则向安全管控系统发出安全管控指令,所述安全管控系统用于为所述用户的终端设备提供用于办公的软件工作环境,并在接收到所述安全管控指令后,通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

7.一种数据安全防控方法,其特征在于,包括:

对用户办公所在的物理工作环境中的图像信息进行采集;

根据采集到的图像信息获取风险行为检测结果;

如果所述风险行为触发预置的管控方案,则向所述用户提供提醒消息。

8.一种数据安全防控方法,其特征在于,包括:

为办公用户的终端设备提供用于办公的软件工作环境;

在接收到安全管控指令后,通过在所述软件工作环境中执行对应的管控动作的方式行安全管控;

其中,所述安全管控指令是对所述用户办公所在的物理工作环境进行图像采集及风险

行为检测后生成的。

9.一种智能音箱,其特征在于,包括:

图像采集模块,用于对用户办公所在的物理工作环境中的图像信息进行采集;所述图像信息用于对所述物理工作环境中的风险行为进行检测;

提醒模块,用于在所检测到的风险行为触发管控方案时,向所述用户提供语音提醒消息。

10.一种增强现实AR眼镜,其特征在于,包括:

多个图像采集模块,用于以用户为中心,对所述用户办公所在的物理工作环境中的图像信息进行多角度采集;所述图像信息用于对所述物理工作环境中的风险行为进行检测;

提醒模块,用于在所检测到的风险行为触发管控方案时,向所述用户提供提醒消息。

11.根据权利要求10所述的AR眼镜,其特征在于,

所述提醒模块包括视觉提醒模块,用于通过所述AR眼镜的镜片提供视觉提醒消息;

和/或,

所述AR眼镜还带有振动器,所述提醒模块包括振动提醒模块,用于通过所述振动器提供振动提醒消息;

和/或,

所述AR眼镜还带有骨传导装置,所述提醒模块包括骨传导提醒模块,用于通过所述骨传导装置提供语音提醒消息。

12.根据权利要求11所述的AR眼镜,其特征在于,

所述视觉提醒模块具体用于,通过输出虚拟图像对所述AR眼镜的镜片进行模糊处理,或者,通过所述AR眼镜输出提醒信息,或者,通过控制所述AR眼镜的镜片对用户观看的目标进行遮挡。

13.一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6至8任一项所述的方法的步骤。

14.一种电子设备,其特征在于,包括:

一个或多个处理器;以及

与所述一个或多个处理器关联的存储器,所述存储器用于存储程序指令,所述程序指令在被所述一个或多个处理器读取执行时,执行权利要求6至8任一项所述的方法的步骤。

数据安全防控方法、系统及AR眼镜

技术领域

[0001] 本申请涉及远程办公场景中的数据安全技术领域，特别是涉及数据安全防控方法、系统及AR眼镜。

背景技术

[0002] 随着互联网在各个领域的广泛运用及各类办公设备在家庭中的普及，居家办公成为越来越多的人可以尝试的一种工作方式，而它的内涵与形式也在发生变化。例如，在商品对象信息服务系统中，一般会为用户提供客户服务系统，帮助用户解答一些关于订单、优惠策略、纠纷等相关的问题。并且，为了能够给用户提供更为优质的服务，这种客户服务系统可能需要全天候24小时都有客服人员在线。在这种情况下，客服人员可能会具有居家远程办公的需求，等等。

[0003] 通过远程办公模式能够实现随时随地开始办公，但是，在远程办公过程中，首当其冲要解决的是数据安全风控问题，尤其是涉及到用户信息等高风险级别的场景，安全风控问题更为突出。

[0004] 因此，在远程办公场景下，如何进行数据安全风险控制，成为需要本领域技术人员解决的技术问题。

发明内容

[0005] 本申请提供了数据安全防控方法、系统及AR眼镜，能够在远程办公场景下，更全面地进行数据安全风险控制。

[0006] 本申请提供了如下方案：

[0007] 一种数据安全防控系统，包括：

[0008] 环境检测子系统，用于对用户办公所在的物理工作环境进行图像采集及风险行为检测，如果检测到的风险行为触发预置的管控方案，则向安全管控子系统发出安全管控指令；

[0009] 安全管控子系统，用于为所述用户的终端设备提供用于办公的软件工作环境，并在接收到所述安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

[0010] 其中，所述环境检测子系统还用于接收到所述用户的第一登录请求后，对用户进行身份验证，如果身份验证信息通过，则确定所述用户办公所在的物理工作环境为可检测状态，并将该状态信息提供给所述安全管控子系统；

[0011] 所述安全管控子系统还用于，在接收到用户的第二登录请求时，根据所述环境检测子系统提供的状态信息，进行登录控制。

[0012] 其中，所述安全管控子系统还用于，将所述用户是否处于工作状态的信息提供给所述环境检测子系统；

[0013] 所述环境检测子系统具体用于，根据所述用户是否处于工作状态，确定是否进入

对物理工作环境的检测状态。

[0014] 其中,所述环境检测子系统包括硬件设备以及检测服务器;

[0015] 所述硬件设备用于对所述物理工作环境进行图像采集;

[0016] 所述硬件设备和/或所述检测服务器用于通过对采集到的图像进行分析,判断所述物理工作环境中是否存在风险行为,以及对应的风险类型。

[0017] 其中,所述硬件设备包括具有图像采集模块的智能音箱设备。

[0018] 其中,所述硬件设备包括具有多个图像采集模块的穿戴式设备,所述多个图像采集模块用于以所述用户为中心,对所述物理工作环境进行多角度的图像采集。

[0019] 其中,所述穿戴式设备还用于,在触发所述管控方案时,向所述用户提供单模态或多模态的提醒消息。

[0020] 其中,所述穿戴式设备包括增强现实AR眼镜;

[0021] 所述AR眼镜具体用于,在触发所述管控方案时,提供以下一种或多种模态的提醒消息:通过所述AR眼镜的镜片提供视觉提醒消息,通过关联的振动器提供振动提醒消息,或者,通过骨传导装置提供语音提醒消息。

[0022] 其中,所述环境检测子系统具体用于,根据检测到的风险行为的类型以及发生频率确定风险等级,并根据不同的风险等级触发不同的管控方案。

[0023] 其中,所述环境检测子系统还用于,在检测到较高风险等级的风险行为时,向任务系统发出管控指令,以便所述任务系统停止向所述用户进行任务分配。

[0024] 其中,不同的管控方案对应不同的管控动作,所述管控动作包括:通过弹出窗口的方式提供提醒消息,对所述终端设备当前页面中展示的内容进行模糊化处理,和/或对所述终端设备进行锁屏处理。

[0025] 其中,较低等级的管控方案还关联有疲劳度信息,所述疲劳度信息用于,如果同一管控方案被触发的频率达到目标阈值,则延长管控动作的执行间隔。

[0026] 一种数据安全防控方法,包括:

[0027] 获取用户办公所在的物理工作环境中的图像信息;

[0028] 根据所述图像信息对所述物理工作环境进行风险行为检测;

[0029] 如果检测到的风险行为触发预置的管控方案,则向安全管控系统发出安全管控指令,所述安全管控系统用于为所述用户的终端设备提供用于办公的软件工作环境,并在接收到所述安全管控指令后,通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

[0030] 其中,所述图像信息是由位于所述物理工作环境中的硬件设备进行采集并按照预置的时间间隔上传的;

[0031] 所述方法还包括:

[0032] 接收硬件设备提交的风险行为检测结果,所述硬件设备提交的风险行为检测结果是根据实时采集的图像信息进行判断获得的。

[0033] 一种数据安全防控方法,包括:

[0034] 对用户办公所在的物理工作环境中的图像信息进行采集;

[0035] 根据采集到的图像信息获取风险行为检测结果;

[0036] 如果所述风险行为触发预置的管控方案,则向所述用户提供提醒消息。

[0037] 其中，所述对所述用户办公所在的物理工作环境中的图像信息进行采集，包括：

[0038] 通过智能音箱设备的图像采集模块，对所述用户办公所在的物理工作环境中的图像信息进行采集；

[0039] 所述向所述用户提供提醒消息，包括：

[0040] 通过所述智能音箱设备，向所述用户提供语音提醒消息。

[0041] 其中，所述对用户办公所在的物理工作环境中的图像信息进行采集，包括：

[0042] 通过所述用户关联的具有多个图像采集模块的穿戴式设备，以所述用户为中心，对所述用户办公所在的物理工作环境中的图像信息进行多角度采集；

[0043] 所述向所述用户提供提醒消息，包括：

[0044] 通过所述穿戴式设备，向所述用户提供单模态或多模态的提醒消息。

[0045] 一种数据安全防控方法，包括：

[0046] 为办公用户的终端设备提供用于办公的软件工作环境；

[0047] 在接收到安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式行安全管控；

[0048] 其中，所述安全管控指令是对所述用户办公所在的物理工作环境进行图像采集及风险行为检测后生成的。

[0049] 一种智能音箱，包括：

[0050] 图像采集模块，用于对用户办公所在的物理工作环境中的图像信息进行采集；所述图像信息用于对所述物理工作环境中的风险行为进行检测；

[0051] 提醒模块，用于在所检测到的风险行为触发管控方案时，向所述用户提供语音提醒消息。

[0052] 其中，还包括：

[0053] 检测模块，用于通过对采集到的图像信息进行分析，对所述物理工作环境中的风险行为进行检测。

[0054] 其中，还包括：

[0055] 检测结果上传模块，用于将检测到的风险行为信息上传到服务器，以便由所述服务器对风险行为进行汇总，并判断是否触发所述管控方案。

[0056] 其中，还包括：

[0057] 图像采集信息上传模块，用于按照预置的时间间隔，将所采集到的图像信息上传到服务器，以便所述服务器通过对接收到的图像信息进行分析，对所述物理工作环境中的风险行为进行检测。

[0058] 一种增强现实AR眼镜，包括：

[0059] 多个图像采集模块，用于以用户为中心，对所述用户办公所在的物理工作环境中的图像信息进行多角度采集；所述图像信息用于对所述物理工作环境中的风险行为进行检测；

[0060] 提醒模块，用于在所检测到的风险行为触发管控方案时，向所述用户提供提醒消息。

[0061] 其中，所述提醒模块包括视觉提醒模块，用于通过所述AR眼镜的镜片提供视觉提醒消息。

[0062] 其中，所述视觉提醒模块具体用于，通过输出虚拟图像对所述AR眼镜的镜片进行模糊处理，或者，通过所述AR眼镜输出提醒信息，或者，通过控制所述AR眼镜的镜片对用户观看的目标进行遮挡。

[0063] 其中，所述AR眼镜还带有振动器；

[0064] 所述提醒模块包括振动提醒模块，用于通过所述振动器提供振动提醒消息。

[0065] 其中，所述AR眼镜还带有骨传导装置；

[0066] 所述提醒模块包括骨传导提醒模块，用于通过所述骨传导装置提供语音提醒消息。

[0067] 一种数据安全防控装置，包括：

[0068] 图像信息获取单元，用于获取用户办公所在的物理工作环境中的图像信息；

[0069] 风险行为检测单元，用于根据所述图像信息对所述物理工作环境进行风险行为检测；

[0070] 指令发送单元，用于如果检测到的风险行为触发预置的管控方案，则向安全管控系统发出安全管控指令，所述安全管控系统用于为所述用户的终端设备提供用于办公的软件工作环境，并在接收到所述安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

[0071] 一种数据安全防控装置，包括：

[0072] 图像采集单元，用于对用户办公所在的物理工作环境中的图像信息进行采集；

[0073] 风险行为检测单元，用于根据采集到的图像信息获取风险行为检测结果；

[0074] 提醒单元，用于如果所述风险行为触发预置的管控方案，则向所述用户提供提醒消息。

[0075] 一种数据安全防控装置，包括：

[0076] 软件工作环境提供单元，用于为办公用户的终端设备提供用于办公的软件工作环境；

[0077] 管控动作执行单元，用于在接收到安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式行安全管控；

[0078] 其中，所述安全管控指令是对所述用户办公所在的物理工作环境进行图像采集及风险行为检测后生成的。

[0079] 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述任一项所述的方法的步骤。

[0080] 一种电子设备，包括：

[0081] 一个或多个处理器；以及

[0082] 与所述一个或多个处理器关联的存储器，所述存储器用于存储程序指令，所述程序指令在被所述一个或多个处理器读取执行时，执行前述任一项所述的方法的步骤。

[0083] 根据本申请提供的具体实施例，本申请公开了以下技术效果：

[0084] 通过本申请实施例，可以提供环境检测子系统，并基于虚拟桌面等系统提供安全管控子系统。这样，在通过虚拟桌面系统为用户的终端设备提供用于办公的软件工作环境的同时，还可以通过环境检测子系统对用户所在的物理工作环境中可能存在的风险行为进行检测，如果检测到的风险行为触发管控方案，则可以由安全管控子系统在所述软件工作

环境中执行对应的管控动作，以此实现对所述用户的安全管控。这样，可以在软件工作环境以及物理工作环境两个方面进行数据安全保障，从而更好的解决远程办公等办公场景中的安全风控问题。

[0085] 当然，实施本申请的任一产品并不一定需要同时达到以上所述的所有优点。

附图说明

[0086] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，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，还可以根据这些附图获得其他的附图。

[0087] 图1是本申请实施例提供的系统的示意图；

[0088] 图2是本申请实施例提供的AR眼镜的示意图；

[0089] 图3是本申请实施例提供的第一方法的流程图；

[0090] 图4是本申请实施例提供的第二方法的流程图；

[0091] 图5是本申请实施例提供的第三方法的流程图；

[0092] 图6是本申请实施例提供的智能音箱的示意图；

[0093] 图7是本申请实施例提供的AR眼镜的示意图；

[0094] 图8是本申请实施例提供的第一装置的示意图；

[0095] 图9是本申请实施例提供的第二装置的示意图；

[0096] 图10是本申请实施例提供的第三装置的示意图；

[0097] 图11是本申请实施例提供的电子设备的示意图。

具体实施方式

[0098] 下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本申请保护的范围。

[0099] 首先需要说明的是，现有技术中，关于远程办公中的数据安全风控问题，主要通过虚拟桌面类的工具实现数据“不落本地”。也即，用户在远程办公时，需要首先打开虚拟桌面类的工具，然后在该工具内通过浏览器等进行数据访问以及处理，但是，具体的数据运算及保存等都可以在云端服务器来完成，不会驻留在用户个人的终端设备本地。通过这种方式，不用担心数据驻留用户个人的终端设备本地而导致的安全漏洞。但是，本申请发明人在实现本申请的过程中发现，远程办公过程中的数据安全风险还可能来自于用户所在的物理环境。例如，非本人办公，使用手机等移动端设备对PC机等工作设备的屏幕中展示出的商业信息或用户数据进行拍照，或者，通过手写的方式记录一些信息，或者，工作过程中周围可能有其他无关人员围观，等等。以上各种因素的存在都会使得数据面临被泄露的风险。

[0100] 因此，在本申请实施例中，还可以在通过上述虚拟桌面类的工具实现数据“不落本地”的同时，可以通过部署相关的硬件设备、服务器，使其与虚拟桌面类工具相结合，实现对用户所在的物理工作环境中可能存在的风险行为进行检测以及管控的功能。例如，通过硬

件设备对员工所在物理工作环境进行图像采集，基于图像采集结果进行风险行为的检测，如果检测到的具体风险行为触发相应的管控方案，则可以通过虚拟桌面类工具，对用户的软件工作环境执行管控动作，例如，通过弹出窗口的方式提供提示信息，或者，可以执行锁屏处理，等等。另外，还可以通过硬件设备提供提醒信息，等等。其中，关于具体的硬件设备，可以包括智能音箱设备，或者，还可以包括穿戴式设备，等等。

[0101] 下面对本申请实施例提供的具体实现方案进行详细介绍。

[0102] 实施例一

[0103] 首先，该实施例一提供了一种数据安全防控系统，参见图1，该系统具体可以包括：

[0104] 环境检测子系统11，用于对用户办公所在的物理工作环境进行图像采集及风险行为检测，如果检测到的风险行为触发预置的管控方案，则向安全管控子系统发出安全管控指令；

[0105] 安全管控子系统12，用于为所述用户的终端设备提供用于办公的软件工作环境，并在接收到所述安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

[0106] 其中，所述物理工作环境具体就可以是用户在进行远程办公时，所在的物理场所的环境。也就是说，在本申请实施例中，在用户通过远程办公的方式工作的过程中，可以通过环境检测子系统对物理工作环境中可能存在的风险行为进行检测，如果发现非本人登录，或者使用手机，或者，周围有人围观等风险行为，则可以通过虚拟桌面类的工具，对用户的软件工作环境进行风险管控。通过这种方式，由于虚拟桌面能够为用户提供安全的软件工作环境，在此基础上，通过对物理工作环境中的风险行为进行管控，因此，可以全方位的保障远程办公环境下的数据安全。当然，在实际应用中，如果在非远程办公的场景中需要对工作环境进行风险管控，也可以采用本申请提供的方案来进行，这里不对具体的应用场景进行限定。

[0107] 具体的，如图1所示，环境检测子系统11可以包括硬件设备111以及检测服务器112，其中，硬件设备111可以部署在上述物理工作环境中，具体可以用于对所述物理工作环境进行图像采集，这种采集到的图像信息就可以用于进行风险行为的检测。具体的，可以通过硬件设备和/或所述检测服务器，对采集到的图像进行分析，并判断所述物理工作环境中是否存在风险行为，以及对应的风险类型(具体实现时，还可以包括具体风险行为的方位信息，等等)。也就是说，硬件设备可以将采集到的图像信息上传到服务器，在服务器端对图像进行分析，以判断是否存在风险行为。或者，也可以在硬件设备本地运行相关的应用程序，通过该应用程序在硬件设备本地进行图像分析，以及风险行为的检测。或者，在另一种方式下，还可以将硬件设备与服务器相结合，例如，可以在硬件设备根据实时采集到的图像信息，对一些比较简单的风险行为进行检测，同时，硬件设备还可以按照一定的时间间隔(例如，每秒等)将采集到的图像信息上传到服务器，通过服务器对一些比较复杂的风险行为进行检测，等等。

[0108] 当然，无论是在硬件设备本地进行风险行为检测，还是在服务器中进行风险行为检测，如果检测到风险行为，都可以确定出对应的风险类型(例如，非本人登录，或者，工作过程中使用手机，或者，周围有人围观，等等)，并且可以将这种检测结果汇总到服务器中，以便在服务器中统一进行风险行为的统计，以判断是否触发具体的管控方案。

[0109] 其中，关于具体的硬件设备111，可以有多种具体的实现形式，例如，一种方式下，具体的硬件设备可以是普通的摄像头类的设备，此时，该硬件设备可以仅具备图像采集及上传的功能，具体的风险行为检测可以在服务器中进行。或者，为了能够在硬件设备中进行一些简单的风险行为检测，因此，还可以使用具有图像采集模块的智能音箱设备来实现。具体的，可以为智能音箱设备配备摄像头等图像采集模块，这样，可以通过智能音箱设备实现对物理工作环境中的图像信息进行采集。另外，由于这种智能音箱设备通常也具备操作系统，可以支持对应用程序的安装等，因此，也可以在这种音箱设备中安装相关的应用程序，通过这种应用程序实现在智能音箱本地的风险行为检测以及检测结果的上传，等等。再者，由于智能音箱设备还具有语音功能，因此，在具体实现时，还可以根据具体检测到的风险行为，或者对管控方案的触发情况为用户提供对应的语音提示信息，例如，提醒用户停止或者注意某风险行为，等等。

[0110] 另一种方式下，具体的硬件设备还可以包括穿戴式设备，这种穿戴式设备还可以配备有多个图像采集模块。通过所述多个图像采集模块，可以以所述用户为中心，对物理工作环境进行多角度的图像采集，例如，可以通过在穿戴式设备的前后左右等多个位置部署摄像头，实现以用户为中心，对物理工作环境的360度的图像采集，等等。通过这种方式，由于可以实现以用户为中心的多角度图像采集，因此，更有利于全面地发现物理工作环境中可能存在的各种风险行为。其中，一种具体的实现方式下，具体的穿戴式设备可以是AR(Augmented Reality，增强现实)眼镜。例如，一种方式下，该AR眼镜上可以配备如图2所示的四个摄像头，以此获得现以用户为中心，对其周围360范围内的检测视野。并且，由于具体的穿戴式设备可以穿戴在用户身上，因此，不需要占用用户的工位空间。另外，由于可以随着用户的移动而移动，因此，能够实现对风险行为的动态检测。再者，在检测到的风险行为触发管控方案时，还可以通过这种穿戴式设备向用户提供单模态或多模态的提醒消息(也就是说，不仅可以通过虚拟桌面类的工具对用户进行安全管控，还可以直接通过硬件设备对用户进行提醒)。

[0111] 其中，具体实现时，由于AR眼镜自身的特性，可以在视觉上进行一些处理，以实现对用户的提醒，另外，还可以在AR眼镜上安装其他的辅助模块，实现多模态的提醒。例如，在触发所述管控方案后，可以通过所述AR眼镜的镜片提供视觉提醒消息。或者，还可以在AR眼镜上安装振动器，这样，可以通过关联的振动器提供振动提醒消息。或者，还可以在AR眼镜上安装骨传导装置，这样，可以通过骨传导装置提供语音提醒消息。

[0112] 其中，具体的视觉提醒消息也可以有多种，例如，可以通过输出虚拟图像对所述AR眼镜的镜片进行模糊处理(也即，在正常状态下，AR眼镜的镜片可以是透明的，而在触发管控方案后，可以对镜片进行模糊处理)，或者，通过所述AR眼镜输出提醒信息(例如，在镜片上展示出具体的提醒文本，提醒其停止相关行为，或者对周围人的行为进行制止，等等)，或者，通过控制所述AR眼镜的镜片对用户观看的目标进行遮挡(例如，通过对镜片中的栅格状态进行处理，对用户视野范围内的部分敏感内容进行遮挡，等等)。

[0113] 总之，可以通过摄像头设备、智能音箱设备、AR眼镜等穿戴式设备作为硬件设备，实现对用户所在物理工作环境的图像采集，然后，可以与服务器相配合，实现对风险行为的检测。之后，还可以由服务器对具体检测出的各种类型的风险行为进行统计，以判断是否触发具体的管控方案，并在触发管控方案的情况下，可以向安全管控子系统发出管控指令，由

安全管控子系统执行具体的管控动作。

[0114] 其中，对具体风险行为的统计过程也可以是实时进行的，例如，某时刻发现用户使用手机，则可以记录下该风险行为的类型，以及对应的发生时间，该类型的风险行为的累计发生次数，等等。通过这种统计信息，可以判断是否触发预置的管控方案。

[0115] 具体实现时，具体的管控方案可以有多种，分别对应不同的风险等级。而关于风险等级，则可以根据具体风险行为的类型、频率等进行确定。例如，如果用户在半小时内使用手机三次以上，则触发某管控方案，等等。具体的管控方案中还可以配置有对应分管控动作信息，也即，根据具体风险等级的不同，可以执行不同的管控动作。例如，对于一些风险等级比较低的情况，具体的管控动作可以是通过弹出窗口的方式向用户提供提醒信息，或者，还可以在弹窗提醒的同时，对所述终端设备当前页面中展示的内容进行暂时性地模糊化处理，在用户通过关闭弹窗等方式确认收到提醒消息后，再逐渐回复对页面中内容的清晰化展示。或者，对于一些风险等级中等的情况，管控动作可以是锁屏，用户需要通过重新输入密码的方式进行解锁。或者，对于一些高风险的情况，管控动作可以是强制锁屏，此时，需要用户联系管理员才能够进行解锁，等等。

[0116] 这里需要说明的是，由于具体的安全管控子系统可以是基于虚拟桌面类的工具来实现的，而虚拟桌面类的工具能够为用户提供软件工作环境，也即，用户在远程办公的过程中，需要在其终端设备中打开虚拟桌面类的工具，然后，其工作过程中所需的软件工作环境是由虚拟桌面类的工具提供的，例如，在虚拟桌面工具内打开浏览器等，进行任务的接收以及处理，等等。因此，具体的虚拟桌面系统能够对用户的软件工作环境进行控制。这样，在虚拟桌面系统的基础上实现的安全管控子系统，就可以在其提供的软件工作环境中执行任意的管控动作。例如，在本申请实施例中，可以包括弹窗提醒，自动锁屏、强制锁屏，等等。

[0117] 需要说明的是，在具体实现时，由于不同的风险等级对管控的必要性需求也可能是不同的，例如，较低等级的风险，可能不需要太过频繁的提醒用户，否则可能会对用户的实际工作造成太严重的干扰。为此，对于较低等级的风险对应的管控方案，还可以关联有疲劳度信息，这样，如果同一管控方案被触发的频率达到目标阈值，则可以延长管控动作的执行间隔。当然，不同的管控方案可以对应设置不同的疲劳度信息，对于高风险等级对应的管控方案，则可以不必设置疲劳度。

[0118] 此外，由于具体在远程办公过程中，可能是由具体的任务系统向用户分配工作任务，然后，用户通过具体虚拟桌面系统提供的软件工作环境接收具体的任务信息并执行对应的任务，例如，包括客服系统中的员工为消费者用户提供的接线服务，等等。在这种情况下，还可以将环境检测子系统与任务系统进行打通，这样，在检测到较高风险等级的风险行为时，还可以向任务系统发出管控指令，以便所述任务系统停止向所述用户进行任务分配。也即，如果发现用户所在的物理工作环境中存在比较高危的风险因素，则可以直接通知任务系统停止为其分配任务，以避免造成客户信息的泄露。当然，如果是检测到某员工的物理环境中存在高风险因素时，该员工正处于为某客户提供服务的过程中，则任务系统在停止为该员工分配新的任务的同时，还可以将当前正在提供的服务转移给其他员工，以降低对客户体验的影响。

[0119] 这里需要说明的是，在具体实现时，具体的图像分析以及风险行为检测都可以通过算法的方式来实现。当然，还可以提供人工检测的入口，具体的，还可以支持在服务器侧

输入某用户的用户名等信息，对该用户当前所在物理工作环境中的图像信息进行查看的功能。如果发现存在风险行为，也可以手动触发具体的管控方案，这样，可以通过不定期的人工抽检的方式，实现更强的管控。

[0120] 另外需要说明的是，在通过本申请实施例提供的系统进行安全风险管控时，一种优选的方式下，可以要求用户在工作开始前，先进入对物理工作环境可检测的状态，直到用户退出工作后，可以自动结束检测。

[0121] 具体的，为了达到上述目的，具体的工作流程可以是：在用户开始工作之前，可以首先通过环境检测子系统进行登录，系统接收到所述用户的第一登录请求后，可以对用户进行身份验证，如果身份验证信息通过，则确定所述用户所在的物理工作环境为可检测状态。

[0122] 也就是说，用户可以分别在环境检测子系统中以及虚拟桌面系统中登录。例如，具体实现时，首先可以打开具体的硬件设备，并通过该硬件设备发出登录请求。具体的，如果是使用智能音箱设备作为硬件设备，则该智能音箱设备还可以配备有显示屏，用户可以通过该智能音箱设备打开相关的应用程序，在其中输入用户名、密码等信息，另外，还可以通过智能音箱设备的摄像头等进行人脸采集(或者采集其他的生物特征信息)，这样，可以通过用户名、密码进行用户身份识别，并通过人脸信息等对用户进行本人验证。如果使用的硬件设备是AR眼镜等穿戴式设备，由于这种设备可能不具备显示屏等，因此，可以预先通过一些方式将这种穿戴式设备与用户名、密码等登录信息进行绑定，例如，可以借助于手机等智能终端设备完成上述绑定过程。这样，具体在打开穿戴式设备之后，可以通过该设备中的摄像头等采集用户的人脸图像，或者，也可以采集用户的虹膜特征信息，通过镜框等位置设置的指纹采集装置采集用户的指纹特征，等等。这样，可以通过穿戴式设备绑定的登录信息进行用户身份识别，并通过上述生物特征，对用户进行本人验证，等等。

[0123] 在用户通过硬件设备完成登录并完成本人身份验证之后，可以主动将该状态信息提供给所述安全管控子系统，或者，在安全管控子系统的请求下，提供给安全管控子系统。这样，安全管控子系统还可以在接收到用户的第二登录请求时，根据所述环境检测子系统提供的状态信息，进行登录控制。例如，用户在硬件设备中完成登录以及身份验证之后，可以在其PC机等终端设备中打开虚拟桌面系统，并在该虚拟桌面系统中输入用户名、密码等登录信息(与在硬件设备中的登录信息可以相同，或者具有对应关系)。虚拟桌面系统中的安全管控子系统在收到该第二登录请求后，可以首先从环境检测子系统的服务器请求获取对应用户的状态信息，判断当前用户是否已经打开硬件设备，进入到可检测的状态，如果是，则可以完成后续的登录过程，并且可以进入到具体的工作状态；否则，可以提示用户先打开硬件设备并登录，等等。

[0124] 这里需要说明的是，用户在硬件设备中完成登录以及身份验证之后，环境检测子系统可以直接对物理环境中的图像进行采集，或者，在优选的实施方式下，还可以根据用户的实际工作情况确定是否进行采集以及检测。也即，安全管控子系统还可以将所述用户是否处于工作状态的信息提供给所述环境检测子系统，这样，环境检测子系统可以根据所述用户是否处于工作状态，确定是否进入对物理工作环境的检测状态。例如，具体的，用户在硬件设备中完成登录以及身份验证之后，进入到可检测的状态，但是，由于用户尚未在虚拟桌面系统中完成登录，也即，尚未进入到工作状态，因此，暂时不必进行图像采集以及风险

行为检测。待用户在虚拟桌面系统中完成登录，并进入工作状态之后，具体的安全管控子系统可以通知给环境检测子系统，此时，再开始进行图像采集以及风险行为的检测。另外，在进入工作状态后，用户也可能会由于午间休息等，进入休息状态，此时，安全管控子系统也可以将该用户进入休息状态的信息通知给环境检测子系统，环境检测子系统可以暂停图像的采集以及风险行为检测，以此降低资源浪费。

[0125] 总之，通过本申请实施例，可以提供环境检测子系统，并基于虚拟桌面等系统提供安全管控子系统。这样，在通过虚拟桌面系统为用户的终端设备提供用于办公的软件工作环境的同时，还可以通过环境检测子系统对用户所在的物理工作环境中可能存在的风险行为进行检测，如果检测到的风险行为触发管控方案，则可以由安全管控子系统在所述软件工作环境中执行对应的管控动作，以此实现具体的安全管控。这样，可以在软件工作环境以及物理工作环境两个方面进行数据安全保障，从而更好的解决远程办公等工作场景中的安全风控问题。

[0126] 实施例二

[0127] 该实施例二是与实施例一相对应的，从环境检测子系统的服务器角度，提供了一种数据安全防控方法，参见图3，该方法具体可以包括：

[0128] S301：获取用户办公所在的物理工作环境中的图像信息；

[0129] S302：根据所述图像信息对所述物理工作环境进行风险行为检测；

[0130] S303：如果检测到的风险行为触发预置的管控方案，则向安全管控系统发出安全管控指令，所述安全管控系统用于为所述用户的终端设备提供用于办公的软件工作环境，并在接收到所述安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

[0131] 具体实现时，具体的图像信息可以是由位于所述物理工作环境中的硬件设备进行采集并按照预置的时间间隔上传的。此时，除了可以由服务器根据接收到的图像信息进行风险行为检测，硬件设备也可以根据实时采集到的图像信息，在本地执行一些简单的风险行为检测，因此，服务器还可以接收硬件设备提交的风险行为检测结果。这样，可以综合硬件设备提交的风险行为检测结果与服务器检测到的风险行为这两部分信息，判断是否触发管控方案。

[0132] 实施例三

[0133] 该实施例三也是与实施例一相对应的，从具体环境检测子系统中的硬件设备关联的应用程序角度，提供了一种数据安全防控方法，参见图4，该方法可以包括：

[0134] S401：对用户办公所在的物理工作环境中的图像信息进行采集；

[0135] S402：根据采集到的图像信息获取风险行为检测结果；

[0136] S403：如果所述风险行为触发预置的管控方案，则向所述用户提供提醒消息。

[0137] 具体的，硬件设备可以包括智能音箱设备，也即，可以通过智能音箱设备的图像采集模块，对所述用户所在的物理工作环境中的图像信息进行采集。此时，可以通过所述智能音箱设备，向所述用户提供语音提醒消息。

[0138] 或者，具体的硬件设备也可以包括穿戴式设备，包括AR眼镜等，此时，可以通过所述用户关联的具有多个图像采集模块的穿戴式设备，以所述用户为中心，对所述用户所在的物理工作环境中的图像信息进行多角度采集。另外，在这种情况下，还可以通过所述穿戴

式设备，向所述用户提供单模态或多模态的提醒消息。例如，通过所述AR眼镜的镜片提供视觉提醒消息，通过关联的振动器提供振动提醒消息，通过骨传导装置提供语音提醒消息，等等。

[0139] 实施例四

[0140] 该实施例四也是与实施例一相对应的，从安全管控子系统的角度，提供了一种数据安全防控方法，参见图5，该方法可以包括：

[0141] S501：为办公用户的终端设备提供用于办公的软件工作环境；

[0142] S502：在接收到安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式行安全管控；其中，所述安全管控指令是对所述用户所在的物理工作环境进行图像采集及风险行为检测后生成的。

[0143] 其中，具体的管控动作也可以是在管控方案中进行定义的，因此，在根据具体的管控方案生成管控指令时，也可以将所需执行的管控动作携带在管控指令中，这样，安全管控子系统在收到具体的管控指令后，就可以直接根据指令中携带的管控动作信息，在用户的软件工作环境中执行对应的管控动作。例如，包括通过弹出窗口的方式提供提醒消息，或者，对所述终端设备进行锁屏处理(包括自动锁屏后，用户通过输入密码的方式解锁，或者强制锁屏后，用户需要联系管理员进行解锁，等等)。

[0144] 实施例五

[0145] 该实施例五还提供了一种智能音箱，参见图6，该智能音箱可以包括：

[0146] 图像采集模块601，用于对用户办公所在的物理工作环境中的图像信息进行采集；所述图像信息用于对所述物理工作环境中的风险行为进行检测；

[0147] 提醒模块602，用于在所检测到的风险行为触发管控方案时，向所述用户提供语音提醒消息。

[0148] 具体实现时，该智能音箱还可以包括：

[0149] 检测模块603，用于通过对采集到的图像信息进行分析，对所述物理工作环境中的风险行为进行检测。

[0150] 具体的检测结果可以直接在本地向用户进行提醒，或者，该智能音箱还可以包括：

[0151] 检测结果上传模块604，用于将检测到的风险行为信息上传到服务器，以便由所述服务器对风险行为进行汇总，并判断是否触发所述管控方案。

[0152] 另外，该智能音箱还可以包括：

[0153] 图像采集信息上传模块605，用于按照预置的时间间隔，将所采集到的图像信息上传到服务器，以便所述服务器通过对接收到的图像信息进行分析，对所述物理工作环境中的风险行为进行检测。

[0154] 实施例六

[0155] 该实施例六提供了一种增强现实AR眼镜，参见图7，该AR眼镜可以包括：

[0156] 多个图像采集模块701，用于以用户为中心，对所述用户办公所在的物理工作环境中的图像信息进行多角度采集；所述图像信息用于对所述物理工作环境中的风险行为进行检测；

[0157] 提醒模块702，用于在所检测到的风险行为触发管控方案时，向所述用户提供提醒消息。

[0158] 其中，所述提醒模块可以包括视觉提醒模块，用于通过所述AR眼镜的镜片提供视觉提醒消息。

[0159] 具体的，所述视觉提醒模块具体可以用于，通过输出虚拟图像对所述AR眼镜的镜片进行模糊处理，或者，通过所述AR眼镜输出提醒信息，或者，通过控制所述AR眼镜的镜片对用户观看的目标进行遮挡。

[0160] 或者，所述AR眼镜还带有振动器；

[0161] 此时，所述提醒模块包括振动提醒模块，用于通过所述振动器提供振动提醒消息。

[0162] 或者，所述AR眼镜还带有骨传导装置；

[0163] 此时，所述提醒模块包括骨传导提醒模块，用于通过所述骨传导装置提供语音提醒消息。

[0164] 关于上述实施例二至实施例六中的未详述部分，可以参见实施例一以及本申请说明书其他部分的记载，这里不再赘述。

[0165] 需要说明的是，本申请实施例中可能会涉及到对用户数据的使用，在实际应用中，可以在符合所在国的适用法律法规要求的情况下(例如，用户明确同意，对用户切实通知，等)，在适用法律法规允许的范围内在本文描述的方案中使用用户特定的个人数据。

[0166] 与实施例二相对应，本申请实施例还提供了一种数据安全防控装置，参见图8，该装置可以包括：

[0167] 图像信息获取单元801，用于获取用户办公所在的物理工作环境中的图像信息；

[0168] 风险行为检测单元802，用于根据所述图像信息对所述物理工作环境进行风险行为检测；

[0169] 指令发送单元803，用于如果检测到的风险行为触发预置的管控方案，则向安全管控系统发出安全管控指令，所述安全管控系统用于为所述用户的终端设备提供用于办公的软件工作环境，并在接收到所述安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控。

[0170] 其中，所述图像信息是由位于所述物理工作环境中的硬件设备进行采集并按照预置的时间间隔上传的；

[0171] 此时，所述装置还包括：

[0172] 检测结果接收单元，用于接收硬件设备提交的风险行为检测结果，所述硬件设备提交的风险行为检测结果是根据实时采集的图像信息进行判断获得的。

[0173] 与实施例三相对应，本申请实施例还提供了一种数据安全防控装置，参见图9，该装置可以包括：

[0174] 图像采集单元901，用于对用户办公所在的物理工作环境中的图像信息进行采集；

[0175] 风险行为检测单元902，用于根据采集到的图像信息获取风险行为检测结果；

[0176] 提醒单元903，用于如果所述风险行为触发预置的管控方案，则向所述用户提供提醒消息。

[0177] 其中，所述图像采集单元具体可以用于：

[0178] 通过智能音箱设备的图像采集模块，对所述用户办公所在的物理工作环境中的图像信息进行采集；

[0179] 所述提醒单元具体可以用于：

[0180] 通过所述智能音箱设备，向所述用户提供语音提醒消息。

[0181] 或者，所述图像采集单元具体可以用于：

[0182] 通过所述用户关联的具有多个图像采集模块的穿戴式设备，以所述用户为中心，对所述用户办公所在的物理工作环境中的图像信息进行多角度采集；

[0183] 此时，所述提醒单元具体可以用于：

[0184] 通过所述穿戴式设备，向所述用户提供单模态或多模态的提醒消息。

[0185] 与实施例四相对应，本申请实施例还提供了一种数据安全防控装置，参见图10，该装置可以包括：

[0186] 软件工作环境提供单元1001，用于为办公用户的终端设备提供用于办公的软件工作环境；

[0187] 管控动作执行单元1002，用于在接收到安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式行安全管控；

[0188] 其中，所述安全管控指令是对所述用户办公所在的物理工作环境进行图像采集及风险行为检测后生成的。

[0189] 另外，本申请实施例还提供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前述方法实施例中任一项所述的方法的步骤。

[0190] 以及一种电子设备，包括：

[0191] 一个或多个处理器；以及

[0192] 与所述一个或多个处理器关联的存储器，所述存储器用于存储程序指令，所述程序指令在被所述一个或多个处理器读取执行时，执行前述方法实施例中任一项所述的方法的步骤。

[0193] 其中，图11示例性的展示出了电子设备的架构，具体可以包括处理器1110，视频显示适配器1111，磁盘驱动器1112，输入/输出接口1113，网络接口1114，以及存储器1120。上述处理器1110、视频显示适配器1111、磁盘驱动器1112、输入/输出接口1113、网络接口1114，与存储器1120之间可以通过通信总线1130进行通信连接。

[0194] 其中，处理器1110可以采用通用的CPU(Central Processing Unit，处理器)、微处理器、应用专用集成电路(Application Specific Integrated Circuit，ASIC)、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本申请所提供的技术方案。

[0195] 存储器1120可以采用ROM(Read Only Memory，只读存储器)、RAM(Random Access Memory，随机存取存储器)、静态存储设备，动态存储设备等形式实现。存储器1120可以存储用于控制电子设备1100运行的操作系统1121，用于控制电子设备1100的低级别操作的基本输入输出系统(BIOS)。另外，还可以存储网页浏览器1123，数据存储管理系统1124，以及数据安全防控处理系统1125等等。上述数据安全防控处理系统1125就可以是本申请实施例中具体实现前述各步骤操作的应用程序。总之，在通过软件或者固件来实现本申请所提供的技术方案时，相关的程序代码保存在存储器1120中，并由处理器1110来调用执行。

[0196] 输入/输出接口1113用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中(图中未示出)，也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[0197] 网络接口1114用于连接通信模块(图中未示出),以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式(例如USB、网线等)实现通信,也可以通过无线方式(例如移动网络、WIFI、蓝牙等)实现通信。

[0198] 总线1130包括一通路,在设备的各个组件(例如处理器1110、视频显示适配器1111、磁盘驱动器1112、输入/输出接口1113、网络接口1114,与存储器1120)之间传输信息。

[0199] 需要说明的是,尽管上述设备仅示出了处理器1110、视频显示适配器1111、磁盘驱动器1112、输入/输出接口1113、网络接口1114,存储器1120,总线1130等,但是在具体实施过程中,该设备还可以包括实现正常运行所必需的其他组件。此外,本领域的技术人员可以理解的是,上述设备中也可以仅包含实现本申请方案所必需的组件,而不必包含图中所示的全部组件。

[0200] 通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例或者实施例的某些部分所述的方法。

[0201] 本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于系统或系统实施例而言,由于其基本相似于方法实施例,所以描述得比较简单,相关之处参见方法实施例的部分说明即可。以上所描述的系统及系统实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0202] 以上对本申请所提供的数据安全防控方法、系统及AR眼镜,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。

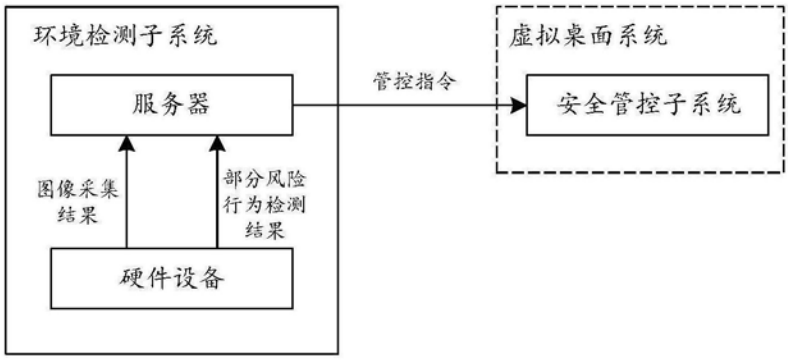

环境检测子系统
服务器
图像采集结果
部分风险行为检测结果
硬件设备
管控指令
虚拟桌面系统
安全管控子系统

图1


摄像头4:后
摄像头2:左
360°监控视野
摄像头2:右
摄像头1:前

图2

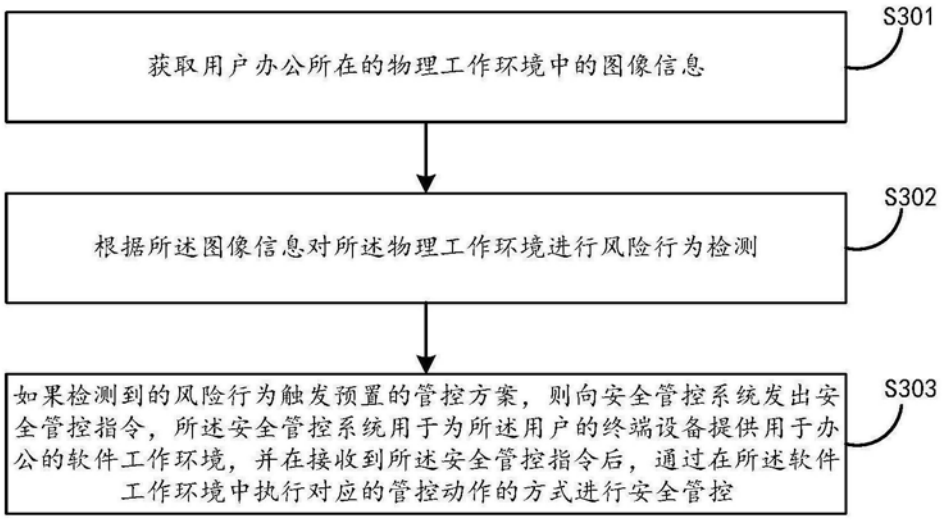

S301
获取用户办公所在的物理工作环境中的图像信息
S302
根据所述图像信息对所述物理工作环境进行风险行为检测
S303
如果检测到的风险行为触发预置的管控方案，则向安全管控系统发出安全管控指令，所述安全管控系统用于为所述用户的终端设备提供用于办公的软件工作环境，并在接收到所述安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式进行安全管控

图3

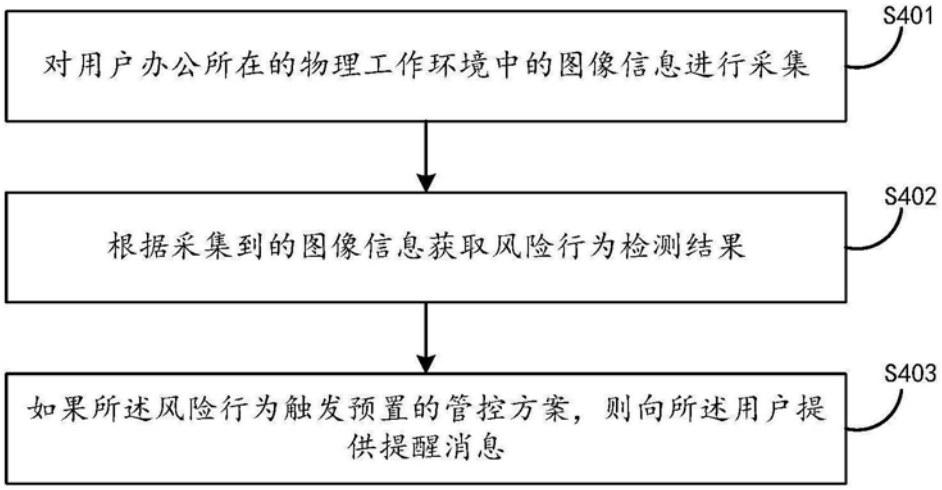

S401
对用户办公所在的物理工作环境中的图像信息进行采集
S402
根据采集到的图像信息获取风险行为检测结果
S403
如果所述风险行为触发预置的管控方案，则向所述用户提供提醒消息

图4

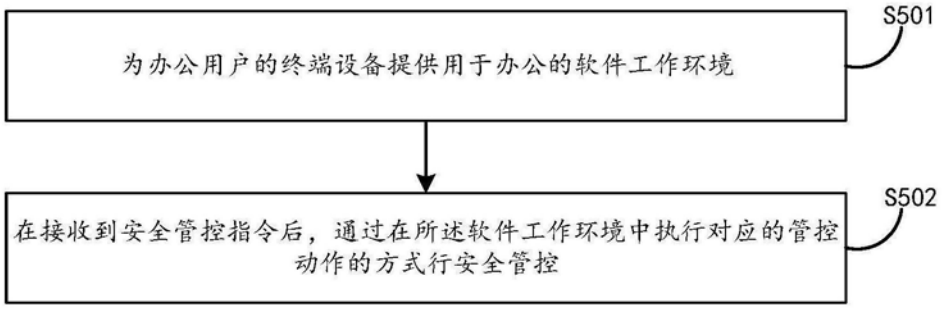

S501
为办公用户的终端设备提供用于办公的软件工作环境
S502
在接收到安全管控指令后，通过在所述软件工作环境中执行对应的管控动作的方式行安全管控

图5


601
图像采集模块
602
提醒模块

图6


701
图像采集模块
图像采集模块
图像采集模块
702
提醒模块

图7


801
图像信息获取单元
802
风险行为检测单元
803
指令发送单元

图8


901
图像采集单元
902
风险行为检测单元
903
提醒单元

图9

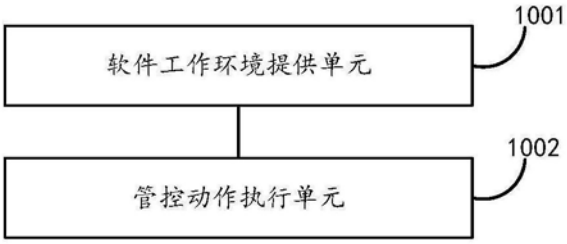

1001
软件工作环境提供单元
1002
管控动作执行单元

图10

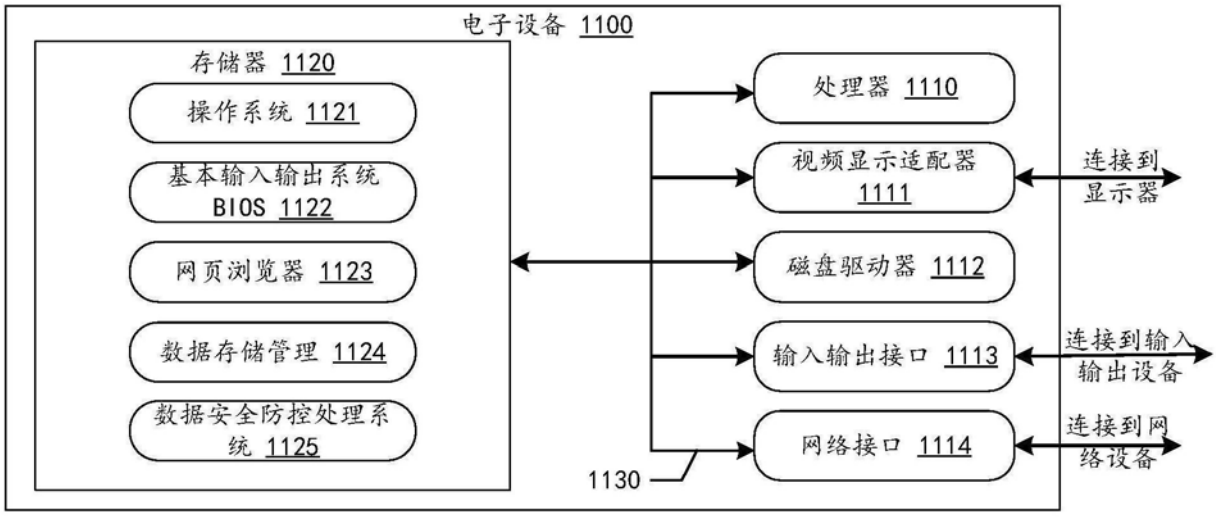

电子设备 1100
存储器 1120
操作系统 1121
基本输入输出系统 BIOS 1122
网页浏览器 1123
数据存储管理 1124
数据安全防控处理系统 1125
处理器 1110
视频显示适配器 1111
磁盘驱动器 1112
输入输出接口 1113
网络接口 1114
1130
连接到显示器
连接到输入输出设备
连接到网络设备

图11