(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109284590 B
(45)授权公告日 2021.06.25

(21)申请号 201811155063.9

(22)申请日 2018.09.29

(65)同一申请的已公布的文献号
申请公布号 CN 109284590 A

(43)申请公布日 2019.01.29

(73)专利权人 武汉极意网络科技有限公司
地址 湖北省武汉市东湖开发区大学园路武汉大学科技园内兴业楼2单元2楼204室-020号

(72)发明人 汪智勇 陈晨

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/56(2013.01)

(56)对比文件
CN 107153786 A,2017.09.12
US 2017185758 A1,2017.06.29

审查员 王青

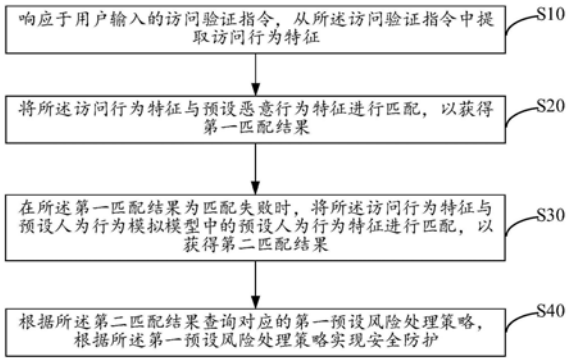
权利要求书2页 说明书10页 附图2页

(54)发明名称

访问行为安全防护的方法、设备、存储介质及装置

(57)摘要

本发明公开了一种访问行为安全防护的方法、设备、存储介质及装置。本发明中所述访问行为安全防护的方法包括以下步骤：响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。由于对存在风险的信息特征进行多次匹配确定对应的风险处理策略以实现安全防护，避免用户在访问验证时造成重大损失，提高用户的体验度。



CN 109284590 B

1.一种访问行为安全防护的方法，其特征在于，所述访问行为安全防护的方法包括以下步骤：

响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；

将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；

在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护；

所述将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果之后，还包括：

在所述第一匹配结果为匹配失败时，基于图卷积神经网络，建立图卷积模型；

通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得刷新的预设恶意行为特征及预设人为行为模拟模型。

2.如权利要求1所述的访问行为安全防护的方法，其特征在于，所述将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果之后，所述访问行为安全防护的方法还包括：

在所述第一匹配结果为匹配成功时，根据所述第一匹配结果查询对应的第二预设风险处理策略；

根据所述第二预设风险处理策略实现安全防护。

3.如权利要求1所述的访问行为安全防护的方法，其特征在于，所述通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，以获得刷新的预设恶意行为特征及预设人为行为模拟模型之后，所述访问行为安全防护的方法还包括：

将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果。

4.如权利要求3所述的访问行为安全防护的方法，其特征在于，所述将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果之后，所述访问行为安全防护的方法还包括：

在所述第二匹配结果为匹配成功时，根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

5.如权利要求3所述的访问行为安全防护的方法，其特征在于，所述将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果之后，所述访问行为安全防护的方法还包括：

在所述第二匹配结果为匹配失败时，通过所述图卷积模型再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得再次刷新的预设恶意行为特征及预设人为行为模拟模型；

将所述匹配结果失败的访问行为特征与所述预设恶意行为特征进行匹配，以获得第三匹配结果；

在所述第三匹配结果为匹配失败时，将所述匹配结果失败的访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第四匹配结果；

根据所述第四匹配结果查询对应的第三预设风险处理策略，根据所述第三预设风险处理策略实现安全防护。

6.如权利要求1至5中任一项所述的访问行为安全防护的方法，其特征在于，所述根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护，具体包括：

根据所述第二匹配结果匹配查找对应的风险等级和对应风险等级的原因；

根据所述风险等级和风险原因确定对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

7.一种用户设备，其特征在于，所述用户设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的访问行为安全防护程序，所述访问行为安全防护程序被所述处理器执行时实现如权利要求1至6中任一项所述的访问行为安全防护的方法的步骤。

8.一种存储介质，其特征在于，所述存储介质上存储有访问行为安全防护程序，所述访问行为安全防护程序被处理器执行时实现如权利要求1至6中任一项所述的访问行为安全防护的方法的步骤。

9.一种访问行为安全防护的装置，其特征在于，所述访问行为安全防护的装置包括：

访问行为特征提取模块，用于响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；

访问行为特征匹配模块，用于将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

风险处理模块，用于根据所述第二匹配结果查询对应的第一预设风险处理策略根据所述第一预设风险处理策略实现安全防护；

所述访问行为特征匹配模块，还用于在所述第一匹配结果为匹配失败时，基于图卷积神经网络，建立图卷积模型；

所述访问行为特征匹配模块，还用于通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得刷新的预设恶意行为特征及预设人为行为模拟模型。

访问行为安全防护的方法、设备、存储介质及装置

技术领域

[0001] 本发明涉及访问行为安全防护技术领域，尤其涉及访问行为安全防护的方法、设备、存储介质及装置。

背景技术

[0002] 目前随着信息科技的快速发展，各大数据平台上出现的病毒或者垃圾广告等恶意信息也越来越多，因此，信息安全的防护也越来越受到大家的关注。

[0003] 考虑到现在各大智能化数据平台存在的安全隐患的因素越来越多，目前现有的安全防护措施针对安全隐患的因素的覆盖不全面，也极容易存在着信息数据的泄露或者未知病毒的侵害等情况，造成重大损失，影响用户的体验。

发明内容

[0004] 本发明的主要目的在于提供访问行为安全防护的方法、设备、存储介质及装置，旨在解决对存在风险的信息特征进行多次匹配确定对应的风险处理策略以实现安全防护的技术问题。

[0005] 为实现上述目的，本发明提供一种访问行为安全防护的方法，所述访问行为安全防护的方法包括以下步骤：

[0006] 响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；

[0007] 将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；

[0008] 在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

[0009] 根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0010] 优选地，所述将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果之后，所述访问行为安全防护的方法还包括：

[0011] 在所述第一匹配结果为匹配成功时，根据所述第一匹配结果查询对应的第二预设风险处理策略；

[0012] 根据所述第二预设风险处理策略实现安全防护。

[0013] 优选地，将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果之后，所述访问行为安全防护的方法还包括：

[0014] 在所述第一匹配结果为匹配失败时，基于图卷积神经网络，建立图卷积模型；

[0015] 通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得刷新的预设恶意行为特征及预设人为行为模拟模型。

[0016] 优选地，所述通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，以获得刷新的预设恶意行为特征及预设人为行为模拟模型之后，所述访问行为安全防护的方法还包括：

[0017] 将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果。

[0018] 优选地，所述将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果之后，所述访问行为安全防护的方法还包括：

[0019] 在所述第二匹配结果为匹配成功时，根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0020] 优选地，所述将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果之后，所述访问行为安全防护的方法还包括：

[0021] 在所述第二匹配结果为匹配失败时，通过所述图卷积模型再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得再次刷新的预设恶意行为特征及预设人为行为模拟模型；

[0022] 将所述匹配结果失败的访问行为特征与所述预设恶意行为特征进行匹配，以获得第三匹配结果；

[0023] 在所述第三匹配结果为匹配失败时，将所述匹配结果失败的访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第四匹配结果；

[0024] 根据所述第四匹配结果查询对应的第三预设风险处理策略，根据所述第三预设风险处理策略实现安全防护。

[0025] 优选地，所述根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护，具体包括：

[0026] 根据所述第二匹配结果匹配查找对应的风险等级和对应风险等级的原因；

[0027] 根据所述风险等级和风险原因确定对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0028] 此外，为实现上述目的，本发明还提供一种用户设备，所述用户设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的访问行为安全防护程序，所述访问行为安全防护程序被所述处理器执行时实现所述的访问行为安全防护的方法的步骤。

[0029] 此外，为实现上述目的，本发明还提供一种存储介质，所述存储介质上存储有访问行为安全防护程序，所述访问行为安全防护程序被处理器执行时实现所述的访问行为安全防护的方法的步骤。

[0030] 此外，为实现上述目的，本发明还提供一种访问行为安全防护的装置，所述访问行为安全防护的装置包括：

[0031] 访问行为特征提取模块，用于响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；

[0032] 访问行为特征匹配模块，用于将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

[0033] 风险处理模块，用于根据所述第二匹配结果查询对应的第一预设风险处理策略根据所述第一预设风险处理策略实现安全防护。

[0034] 本发明中，响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述

第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。由于将所述访问行为特征与所述预设恶意行为特征及所述预设人为行为模拟模型中的预设认为行为特征进行多次匹配，从而根据所述风险等级和风险原因确定对应的风险处理策略以实现安全防护，避免用户在访问验证时造成重大损失，提高用户的体验度。

附图说明

[0035] 图1是本发明实施例方案涉及的硬件运行环境的用户设备结构示意图；

[0036] 图2为本发明访问行为安全防护的方法第一实施例的流程示意图；

[0037] 图3为本发明访问行为安全防护的方法第二实施例的流程示意图；

[0038] 图4为本发明访问行为安全防护的装置的功能模块图。

[0039] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0040] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0041] 参照图1，图1是本发明实施例方案涉及的硬件运行环境的用户设备结构示意图。

[0042] 如图1所示，所述用户设备可以包括：处理器1001，例如CPU，通信总线1002、用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储服务器。

[0043] 本领域技术人员可以理解，图1中示出的结构并不构成对所述用户设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0044] 如图1所示，作为一种存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及访问行为安全防护程序。

[0045] 在图1所示的结构中，网络接口1004主要用于连接服务器，与所述服务器进行数据通信；用户接口1003主要用于连接用户设备，与所述用户设备进行数据通信；所述用户设备通过处理器1001调用存储器1005中存储的访问行为安全防护程序，并执行以下操作：

[0046] 响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；

[0047] 将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；

[0048] 在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

[0049] 根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0050] 进一步地，处理器1001可以调用存储器1005中存储的访问行为安全防护程序，还执行以下操作：

[0051] 在所述第一匹配结果为匹配成功时，根据所述第一匹配结果查询对应的第二预设

风险处理策略；

[0052] 根据所述第二预设风险处理策略实现安全防护。

[0053] 进一步地，处理器1001可以调用存储器1005中存储的访问行为安全防护程序，还执行以下操作：

[0054] 在所述第一匹配结果为匹配失败时，基于图卷积神经网络，建立图卷积模型；

[0055] 通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得刷新的预设恶意行为特征及预设人为行为模拟模型。

[0056] 进一步地，处理器1001可以调用存储器1005中存储的访问行为安全防护程序，还执行以下操作：

[0057] 将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果。

[0058] 进一步地，处理器1001可以调用存储器1005中存储的访问行为安全防护程序，还执行以下操作：

[0059] 在所述第二匹配结果为匹配成功时，根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0060] 进一步地，处理器1001可以调用存储器1005中存储的访问行为安全防护程序，还执行以下操作：

[0061] 在所述第二匹配结果为匹配失败时，通过所述图卷积模型再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得再次刷新的预设恶意行为特征及预设人为行为模拟模型；

[0062] 将所述匹配结果失败的访问行为特征与所述预设恶意行为特征进行匹配，以获得第三匹配结果；

[0063] 在所述第三匹配结果为匹配失败时，将所述匹配结果失败的访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第四匹配结果；

[0064] 根据所述第四匹配结果查询对应的第三预设风险处理策略，根据所述第三预设风险处理策略实现安全防护。

[0065] 进一步地，处理器1001可以调用存储器1005中存储的访问行为安全防护程序，还执行以下操作：

[0066] 根据所述第二匹配结果匹配查找对应的风险等级和对应风险等级的原因；

[0067] 根据所述风险等级和风险原因确定对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0068] 本实施例中，响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。由于将所述访问行为特征与所述预设恶意行为特征及所述预设人为行为模拟模型中的预设认为行为特征进行多次匹配，从而根据所述风险等级和风险原因确定对应的风险处理策略以实现安全防护，避免用户在访问验证时造成重大损失，提高用户的体验度。

[0069] 基于上述硬件结构，提出本发明访问行为安全防护的方法的实施例。

[0070] 参照图2，图2为本发明访问行为安全防护的方法第一实施例的流程示意图。

[0071] 在第一实施例中，所述智能安全防护的方法包括以下步骤：

[0072] 步骤S10：响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征。

[0073] 可以理解的是，本实施例的执行主体是用户设备，应用场景是用户在使用设备时登陆网站注册、投票、请求或者不同网页接口及不同网页小程序等，将访问验证指令输入到此设备中，用户设备响应于所述访问验证指令，通过埋点技术从所述访问验证指令中提取访问行为特征，所述访问行为特征可以是标识、行为等访问行为特征，也可以是设备、网络及嗅探等，此处不再一一赘述。

[0074] 在具体实现中，所述访问验证指令可以是用户在设备上点击网页的验证事件，也可以是用户在触摸屏上输入的开机触摸事件，本实施例对此不加以限制。通过埋点技术从所述访问验证指令中获取信息特征以提取访问行为特征进行验证匹配。

[0075] 步骤S20：将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；

[0076] 需要说明的是，为了获得第一匹配结果，预先将在用户设备中存储预设恶意行为特征，以便将所述访问行为特征与预设恶意行为特征进行一一匹配。所述预设恶意行为特征可以是预先通过多种实验验证手段记录的有明显恶意标识的黑名单，也可以是在设备运行过程中获取的恶意行为特征，本实施例对此不加以限制。

[0077] 在具体实现中，将所述访问行为特征与预设恶意行为特征进行匹配，例如，所述访问行为特征中的标识特征与预设恶意行为特征进行匹配，即与预设恶意行为特征中有恶意标识特征进行匹配，则所述第一匹配结果为匹配成功；若预设恶意行为特征中不包括有恶意标识特征，则所述第一匹配结果为匹配失败。

[0078] 步骤S30：在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

[0079] 需要说明的是，为了获得第二匹配结果，预先将在用户设备中存储预设人为行为模拟模型，以便将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行一一匹配。所述预设人为行为模拟模型可以是预先通过多种实验验证手段建立的人为行为模拟模型，也可以是在设备运行过程中获取的各类人为行为模拟模型，比如行为行为模型及性能模型，本实施例对此不加以限制。

[0080] 在具体实现中，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，例如，所述访问行为特征中的行为特征与预设人为行为模拟模型进行匹配，即与预设人为行为模拟模型中的预设人为行为特征进行匹配，则所述第二匹配结果为匹配成功；若预设人为行为模拟模型中的预设人为行为特征中不包括有所述访问行为特征中的行为特征，则所述第二匹配结果为匹配失败。

[0081] 步骤S40：根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0082] 需要说明的是，为了使得所述第二匹配结果能查询到对应的的第一预设风险处理策略，预先在用户设备中存储有不同风险处理策略，例如弹出验证、拦截、限制活动即限制

资源，本实施例对此不加以限制。

[0083] 在具体实现中，根据所述第二匹配结果匹配查找对应的风险等级和对应风险等级的原因，根据所述风险等级和风险原因确定对应的第一预设风险处理策略，例如，所述高危风险等级对应的是限制活动的风险处理策略，根据所述限制活动的风险处理策略实现安全防护。

[0084] 本实施例中，响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。由于将所述访问行为特征与所述预设恶意行为特征及所述预设人为行为模拟模型中的预设认为行为特征进行多次匹配，从而根据所述风险等级和风险原因确定对应的风险处理策略以实现安全防护，避免用户在访问验证时造成重大损失，提高用户的体验度。

[0085] 参照图3，图3为本发明访问行为安全防护的方法第二实施例的流程示意图，基于上述图2所示的实施例，提出本发明访问行为安全防护的方法第二实施例。

[0086] 在第二实施例中，所述S20步骤之后，还包括：

[0087] 步骤S410：在所述第一匹配结果为匹配成功时，根据所述第一匹配结果查询对应的第二预设风险处理策略。

[0088] 需要说明的是，在所述第一匹配结果为匹配成功时，即所述访问行为特征第一次与预设恶意行为特征进行匹配时，所述预设恶意行为特征包括有所述访问行为特征，则根据所述第一匹配结果查找对应的风险等级和对应风险等级的原因。

[0089] 步骤S411：根据所述第二预设风险处理策略实现安全防护。

[0090] 需要说明的是，通过步骤S410所述第一匹配结果查找对应的风险等级和对应风险等级的原因，确定对应的第二预设风险处理策略，根据所述第二预设风险处理策略实现安全防护。

[0091] 进一步地，在第二实施例中，所述S20步骤之后，还包括：

[0092] 步骤S220：在所述第一匹配结果为匹配失败时，基于图卷积神经网络，建立图卷积模型；通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得刷新的预设恶意行为特征及预设人为行为模拟模型。

[0093] 需要说明的是，所述图卷积模型基于图卷积神经网络的算法来建立，通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，以获得刷新的预设恶意行为特征及预设人为行为模拟模型，以使得刷新的预设恶意行为特征及预设人为行为模拟模型与所述访问行为特征多次匹配后的匹配结果为匹配成功的机率更高。

[0094] 步骤S31：将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果。

[0095] 步骤S420：在所述第二匹配结果为匹配成功时，根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0096] 需要说明的是，通过步骤S220中所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，使得所述访问行为特征与所述预设人为行为模拟

模型中的预设人为行为特征进行匹配的匹配结果为匹配成功，提高了匹配成功的机率。

[0097] 步骤S230：在所述第二匹配结果为匹配失败时，通过所述图卷积模型再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得再次刷新的预设恶意行为特征及预设人为行为模拟模型。

[0098] 需要说明的是，经过所述第二匹配结果显示为匹配失败时，所述图卷积模型会再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，以便所述预设恶意行为特征及所述预设人为行为模拟模型的特征能进行刷新，以此来提高匹配成功的机率。

[0099] 步骤S21：将所述匹配结果失败的访问行为特征与所述预设恶意行为特征进行匹配，以获得第三匹配结果。

[0100] 步骤S32：在所述第三匹配结果为匹配失败时，将所述匹配结果失败的访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第四匹配结果。

[0101] 步骤S430：根据所述第四匹配结果查询对应的第三预设风险处理策略，根据所述第三预设风险处理策略实现安全防护。

[0102] 本实施例中，通过所述图卷积模型再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，上述步骤S21的具体做法跟步骤S20类似，即获得第三匹配结果，通过步骤S32获得第四匹配结果，步骤S430根据所述第四匹配结果查询对应的第三预设风险处理策略，根据所述第三预设风险处理策略实现安全防护，整个实现过程则是跟步骤S20、步骤S30及步骤S40的方法类似，此处不再一一赘述，由此将所述访问行为特征与所述预设恶意行为特征及所述预设人为行为模拟模型中的预设认为行为特征进行多次匹配。从而根据所述风险等级和风险原因确定对应的风险处理策略以实现安全防护，避免用户在访问验证时造成重大损失，提高用户的体验度。

[0103] 此外，本发明实施例还提出一种存储介质，所述存储介质上存储有访问行为安全防护程序，所述访问行为安全防护程序被处理器执行时实现如下操作：

[0104] 响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；

[0105] 将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；

[0106] 在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

[0107] 根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0108] 进一步地，所述访问行为安全防护程序被处理器执行时还实现如下操作：

[0109] 在所述第一匹配结果为匹配成功时，根据所述第一匹配结果查询对应的第二预设风险处理策略；

[0110] 根据所述第二预设风险处理策略实现安全防护。

[0111] 进一步地，所述访问行为安全防护程序被处理器执行时还实现如下操作：

[0112] 在所述第一匹配结果为匹配失败时，基于图卷积神经网络，建立图卷积模型；

[0113] 通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得刷新的预设恶意行为特征及预设人为行为模拟模型。

[0114] 进一步地，所述访问行为安全防护程序被处理器执行时还实现如下操作：

[0115] 将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果。

[0116] 进一步地，所述访问行为安全防护程序被处理器执行时还实现如下操作：

[0117] 在所述第二匹配结果为匹配成功时，根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0118] 进一步地，所述访问行为安全防护程序被处理器执行时还实现如下操作：

[0119] 在所述第二匹配结果为匹配失败时，通过所述图卷积模型再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得再次刷新的预设恶意行为特征及预设人为行为模拟模型；

[0120] 将所述匹配结果失败的访问行为特征与所述预设恶意行为特征进行匹配，以获得第三匹配结果；

[0121] 在所述第三匹配结果为匹配失败时，将所述匹配结果失败的访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第四匹配结果；

[0122] 根据所述第四匹配结果查询对应的第三预设风险处理策略，根据所述第三预设风险处理策略实现安全防护。

[0123] 进一步地，所述访问行为安全防护程序被处理器执行时还实现如下操作：

[0124] 根据所述第二匹配结果匹配查找对应的风险等级和对应风险等级的原因；

[0125] 根据所述风险等级和风险原因确定对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。

[0126] 本实施例中，响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。由于将所述访问行为特征与所述预设恶意行为特征及所述预设人为行为模拟模型中的预设认为行为特征进行多次匹配，从而根据所述风险等级和风险原因确定对应的风险处理策略以实现安全防护，避免用户在访问验证时造成重大损失，提高用户的体验度。

[0127] 此外，参照图4，本发明实施例还提出一种访问行为安全防护的装置，所述访问行为安全防护的装置包括：

[0128] 访问行为特征提取模块10，用于响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；

[0129] 在具体实现中，所述访问验证指令可以是用户在设备上点击网页的验证事件，也可以是用户在触摸屏上输入的开机触摸事件，本实施例对此不加以限制。通过埋点技术从所述访问验证指令中获取信息特征以提取访问行为特征进行验证匹配。

[0130] 访问行为特征匹配模块20，用于将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；

[0131] 需要说明的是，为了获得第一匹配结果，预先将在用户设备中存储预设恶意行为特征，以便将所述访问行为特征与预设恶意行为特征进行一一匹配。所述预设恶意行为特

征可以是预先通过多种实验验证手段记录的有明显恶意标识的黑名单，也可以是在设备运行过程中获取的恶意行为特征，本实施例对此不加以限制。为了获得第二匹配结果，预先将在用户设备中存储预设人为行为模拟模型，以便将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行一一匹配。所述预设人为行为模拟模型可以是预先通过多种实验验证手段建立的人为行为模拟模型，也可以是在设备运行过程中获取的各类人为行为模拟模型，比如行为行为模型及性能模型，本实施例对此不加以限制。

[0132] 在具体实现中，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，例如，所述访问行为特征中的行为特征与预设人为行为模拟模型进行匹配，即与预设人为行为模拟模型中的预设人为行为特征进行匹配，则所述第二匹配结果为匹配成功；若预设人为行为模拟模型中的预设人为行为特征中不包括有所述访问行为特征中的行为特征，则所述第二匹配结果为匹配失败。

[0133] 风险处理模块30，用于根据所述第二匹配结果查询对应的第一预设风险处理策略根据所述第一预设风险处理策略实现安全防护。

[0134] 需要说明的是，为了使得所述第二匹配结果能查询到对应的的第一预设风险处理策略，预先在用户设备中存储有不同风险处理策略，例如弹出验证、拦截、限制活动即限制资源，本实施例对此不加以限制。

[0135] 在具体实现中，根据所述第二匹配结果匹配查找对应的风险等级和对应风险等级的原因，根据所述风险等级和风险原因确定对应的第一预设风险处理策略，例如，所述高危风险等级对应的是限制活动的风险处理策略，根据所述限制活动的风险处理策略实现安全防护。

[0136] 本实施例中，响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征；将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果；在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果；根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护。由于将所述访问行为特征与所述预设恶意行为特征及所述预设人为行为模拟模型中的预设认为行为特征进行多次匹配，从而根据所述风险等级和风险原因确定对应的风险处理策略以实现安全防护，避免用户在访问验证时造成重大损失，提高用户的体验度。

[0137] 本发明所述访问行为安全防护的装置的其他实施例或具体实现方式可参照上述各方法实施例，此处不再赘述。

[0138] 需要说明的是，在本文中，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、物品或者系统不仅包括那些要素，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、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0139] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。词语第一、第二、以及第三等的使用不表示任何顺序，可将这些词解释为名称。

[0140] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下

前者是更佳的实施方式。基于这样的理解，本发明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，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0141] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

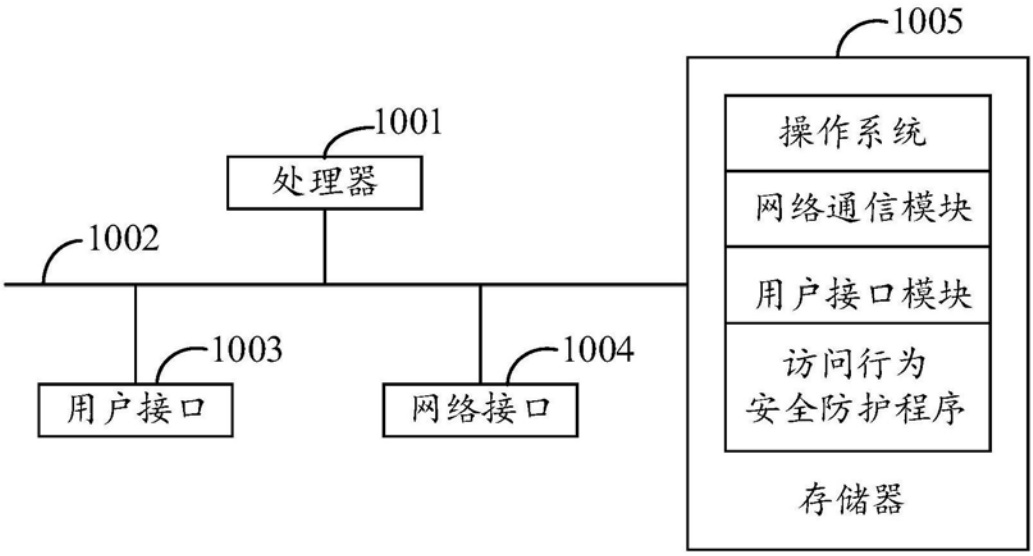

1005
操作系统
网络通信模块
用户接口模块
访问行为
安全防护程序
存储器
1001
处理器
1002
1003
用户接口
1004
网络接口

图1

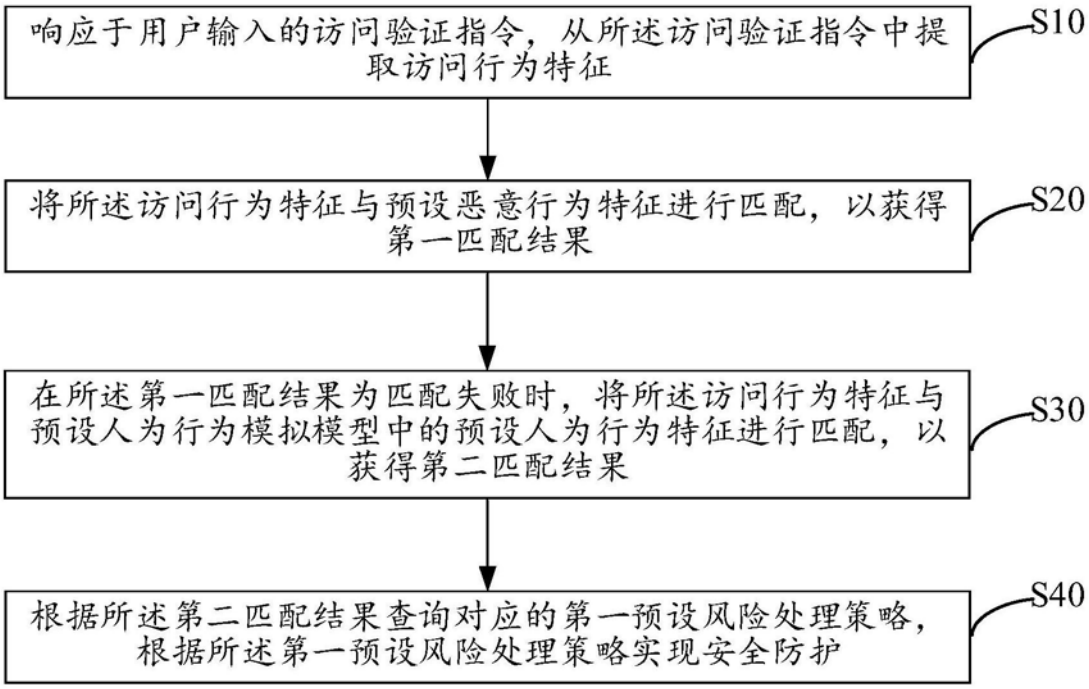

响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征
S10
将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果
S20
在所述第一匹配结果为匹配失败时，将所述访问行为特征与预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果
S30
根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护
S40

图2

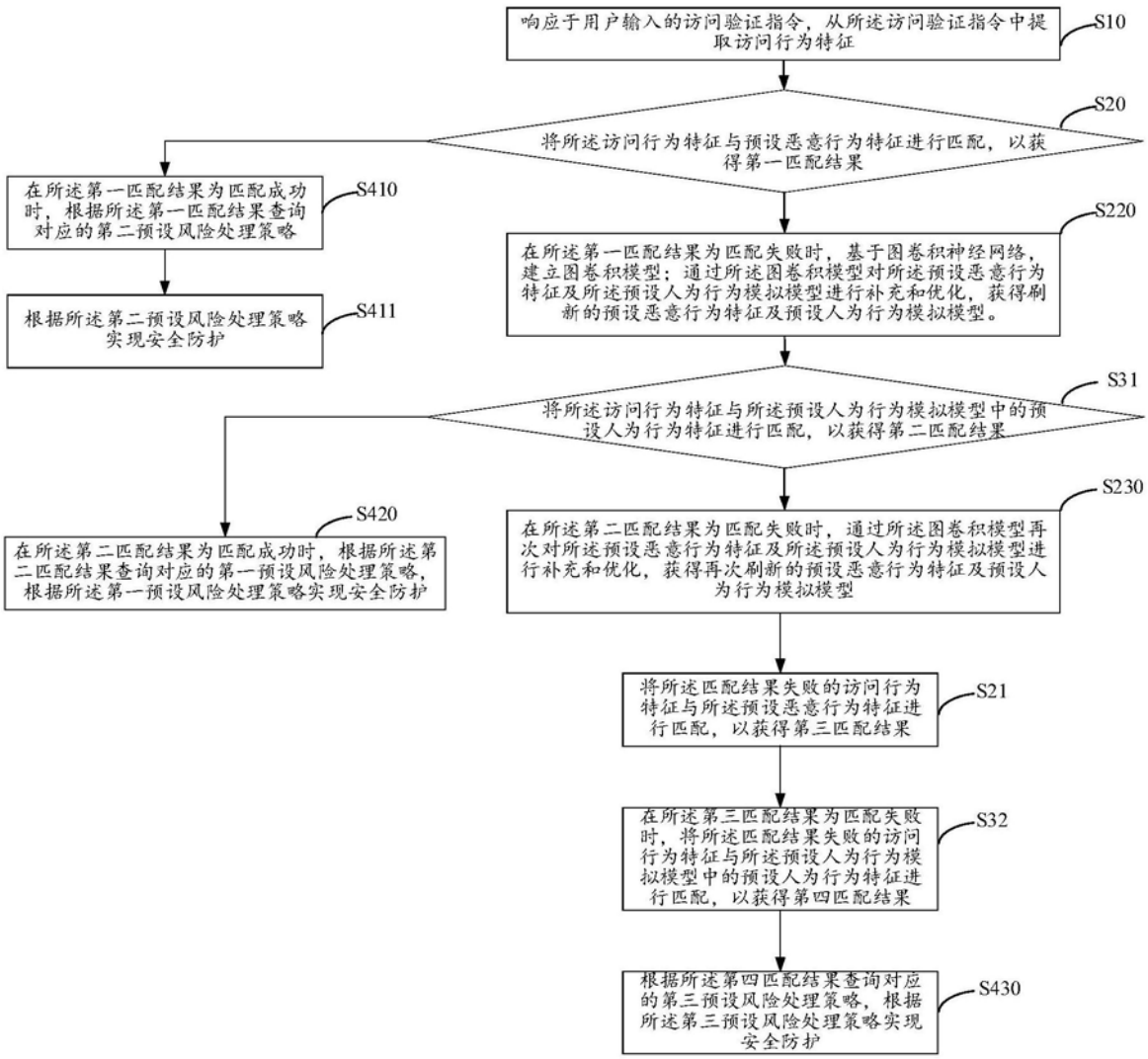

响应于用户输入的访问验证指令，从所述访问验证指令中提取访问行为特征
S10
将所述访问行为特征与预设恶意行为特征进行匹配，以获得第一匹配结果
S20
在所述第一匹配结果为匹配成功时，根据所述第一匹配结果查询对应的第二预设风险处理策略
S410
根据所述第二预设风险处理策略实现安全防护
S411
在所述第一匹配结果为匹配失败时，基于图卷积神经网络，建立图卷积模型；通过所述图卷积模型对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得刷新的预设恶意行为特征及预设人为行为模拟模型。
S220
将所述访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第二匹配结果
S31
在所述第二匹配结果为匹配成功时，根据所述第二匹配结果查询对应的第一预设风险处理策略，根据所述第一预设风险处理策略实现安全防护
S420
在所述第二匹配结果为匹配失败时，通过所述图卷积模型再次对所述预设恶意行为特征及所述预设人为行为模拟模型进行补充和优化，获得再次刷新的预设恶意行为特征及预设人为行为模拟模型
S230
将所述匹配结果失败的访问行为特征与所述预设恶意行为特征进行匹配，以获得第三匹配结果
S21
在所述第三匹配结果为匹配失败时，将所述匹配结果失败的访问行为特征与所述预设人为行为模拟模型中的预设人为行为特征进行匹配，以获得第四匹配结果
S32
根据所述第四匹配结果查询对应的第三预设风险处理策略，根据所述第三预设风险处理策略实现安全防护
S430

图3

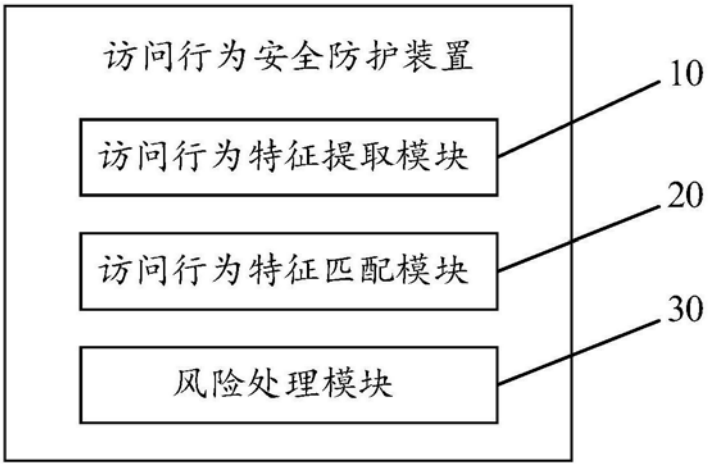

访问行为安全防护装置
访问行为特征提取模块
10
访问行为特征匹配模块
20
风险处理模块
30

图4