

一种核身方法和装置

技术领域

[01]本申请涉及计算机技术领域，尤其涉及一种核身方法和装置。

背景技术

5 [02]随着移动互联网的普及，以及移动支付业务的发展，越来越多的用户使用智能终端进行在线购物、支付等操作。

[03]为保护业务安全和用户对应资源的安全，在用户登录系统或者参与业务时，通常需
要对用户进行核身，以便确认请求登录系统或者参与业务的用户是否拥有对应的权限，
即判断当前登录系统的用户是否是用户本人。这就对核身的安全性和可靠性提出了较高
10 的要求。

[04]因此，亟需一种有利于提高核身安全性和可靠性，并满足用户使用需求的核身方法。

发明内容

[05]本申请实施例提供一种核身方法和装置，旨在提高核身的安全性和可靠性，并满足
用户的使用需求。

15 [06]本申请实施例采用下述技术方案：

[07]第一方面，本申请实施例提供一种核身方法，包括：

[08]接收来自待验证设备的核身请求，所述核身请求中包括所述待验证设备的设备环境
信息，用于请求对待验证设备所对应的用户进行核身；

[09]根据历史特征信息以及所述设备环境信息，确定所述待验证设备的可信程度；所述
20 历史特征信息包括历史设备的设备环境信息；

[10]根据所述待验证设备的可信程度，确定对用户进行核身的核身策略，以便按照所述
核身策略进行核身。

[11]优选地，第一方面提供的核身方法中，根据历史特征信息以及所述设备环境信息，
确定所述待验证设备的可信程度，包括：

- [12]当所述设备环境信息中所包含的信息类型与预设信息类型相匹配时,根据所述设备环境信息确定与所述待验证设备相对应的特征向量;
- [13]将所述特征向量输入设备验证模型,利用所述设备验证模型确定所述待验证设备的可信程度;其中,所述设备验证模型用于基于设备的设备环境信息,确定发出核身请求的设备的可信度标签,以及该核身请求被预测为可信请求的概率。
- [14]优选地,第一方面提供的核身方法中,在将所述特征向量输入设备验证模型,利用所述设备验证模型确定所述待验证设备的可信程度之前,所述方法还包括:
- [15]获取历史特征信息,所述历史特征信息与历史设备相对应;
- [16]根据历史特征信息所对应的时间区间,确定第一历史特征信息构成的训练集和第二历史特征信息构成的验证集;
- [17]采用第一历史特征信息对所述设备验证模型进行训练,采用第二历史特征信息对所述设备验证模型进行验证。
- [18]优选地,第一方面提供的核身方法中,根据历史特征信息所对应的时间区间,确定第一历史特征信息构成的训练集和第二历史特征信息构成的验证集,包括:
- [19]根据历史特征信息所对应的时间区间,将生成时间较早的第一历史特征信息分入所述训练集,将生成时间较晚的第二历史特征信息分入所述验证集。
- [20]优选地,第一方面提供的核身方法中,所述设备验证模型包括逻辑回归 LR 模型和极限梯度提升 XGBoost 模型;则采用第一历史特征信息对所述设备验证模型进行训练,包括:
- [21]根据第一历史特征信息,确定第一历史特征向量、第二历史特征向量,以及与所述第一历史特征信息相对应的历史设备的第一可信度标签;
- [22]将第一历史特征向量输入逻辑回归 LR 模型;根据所述第一可信度标签与所述逻辑回归 LR 模型输出的第一目标标签,调整所述逻辑回归 LR 模型的模型参数,直至所述逻辑回归 LR 模型的输出满足预设条件;
- [23]根据训练后的所述逻辑回归 LR 模型的输出,计算第一历史特征信息所对应设备发出的核身请求被预测为可信请求的第一概率;
- [24]将第一概率以及第二历史特征向量输入极限梯度提升 XGBoost 模型;利用所述极限梯度提升 XGBoost 模型的输出与所述第一可信度标签,调整所述极限梯度提升 XGBoost

模型的模型参数,直至所述极限梯度提升 XGBoost 模型的输出满足预设条件;其中,所述极限梯度提升 XGBoost 模型的输出,包括第一历史特征信息所对应历史设备的可信度标签,以及该历史设备发出的核身请求被预测为可信请求的概率。

5 [25]优选地,第一方面提供的核身方法中,采用第二历史特征信息对所述设备验证模型进行验证,包括:

[26]根据第二历史特征信息,确定第三历史特征向量、第四历史特征向量,以及与所述第二历史特征信息相对应的历史设备的第二可信度标签;

10 [27]将第三历史特征向量输入训练后的所述逻辑回归 LR 模型;根据训练后的所述逻辑回归 LR 模型的输出,计算第二历史特征信息所对应设备发出的核身请求被预测为可信请求的第二概率;

[28]将第二概率以及第四历史特征向量输入训练后的所述极限梯度提升 XGBoost 模型,利用训练后的所述极限梯度提升 XGBoost 模型得到所述设备验证模型的输出;所述设备验证模型的输出,包括第二历史特征信息所对应历史设备的可信度标签,以及该历史设备发出的核身请求被预测为可信请求的第三概率;

15 [29]根据所述设备验证模型的输出和所述第二可信度标签,利用二分类评估方法,得到所述设备验证模型的评估数据;

[30]根据所述评估数据调整所述逻辑回归 LR 模型和/或所述极限梯度提升 XGBoost 模型的模型参数,直至所述设备验证模型的评估数据满足预设条件。

20 [31]优选地,第一方面提供的核身方法中,所述设备验证模型的评估数据,包括 F1 分数和曲线下面积 AUC 值中至少一项。

[32]优选地,第一方面提供的核身方法中,所述逻辑回归 LR 模型的模型参数,包括正则项、正则系数、最大迭代次数中至少一项。

[33]优选地,第一方面提供的核身方法中,第一历史特征向量中分量的数量大于第二历史特征向量中分量的数量。

25 [34]优选地,第一方面提供的核身方法中,所述历史设备,包括历史登录设备和历史核身设备中至少一项。

[35]优选地,第一方面提供的核身方法中,根据历史特征信息以及所述设备环境信息,确定所述待验证设备的可信程度,包括:

[36]当所述设备环境信息中所包含的信息类型与预设信息类型不匹配时，确定所述待验证设备不可信。

[37]优选地，第一方面提供的核身方法中，所述预设信息类型，包括设备的身份标识 ID，以及设备所对应的无线连接 WIFI、基于位置服务 LBS 和互联网协议 IP 地址中至少一个。

5 [38]优选地，第一方面提供的核身方法中，根据所述待验证设备的可信程度，确定对用户进行核身的核身策略，包括：

[39]根据所述待验证设备的可信程度，以及核身策略与可信程度区间的对应关系，确定对用户进行核身的核身策略；

[40]其中，所述核身策略所匹配的风险等级与用户所持设备的可信程度负相关。

10 [41]优选地，第一方面提供的核身方法中，所述核身策略中包括核身信息类型、核身信息数量和核身阈值范围中至少一项；

[42]则所述核身策略所匹配的风险等级与用户所持设备的可信程度负相关，包括以下至少一项：

[43]当所述核身策略中包括所述核身信息类型时，所述核身策略中核身信息类型的安全
15 等级与用户所持设备的可信程度负相关；

[44]当所述核身策略中包括所述核身信息数量时，所述核身策略中的核身信息数量与用户所持设备的可信程度负相关；

[45]当所述核身策略中包括所述核身阈值范围时，所述核身策略中的核身阈值范围与用户所持设备的可信程度正相关。

20 [46]优选地，第一方面提供的核身方法中，按照所述核身策略进行核身，包括：

[47]按照所述核身策略确定核身流程、核身所需信息、以及核身所需信息的核身阈值范围；

[48]按照所述核身流程，提示所述待验证设备上报所述核身所需信息；

[49]当接收到所述待验证设备上报的所述核身所需信息时，根据核身所需信息的核身阈
25 值范围进行核身。

[50]第二方面，本申请实施例提供一种核身装置，包括：

[51]请求接收模块，接收来自待验证设备的核身请求，所述核身请求中包括所述待验证

设备的设备环境信息，用于请求对待验证设备所对应的用户进行核身；

[52]可信程度确定模块，根据历史特征信息以及所述设备环境信息，确定所述待验证设备的可信程度；所述历史特征信息包括历史设备的设备环境信息；

5 [53]核身策略确定模块，根据所述待验证设备的可信程度，确定对用户进行核身的核身策略，以便按照所述核身策略进行核身。

[54]第三方面，本申请实施例提供一种电子设备，包括：

[55]处理器；以及

[56]被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

10 [57]接收来自待验证设备的核身请求，所述核身请求中包括所述待验证设备的设备环境信息，用于请求对待验证设备所对应的用户进行核身；

[58]根据历史特征信息以及所述设备环境信息，确定所述待验证设备的可信程度；所述历史特征信息包括历史设备的设备环境信息；

15 [59]根据所述待验证设备的可信程度，确定对用户进行核身的核身策略，以便按照所述核身策略进行核身。

[60]第四方面，本申请实施例提供一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备执行以下操作：

20 [61]接收来自待验证设备的核身请求，所述核身请求中包括所述待验证设备的设备环境信息，用于请求对待验证设备所对应的用户进行核身；

[62]根据历史特征信息以及所述设备环境信息，确定所述待验证设备的可信程度；所述历史特征信息包括历史设备的设备环境信息；

[63]根据所述待验证设备的可信程度，确定对用户进行核身的核身策略，以便按照所述核身策略进行核身。

25 [64]本申请实施例采用的上述至少一个技术方案能够达到以下有益效果：

[65]采用本申请实施例，在接收到来自待验证设备的核身请求后并未直接进行核身，而是根据历史设备的设备环境信息以及待验证设备的设备环境信息，确定待验证设备的可

信程度，并进而根据可信程度确定对用户进行核身的核身策略。采用本申请实施例的方法，可以在用户无感知的情况下，根据用户所持设备的可信程度，为用户选择适用于当前所持设备的核身策略。因此，本申请实施例有利于提高核身的安全性和可靠性，并能够满足用户的使用需求，提升用户体验。

5 附图说明

[66]此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[67]图 1 为本申请实施例提供的核身方法的流程示意图；

[68]图 2 为本申请实施例提供的核身方法中第二种流程示意图；

10 [69]图 3 为本申请实施例提供的核身方法中第三种流程示意图；

[70]图 4 为本申请实施例提供的核身方法中第四种流程示意图；

[71]图 5 为本申请实施例提供的核身方法中第五种流程示意图；

[72]图 6 为本申请实施例提供的核身方法中第六种流程示意图；

[73]图 7 为本申请实施例提供的核身装置的结构示意图；

15 [74]图 8 为本申请实施例提供的一种电子设备的结构示意图。

具体实施方式

[75]为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例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在
20 没有做出创造性劳动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。

[76]在互联网时代，无论是移动互联网还是移动支付业务，为了网络平台和业务系统的安全，都需要对访问网络平台或者使用业务系统的用户进行核身，也可以称为身份验证、身份鉴权等，以确保访问网络平台或者使用业务系统的用户拥有合法资格。在具体实施
25 时，实现核身功能的核身系统既可以是独立于业务系统的专用核身系统，也可以是业务系统中的一部分。

[77]在对用户进行核身时，可以将申请核身用户输入核身系统的信息（例如，登录密码，

支付密码, 指纹等) 与核身系统后台预留的信息进行比对, 比对符合条件 (例如, 完全一致, 或者偏差在预设范围之内等) 时, 可以认为申请核身的用户通过身份验证, 具备参与业务的权限。

[78]可选的, 核身时可以采用生物识别技术, 例如, 指纹识别、人脸识别、声纹识别、虹膜识别等。在具体实施时, 可以将申请核身用户的生物特征与后台预留的生物特征进行比对, 根据比对的结果来验证用户的身份。

[79]可选的, 核身时也可以采用短信码验证或安全问题验证等方式。在具体实施时, 核身系统可以将随机生成的短信验证码或者预设的安全问题提供给申请核身的用户, 在收到用户反馈的短信码或者对安全问题的回答之后, 可以通过判断用户的回答与预留答案或者核身系统判定的正确答案是否一致来验证用户的身份。

[80]为提高核身的安全性和可靠性, 如果单独优化上述某一方面的性能, 例如, 通过设计更长、更复杂、更具时效性的密码来提高密码鉴权方法的安全性, 或者通过提升带宽和服务器稳定性来保证第三方口令 (如短信验证码) 的发送稳定性等, 随着技术水平的提高, 这种优化方式的边际成本也会越来越高。

[81]为了提高核身的安全性和可靠性, 并满足用户的使用需求, 本申请实施例提出了一种核身方法, 由核身系统执行。可以理解到, 核身系统可以独立于业务系统, 也可以作为业务系统的一部分, 在业务流程中实现验证用户身份的功能。本申请实施例提供的核身方法中, 利用设备环境信息进行辅助验证, 确定申请核身用户的潜在风险。具体的, 通过用户所持终端设备的设备环境信息以及历史设备的设备环境信息, 确定用户所持终端设备的可信程度, 并进而根据可信程度确定对用户进行核身的核身策略。

[82]需要说明的是, 终端设备的可信度越高, 表示申请核身用户使用该终端设备越合理、越安全, 可以采用相对宽松、与较低风险等级相匹配的核身策略对该用户进行核身。相对应的, 终端设备的可信度越低, 表示申请核身用户使用该终端设备越不合理, 越不安全, 需要采用相对严格、与较高风险等级相匹配的核身策略对该用户进行核身。

[83]能够理解, 用户所持的终端设备, 以及本申请实施例中所说的待验证设备, 可以是如个人计算机等设备, 也可以是如智能手机、平板电脑等移动终端设备, 该终端设备为用户在发出核身请求、申请参与业务时所使用的终端设备。

[84]采用本申请实施例的方法, 可以在用户无感知、可持续的情况下, 利用设备环境信息进行辅助核身。并且, 还可以与诸如生物特征、安全问题等强校验方式相结合, 根据

对用户所持设备的可信程度的确定结果，为用户选择适用于当前所持设备的核身策略。可选的，可以根据设备的可信程度，适当的调整生物识别或者安全问题验证方式的安全校验等级。例如，设备的可信程度越高，人脸核身时的比对阈值可以越低；又例如，设备的可信程度越高，安全问题校验时问题的个数可以越少，等等。

- 5 [85]因此，本申请实施例利用设备环境信息进行辅助核身，有利于提高核身的安全性和可靠性；并且，根据设备的可信程度，可以选择核身策略，能够更好的满足用户的使用需求，提升用户体验。

[86]以下结合附图，详细说明本申请各实施例提供的技术方案。

- 10 [87]参见图 1 所示，本申请实施例提供了一种核身方法，可以由核身系统执行，该方法可包括：

[88]S101：接收来自待验证设备的核身请求，核身请求中包括待验证设备的设备环境信息，用于请求对待验证设备所对应的用户进行核身。

- 15 [89]能够理解，当用户希望登录业务系统，或者在业务系统发起业务请求时，通常需要先进行身份验证，即核实其用户身份。核身系统执行步骤 S101 接收到的核身请求，可以是用户通过所持有的终端设备发起的登录请求或者业务请求，也可以是专用于请求对设备所对应的用户进行核身的核身请求。

- 20 [90]可选的，待验证设备的设备环境信息，可以包括待验证设备的身份标识 ID(Identity)和待验证设备所连接网络上的互联网协议 IP(Internet Protocol)地址等。对于连接到移动通信网络或者无线网络的待验证设备而言，待验证设备的设备环境信息还可以进一步包括设备所连接到的无线连接 WIFI(Wireless-Fidelity，又可简称为 WI-FI)和基于位置服务 LBS(Location Based Service)等。

- 25 [91]可以理解到，待验证设备向核身系统发送核身请求时，必然已经连接到互联网或者移动互联网。因此，待验证设备向核身系统发送的设备环境信息，能够反映待验证设备的身份(通过携带身份标识 ID 体现)，以及用户在使用待验证设备申请核身时所授权使用的网络环境，可具体通过设备所对应的 IP 地址、WIFI、LBS 等体现。

[92]S103：根据历史特征信息以及设备环境信息，确定待验证设备的可信程度，历史特征信息包括历史设备的设备环境信息。

[93]在接收到待验证设备的设备环境信息的基础上，核身系统进一步执行步骤 S103，结合包括历史设备的设备环境信息的历史特征信息，确定待验证设备的可信程度。能够理

解, 某一特定用户, 往往会对应到常用的一个或多个终端设备 (例如, 智能手机, 平板电脑, 可穿戴智能设备, 笔记本电脑等), 以及经常连接的一个或多个网络环境 (例如, 家庭网络, 办公网络, 常去的商场网络, 餐厅网络等), 这些常用的终端设备和经常连接的网络环境, 可以由上述历史特征信息体现。因此, 核身系统基于历史特征信息以及当前申请核身的设备环境信息, 可以确定待验证设备的可信程度, 通过可信程度反映特定用户使用该待验证申请核身是否合理, 是否符合常规。

[94]根据历史特征信息以及设备环境信息, 确定待验证设备的可信程度的方式和具体标准多种多样。例如, 可以将待验证设备的身份标识 ID 与历史特征信息中历史设备的身份标识 ID 进行对比, 若相同, 则可以认为待验证设备更可能可信。又例如, 可以将待验证设备所连接的网络环境与历史特征信息中历史设备所连接的网络环境进行匹配, 若相匹配 (例如, 待验证设备连接到与历史设备相同的 WIFI), 则可以认为待验证设备更可能可信。再例如, 可以将待验证设备基于 LBS 确定的位置信息与历史特征信息中历史设备基于 LBS 确定的位置信息进行匹配, 若不相匹配 (例如, 待验证设备所在的位置未出现在历史特征信息中), 则可以认为待验证设备更可能不可信。

[95]可选的, 核身系统在根据历史特征信息以及设备环境信息, 确定待验证设备的可信程度时, 如果待验证设备的设备环境信息中所包含的信息类型与预设信息类型不匹配, 核身系统可以直接判定待验证设备不可信。能够理解, 预设信息类型, 可以包括设备的身份标识 ID, 以及设备所对应的无线连接 WIFI、基于位置服务 LBS 和互联网协议 IP 地址中至少一个。需要说明的是, 由于用户所用设备以及可能接入的网络环境有不同类型, 因此, 根据设备正常接入网络能够具备的信息类型, 为不同情况的网络环境预先设定不同的预设信息类型。在这种情况下, 如果待验证设备发送到核身系统的设备环境信息中缺乏预设信息类型中已指定的信息类型, 则可以认为待验证设备可能被非法使用, 导致理应上报的设备环境信息被屏蔽以规避核身系统的验证, 因此, 核身系统可以直接判定该待验证设备不可信, 进而采用更加严格、适用于风险等级较高的核身策略进行核身。

[96]可选的, 核身系统在根据历史特征信息以及设备环境信息, 确定待验证设备的可信程度时, 可以利用一个设备验证模型进行。具体的, 该设备验证模型的输入为根据待验证设备的设备环境信息确定的特征向量, 输出为该待验证设备的可信度标签、以及该待验证设备发出的核身请求被预测为可信请求的概率。从而可以在此基础上确定对用户进行核身的核身策略。

[97]后文将详细举例说明设备验证模型的构建和训练方法，以及利用设备验证模型确定待验证设备的可信程度的具体实施过程。

[98]S105：根据待验证设备的可信程度，确定对用户进行核身的核身策略，以便按照核身策略进行核身。

- 5 [99]可选的，可以根据待验证设备的可信程度，以及核身策略与可信程度区间的对应关系，确定对用户进行核身的核身策略。其中，核身策略所匹配的风险等级与用户所持设备的可信程度负相关。

[100] 在具体实施时，可以在执行步骤 S105 之前，预先设定核身策略与可信程度区间的对应关系。设备的可信程度越高，表示该设备越可信，越合理，允许该设备登录或访问业务系统所带来的风险越低，因此，可以采用与越低风险等级相匹配的核身策略进行核身。反之，设备的可信程度越低，表示该设备越不可信，越不合理，允许该设备登录或访问业务系统所带来的风险越高，因此，需要采用与越高风险等级相匹配的核身策略进行核身。

10

[101] 在根据待验证设备的可信程度，确定对用户进行核身的核身策略时，当待验证设备的可信程度落入某可信程度区间时，即可将该可信程度区间所对应的核身策略确定为对使用该待验证设备的用户进行核身的核身策略。

15

[102] 需要说明的是，不同的核身策略，在核身信息类型、核身信息数量和核身阈值范围等方面中存在一项或多项不同。

[103] 例如，若核身策略中包括核身信息类型，核身策略中核身信息类型的安全等级越高，越适用于用户所持设备的可信程度越低的情况。因此，可以理解为核身信息类型的安全等级与设备的可信程度负相关。关于核身信息类型的安全等级，可以有多种界定标准。例如，用户的指纹、人脸、虹膜、声纹等生物特征，由于其专有性和不可复制性，因此，可以认为这些用户独有的生物特征信息构成的核身信息，安全等级通常高于短信认证、密码认证、安全问题验证等核身信息。又例如，可以认为单次有效的动态短信认证码，其安全等级通常高于固化不变的安全问题验证这类核身信息。能够理解，当用户所持设备的可信程度较低时，可以采用安全等级更高的核身信息进行核身，以便保证核身结果的可靠性，保障业务系统的安全；当用户所持设备的可信程度较高时，可以采用安全等级更低的核身信息进行核身，满足核身系统的核身要求即可。

20

25

[104] 又例如，若核身策略中包括核身信息数量，核身策略中的核身信息数量越多，

越适用于用户所持设备的可信程度越低的情况。因此，可以理解为核身信息的数量与设备的可信程度负相关。能够理解，核身信息的数量越多，能够从更多维度对用户进行核身，核身的结果更加可靠。可选的，当用户所持设备的可信程度较低时，可以增加核身信息的数量，以便对用户进行更全面的核身，保障业务系统的安全。可选的，当用户所持设备的可信程度较高时，则可以减少核身信息的数量（例如，减少安全校验问题的数量等），以便精简核身流程，提高核身效率，提高用户体验。

[105] 再例如，若核身策略中包括核身阈值范围，核身策略中的核身阈值范围越大，表示核身通过的标准越宽松，越适用于用户所持设备的可信程度较高的情况。因此，可以理解为核身阈值范围与设备的可信程度正相关。可选的，当用户所持设备的可信程度较低时，需要对用户进行更加严格的核身，因此，可以采用较小的核身阈值范围，核身信息未落入该范围的用户将无法通过核身。而当用户所持设备的可信程度较高时，可以对用户进行更加宽松的核身，因此，可以采用较大的核身阈值范围，使得用户的核身信息更大可能的落入该范围，有利于用户顺利通过核身，提高用户体验。

[106] 在一种场景下，假设核身系统采用人脸识别的信息作为核身信息，当用户所持设备的可信程度较高时，可以适当降低人脸比对阈值，即降低对被核身用户的人脸信息与核身系统中预留的人脸信息的匹配程度的要求，从而使得用户在诸如光线不足、光照不均等人脸采集环境不佳的情况下，能够更容易的通过核身，进行正常的业务处理。

[107] 可选的，在确定对用户进行核身的核身策略后，按照核身策略进行核身时，可以先按照核身策略确定核身流程、核身所需信息、以及核身所需信息的核身阈值范围。然后，核身系统按照核身流程提示待验证设备上报核身所需信息。用户持待验证设备收到核身系统的提示后，按照提示上报核身所需信息，例如，当接收到待验证设备上报的核身所需信息时，根据核身所需信息的核身阈值范围进行核身。

[108] 以上举例介绍了本申请实施例的主要实施过程。可以理解到，采用本申请实施例，在接收到来自待验证设备的核身请求后并未直接进行核身，而是根据历史设备的设备环境信息以及待验证设备的设备环境信息，确定待验证设备的可信程度，并进而根据可信程度确定对用户进行核身的核身策略。采用本申请实施例的方法，可以在用户无感知的情况下，根据用户所持设备的可信程度，为用户选择适用于当前所持设备的核身策略。因此，本申请实施例有利于提高核身的安全性和可靠性，并能够满足用户的使用需求，提升用户体验。

[109] 以下将进一步举例说明执行步骤 S103，根据历史特征信息以及设备环境信息，

确定待验证设备的可信程度的一种可选的方式。具体的，可以按以下步骤进行，参见图 2 所示：

[110] S1031：当设备环境信息中所包含的信息类型与预设信息类型相匹配时，根据设备环境信息确定与待验证设备相对应的特征向量。

- 5 [111] 可以理解到，核身系统可以按照不同的设备类型预先设定进行可信程度确定的预设信息类型。可选的，预设信息类型可包括设备的身份标识 ID、设备所连接网络上的 IP 地址、WIFI 和 LBS。对于正常连接到网络的设备，完整的设备环境信息应该包括所有预设信息类型的信息。如果核身系统接收到的设备环境信息有缺失（此时，设备环境信息中所包含的信息类型与预设信息类型不匹配），在无法判断是由于客观上网络环境等原因造成，还是由于非法用户主观上刻意阻碍、规避等原因造成的情况下，核身系统可以直接判定待验证设备不可信，即待验证设备的可信程度为最低级别。

[112] 当设备环境信息中所包含的信息类型与预设信息类型相匹配时，核身系统可以认为接收到的设备环境信息是有效的信息。因此，可在此基础上根据设备环境信息确定与待验证设备相对应的特征向量。

- 15 [113] 在根据设备环境信息确定特征向量时，可以有多种方式。可选的，可以根据待验证设备的设备环境信息，结合历史特征信息进行特征向量的确定。

- [114] 例如，可以判断待验证设备的设备环境信息与历史设备的设备环境信息是否一致，并将判断的结果作为特征向量的一个或多个分量。对于设备环境信息中有多项具体内容的情况，对每项具体内容可以分别比对。这一比对过程，可以理解为，考察历史设备的设备环境信息中是否包含待验证设备的设备环境信息，相当于确定待验证设备是否参与过业务系统，或者待验证设备所接入的网络环境是否曾经被用户持其他设备接入过。需要说明的是，各项内容的比对结果可以作为特征向量中的不同分项，也可以将比对结果采用预设的规则进行汇总，共同作为特征向量中的分项。例如，预设的规则可以是，多项内容的比对结果均为符合时，特征向量中分量的取值为 1，而多项内容中任一项的
20 比对结果为不符合时，特征向量中分量的取值为 0。

- 25 [115] 又例如，可以判断待验证设备的设备环境信息与历史上接入次数最多的设备环境信息是否一致，并将判断的结果作为特征向量的一个或多个分量。再例如，可以将待验证设备的设备环境信息与历史设备的设备环境信息的缺失值进行比较，根据比较的结果确定特征向量中的一个或多个分量。具体的比对判断过程，以及根据比对判断的结果

确定特征向量中对应分量的方式，与前述示例类似，此处不再赘述。

[116] 可以理解到，确定待验证设备相对应的特征向量时，采用用户使用待验证设备时的设备环境信息与用户历史上所用过设备的设备环境信息去对比。在很多正常情况下，用户的设备环境信息往往是不变的。如果用户所持设备不变（此时，设备的身份标识 ID 5 也不会变），而网络环境信息（例如，LBS）发生了变化，则有可能仍然是用户本人发出的正常的核身请求，但也仍然存在设备被盗用的风险。而如果用户所持设备变了（此时，设备的身份标识 ID 会发生变化），而网络环境信息均未变化，则很有可能只是用户更换了设备发起核身请求。而如果与用户相对应的设备环境信息（包括设备的标识信息和网络环境信息）均与历史特征信息不符，则允许待验证设备访问业务系统的风险会 10 更大，因而可以采用更加严格、匹配风险等级更高的核身策略对用户进行核身。

[117] S1033：将特征向量输入设备验证模型，利用设备验证模型确定待验证设备的可信程度；其中，设备验证模型用于基于设备的设备环境信息，确定发出核身请求的设备的可信度标签，以及该核身请求被预测为可信请求的概率。

[118] 在根据待验证设备的设备环境信息生成对应的特征向量后，可进一步利用设备 15 验证模型确定待验证设备的可信程度。可以理解到，设备的可信程度，可以具体体现为设备验证模型输出的设备的可信标签、以及该设备发出的核身请求被预测为可信请求的概率。需要说明的是，在根据待验证设备的可信程度确定核身策略时，可以具体体现为：根据设备的可信标签、以及该设备发出的核身请求被预测为可信请求的概率，确定可信 20 标签和/或被预测为可信请求的概率所落入的可信程度区间，进而将该可信程度区间所对应的核身策略确定为对持有该待验证设备申请核身的用户的核身策略。

[119] 可选的，可以采用机器学习算法离线搭建和训练设备验证模型。具体的，在将特征向量输入设备验证模型，利用设备验证模型确定待验证设备的可信程度之前，可以先执行以下步骤，完成设备验证模型的训练和验证，参见图 3 所示：

[120] S201：获取历史特征信息，历史特征信息与历史设备相对应。

25 [121] 能够理解到，执行步骤 S201 获取到的历史特征信息，可以是与历史设备相对应的离线历史特征信息，参见图 4 所示。其中，历史设备，既可以是曾经登录业务系统的历史登录设备（历史登录设备产生历史特征信息中的历史登录信息），也可以是曾经进行过核身（包括核身通过与核身不通过）、在业务系统中进行过业务处理的历史核身设备（历史核身设备产生历史特征信息中的历史核身信息）。

[122] 需要说明的是, 在进行设备验证模型训练时, 可以根据历史特征信息的不同内涵, 训练适用于不同用户的设备验证模型。对于首次使用业务系统的用户, 由于用户仅进行过登录系统的操作, 历史特征信息中仅能够包含历史登录设备的设备环境信息(可以简称为历史登录信息), 而并不包含历史核身设备的设备环境信息。因此, 适用于这类用户的设备验证模型, 其输入参数仅参考历史特征信息中的历史登录信息确定。而对于曾经进行过核身的用户, 由于用户进行过核身操作, 甚至使用业务系统进行过业务操作, 历史特征信息中既可以包含历史登录信息, 也会包含历史核身信息。因此, 适用于这类用户的设备验证模型, 其输入参数可以同时参考历史登录信息和历史核身信息确定。

5 [123] S203: 根据历史特征信息所对应的时间区间, 确定第一历史特征信息构成的训练集和第二历史特征信息构成的验证集。

[124] 可选的, 在根据历史特征信息所对应的时间区间划分训练集和验证集时, 将生成时间较早的第一历史特征信息分入训练集, 将生成时间较晚的第二历史特征信息分入验证集。由于验证集中的历史特征信息生成时间较晚, 将更贴近用户的当前应用需求, 因此, 将生成时间较晚的历史特征信息分入验证集, 能够更加准确的判断设备验证模型输出的验证结果的是否正确。例如, 可以提取最近 50 天的核身/登录时间所产生的历史特征信息用于训练设备验证模型, 将其中最近 10 天产生的历史特征信息作为第二历史特征信息, 构成验证集, 剩余的近期 40 天产生的历史特征信息作为第一历史特征信息, 构成训练集, 参见图 4 所示。

15 [125] 可选的, 历史特征信息中包含用户进行登录/核身所用设备的 ID、Wi-Fi、LBS 及 IP 等网络环境信息。历史特征信息中还可以体现用户发起的核身请求所对应的应用场景, 例如, 登录业务系统, 线上支付的二次验证、修改支付密码等。历史特征信息中还可以体现根据设备的可信程度确定的核身策略中所对应的核身信息类型, 例如, 刷脸核身, 指纹核身, 短信验证码核身, 等等。历史特征信息中还可进一步反映对应登录/核身事件的核身结果。

25 [126] S205: 采用第一历史特征信息对设备验证模型进行训练。

[127] 可选的, 搭建的设备验证模型中, 可以包括逻辑回归 LR (Logistic Regression) 模型和极限梯度提升 XGBoost (eXtreme Gradient Boosting) 模型。在采用第一历史特征信息对设备验证模型进行训练时, 整体上包括了一阶段 LR 模型的训练和二阶段 XGboost 模型的训练这两部分, XGboost 模型的输入包含了 LR 模型的输出, 整个设备验证模型的训练过程是串联式进行的, 参见图 4 所示。

30

[128] 更具体的, 对设备验证模型的训练, 可以具体包括以下步骤, 参见图 4 和图 5 所示:

[129] S2051: 根据第一历史特征信息, 确定第一历史特征向量、第二历史特征向量, 以及与第一历史特征信息相对应的历史设备的第一可信度标签。

5 [130] 可选的, 历史特征信息所对应设备的可信度标签, 可具体化为黑样本和白样本两种。对可信度标签为黑样本还是白样本的确定, 可以根据历史案件的情况、历史核身请求通过与否的情况、在核身通过的情况下对业务系统的非法操作情况等进行。

[131] 例如, 根据历史案件的情况, 若某设备涉及到多起案件, 或者涉及到金额较大的案件, 则可将该设备的可信度标签标记为黑样本。与该设备相对应的历史特征信息所
10 对应的核身请求, 也都可标记为不可信请求。这里所说的案件, 可以是违法用户利用该设备攻破合法用户的账户, 非法获取了合法用户账户中的金钱, 等。

[132] 又例如, 若历史上某设备发出的历史核身请求多次未通过, 则表示该设备很可能被非法使用, 则可将该设备的可信度标签标记为黑样本, 与该设备相对应的历史特征信息所对应的核身请求, 也都可标记为不可信请求。

15 [133] 再例如, 若存在核身已通过, 而用户利用某设备对业务系统进行了非法业务操作, 则可将该设备的可信度标签标记为黑样本。与该设备相对应的历史特征信息所对应的核身请求, 也都可标记为不可信请求。

[134] 可以理解到, 对设备的可信度标签的定义和确定方式, 并不局限于以上示例。根据具体的应用需求, 可以对可信度标签赋予不同的含义, 亦有多种不同的确定方式,
20 本申请实施例对此不做限定。

[135] 可选的, 在根据历史特征信息, 确定特征向量时, 在设备验证模型的训练阶段, 可以采用离线历史特征信息, 进行离线统计, 得到特征向量。具体的, 可以根据不同的时间窗口、不同的用户主体(可通过用户标识进行区分)分别进行特征向量的累计计算。可选的, 可以按照时间窗口、设备标识、用户标识等不同维度及其组合对历史行为进行
25 次数累计, 根据累计值确定特征向量中的对应分量。也可以对各历史特征信息, 判断当前设备环境信息与历史设备的环境信息一致与否, 当前设备环境信息与历史登录成功最多和/或核身通过次数最多的设备环境信息一致与否等, 根据判断的结果确定特征向量中的对应分量。还可以根据当前设备环境信息与历史环境信息的缺失值比较结果, 设备环境信息在最近预设天数中的变化情况等多方面因素, 确定特征向量中的对应分量。

[136] 可选的,在根据历史特征信息,确定特征向量时,在设备验证模型的使用阶段,可以采用实时设备环境信息,进行在线实时统计,得到特征向量,以便实时监控设备验证模型的输出,对设备验证模型进行评估,当设备验证模型的评估数据不满足预设条件时,可以对设备验证模型进行更新,也就是将更新后的历史特征信息作为训练集和验证集,重新训练设备验证模型。

[137] 需要说明的是,特征向量中分量的数量,可以根据核身系统和业务系统的实际需求而定。可选的,输入逻辑回归 LR 模型的第一历史特征向量中分量的数量,可以比输入极限梯度提升 XGBoost 模型的第二历史特征向量中分量的数量要多。例如,从历史特征信息中提取出的第一历史特征向量中,可以有 300 个左右分量,输入逻辑回归 LR 模型;而从历史特征信息中提取出的第二历史特征向量,可以考虑特征向量中各分量的权重高低,还可以结合历史经验确定更能够区分黑白样本的特征,从而可以从 300 多个分量中挑选出 30 多个,作为第二历史特征向量中的分量。

[138] 还需要说明的是,对于首次使用业务系统的用户所适用的设备验证模型,其训练过程中所采用的历史特征信息中也仅包含历史登录设备的设备环境信息(可以简称为历史登录信息),而并不包含历史核身设备的设备环境信息(可以简称为历史核身信息)。相对应的,输入该模型的特征向量中,也仅包括反映历史登录信息的分量,而不会包括反映历史核身信息的分量。

[139] 而对于曾经进行过核身的用户所适用的设备验证模型,其训练过程中所采用的历史特征信息中将同时包括历史登录信息和历史核身信息。因此,输入该模型的特征向量中,将同时包括反映历史登录信息和历史核身信息的分量。

[140] S2053: 将第一历史特征向量输入逻辑回归 LR 模型;根据第一可信度标签与逻辑回归 LR 模型输出的第一目标标签,调整逻辑回归 LR 模型的模型参数,直至逻辑回归 LR 模型的输出满足预设条件。

[141] 可选的,在对逻辑回归 LR 模型进行训练的过程中,可以对模型的正则项、正则系数、最大迭代次数等模型参数中的一项或多项进行调整,直至逻辑回归 LR 模型的输出满足预设条件。

[142] 可以理解到,将第一历史特征向量输入逻辑回归 LR 模型,由逻辑回归 LR 模型输出第一目标标签,其中,第一目标标签为逻辑回归 LR 模型预测的、由与生成第一历史特征向量的历史特征信息所对应设备的可信度标签。根据经过标定的第一可信度标签,

就可以判断逻辑回归 LR 模型输出的第一目标标签是否正确、是否准确,进而根据判断结果调整逻辑回归 LR 模型的模型参数,使得逻辑回归 LR 模型能够足够正确的输出目标标签。并且,通过调整正则项、最大迭代次数、正则系数等模型参数,得到最优的逻辑回归 LR 模型。

- 5 [143] S2055: 根据训练后的逻辑回归 LR 模型的输出,计算第一历史特征信息所对应设备发出的核身请求被预测为可信请求的第一概率。

[144] 在完成对逻辑回归 LR 模型的训练后,可以根据逻辑回归 LR 模型的输出,计算出核身请求预测为白样本的概率(即第一概率),作为极限梯度提升 XGBoost 模型的输入参数之一,进而进行对极限梯度提升 XGBoost 模型的训练,参见图 4 所示。

- 10 [145] S2057: 将第一概率以及第二历史特征向量输入极限梯度提升 XGBoost 模型;利用极限梯度提升 XGBoost 模型的输出与第一可信度标签,调整极限梯度提升 XGBoost 模型的模型参数,直至极限梯度提升 XGBoost 模型的输出满足预设条件;其中,极限梯度提升 XGBoost 模型的输出,包括第一历史特征信息所对应历史设备的可信度标签,以及该历史设备发出的核身请求被预测为可信请求的概率。

- 15 [146] 可选的,对极限梯度提升 XGBoost 模型的参数调整,主要涉及到对树的颗数、步长等参数的调整。

- [147] 可以理解到,将根据逻辑回归 LR 模型的输出计算得到的第一概率作为极限梯度提升 XGBoost 模型的入参之一,再将第二历史特征向量作为极限梯度提升 XGBoost 模型的其余入参,进而得到极限梯度提升 XGBoost 模型的输出,即第一历史特征信息所对应历史设备的可信度标签,以及该历史设备发出的核身请求被预测为可信请求的概率。
- 20 通过将极限梯度提升 XGBoost 模型输出的可信度标签与经过标定的第一可信度标签进行对比,就可以判断极限梯度提升 XGBoost 模型输出的可信度标签是否正确、是否准确,进而可以根据判断结果调整极限梯度提升 XGBoost 模型的模型参数,使得极限梯度提升 XGBoost 模型能够足够正确的输出可信度标签。并且,通过调整树的颗数、步长等参数,
- 25 得到最优的极限梯度提升 XGBoost 模型。

[148] S207: 采用第二历史特征信息对设备验证模型进行验证。

[149] 可以理解到,对设备验证模型的验证,可以在完成对设备验证模型的训练后即刻进行,以判断设备验证模型的输出准确性能否满足应用需求。需要说明的是,可以在设备验证模型运行使用一段时间后,定期或不定期对设备验证模型的输出效果进行验

证,以便在设备验证模型的输出不够准确,无法满足应用需求时,利用更新的历史特征信息对设备验证模型进行重新训练,以满足应用需求。

[150] 可选的,在对设备验证模型进行验证时,可以采用以下方式进行,参见图 6 所示:

5 [151] S2071: 根据第二历史特征信息,确定第三历史特征向量、第四历史特征向量,以及与第二历史特征信息相对应的历史设备的第二可信度标签;

[152] S2073: 将第三历史特征向量输入训练后的逻辑回归 LR 模型;根据训练后的逻辑回归 LR 模型的输出,计算第二历史特征信息所对应设备发出的核身请求被预测为可信请求的第二概率;

10 [153] S2075: 将第二概率以及第四历史特征向量输入训练后的极限梯度提升 XGBoost 模型,利用训练后的极限梯度提升 XGBoost 模型得到设备验证模型的输出;设备验证模型的输出,包括第二历史特征信息所对应历史设备的可信度标签,以及该历史设备发出的核身请求被预测为可信请求的第三概率;

[154] S2077: 根据设备验证模型的输出和第二可信度标签,利用二分类评估方法,得到设备验证模型的评估数据;

[155] S2079: 根据评估数据调整逻辑回归 LR 模型和/或极限梯度提升 XGBoost 模型的模型参数,直至设备验证模型的评估数据满足预设条件。

[156] 能够理解到,将验证集中的第二历史特征信息作为设备验证模型的输入,经过设备验证模型中串行的逻辑回归 LR 模型和极限梯度提升 XGBoost 模型后,输出第二历史特征信息所对应历史设备的可信度标签,以及该历史设备发出的核身请求被预测为可信请求的第三概率。进而可结合经过标定的第二可信度标签,利用二分类评估方法,得到设备验证模型的评估数据。

[157] 可选的,设备验证模型的评估数据可以包括 F1 分数 (F1-score) 和曲线下面积 AUC (全称 Area Under the Curve) 值中至少一项。具体的, F1 分数是对模型准确率和召回率进行综合考量的一个参数指标。F1 分数越高,说明分类模型 (此处具体为设备验证模型) 越稳健。曲线下面积 AUC 值是指随机给定一个正样本和一个负样本,分类模型输出该正样本为正的那个概率值比分类器输出该负样本为正的那个概率值要大的可能性。F1 分数和曲线下面积 AUC 值是针对模型训练好坏的判断。通过模型的评估数据对模型预测可信程度的效果进行考察,并不断调整逻辑回归 LR 模型和/或极限梯度提

升 XGBoost 模型的模型参数,从而得到最优的逻辑回归 LR 模型和极限梯度提升 XGBoost 模型组合模型。

[158] 需要说明的是,在实际的应用中,设备验证模型的评估数据除考虑模型本身的数学参数之外,还可以结合模型的实际应用场景,考虑对于黑样本的误判率和白样本的准确率。这是因为,若将黑样本判断为白样本,会使得非法用户核身通过,对业务系统的安全性造成威胁;而若将白样本判断为黑样本,虽然对合法用户加严核身并不会影响业务系统的安全,但是可能会影响用户体验。因此,也需要考虑设备验证模型的判断准确率和误判率。当准确率下降,误判率上升时,就可以触发进行模型的更新,也就是利用更新的历史特征信息对设备验证模型进行重新训练。

10 [159] 采用本申请实施例,在接收到来自待验证设备的核身请求后并未直接进行核身,而是根据历史设备的设备环境信息以及待验证设备的设备环境信息,确定待验证设备的可信程度,并进而根据可信程度确定对用户进行核身的核身策略。采用本申请实施例的方法,可以在用户无感知的情况下,根据用户所持设备的可信程度,为用户选择适用于当前所持设备的核身策略。因此,本申请实施例有利于提高核身的安全性和可靠性,并
15 能够满足用户的使用需求,提升用户体验。

[160] 本申请实施例还提供了一种核身装置,应用于核身系统中。参见图 7 所示,该核身装置可包括:

[161] 请求接收模块 101,接收来自待验证设备的核身请求,核身请求中包括待验证设备的设备环境信息,用于请求对待验证设备所对应的用户进行核身;

20 [162] 可信程度确定模块 103,根据历史特征信息以及设备环境信息,确定待验证设备的可信程度;历史特征信息包括历史设备的设备环境信息;

[163] 核身策略确定模块 105,根据待验证设备的可信程度,确定对用户进行核身的核身策略,以便按照核身策略进行核身。

[164] 能够理解,图 7 示例的核身装置与前述实施例中提供的核身系统执行的核身方法
25 相对应,能够实现前述实施例中的核身方法,此处不再赘述。

[165] 图 8 是本申请的一个实施例电子设备的结构示意图。请参考图 8,在硬件层面,该电子设备包括处理器,可选地还包括内部总线、网络接口、存储器。其中,存储器可能包含内存,例如高速随机存取存储器(Random-Access Memory, RAM),也可能还包括非易失性存储器(non-volatile memory),例如至少 1 个磁盘存储器等。当然,该电子

设备还可能包括其他业务所需要的硬件。

[166] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA(Industry Standard Architecture, 工业标准体系结构)总线、PCI(Peripheral Component Interconnect, 外设部件互连标准)总线或 EISA(Extended Industry Standard Architecture, 扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图8中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[167] 存储器,用于存放程序。具体地,程序可以包括程序代码,所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器,并向处理器提供指令和数据。

[168] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,在逻辑层面上形成核身装置。处理器,执行存储器所存放的程序,并具体用于执行以下操作:

[169] 接收来自待验证设备的核身请求,核身请求中包括待验证设备的设备环境信息,用于请求对待验证设备所对应的用户进行核身;

[170] 根据历史特征信息以及设备环境信息,确定待验证设备的可信程度;历史特征信息包括历史设备的设备环境信息;

[171] 根据待验证设备的可信程度,确定对用户进行核身的核身策略,以便按照核身策略进行核身。

[172] 上述如本申请图1所示实施例揭示的核身装置执行的方法可以应用于处理器中,或者由处理器实现。处理器可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit, CPU)、网络处理器(Network Processor, NP)等;还可以是数字信号处理器(Digital Signal Processor, DSP)、专用集成电路(Application Specific Integrated Circuit, ASIC)、现场可编程门阵列(Field-Programmable Gate Array, FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器 etc 本领域成熟的存储介质中。该存储介质位于存储器,处理器读取存储器中的信息,结

合其硬件完成上述方法的步骤。

[173] 该电子设备还可执行图 1 中核身装置执行的方法，并实现核身装置在图 1 所示实施例的功能，本申请实施例在此不再赘述。

5 [174] 本申请实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的电子设备执行时，能够使该电子设备执行图 1 所示实施例中核身装置执行的方法，并具体用于执行：

[175] 接收来自待验证设备的核身请求，核身请求中包括待验证设备的设备环境信息，用于请求对待验证设备所对应的用户进行核身；

10 [176] 根据历史特征信息以及设备环境信息，确定待验证设备的可信程度；历史特征信息包括历史设备的设备环境信息；

[177] 根据待验证设备的可信程度，确定对用户进行核身的核身策略，以便按照核身策略进行核身。

15 [178] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

20 [179] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

25

[180] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[181] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

- 5 [182] 在一个典型的配置中,计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[183] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器 (RAM) 和/或非易失性内存等形式,如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

- 10 [184] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体 (transitory media),如调制的数据信号和载波。
- 15

- [185] 还需要说明的是,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、商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、商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、商品或者设备中还存在另外的相同要素。
- 20

- [186] 本领域技术人员应明白,本申请的实施例可提供为方法、系统或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。
- 25

[187] 以上所述仅为本申请的实施例而已,并不用于限制本申请。对于本领域技术人

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理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权利要求范围之内。

权利要求书

1、一种核身方法，包括：

接收来自待验证设备的核身请求，所述核身请求中包括所述待验证设备的设备环境信息，用于请求对待验证设备所对应的用户进行核身；

- 5 根据历史特征信息以及所述设备环境信息，确定所述待验证设备的可信程度，所述历史特征信息包括历史设备的设备环境信息；

根据所述待验证设备的可信程度，确定对用户进行核身的核身策略，以便按照所述核身策略进行核身。

- 2、根据权利要求 1 所述方法，根据历史特征信息以及所述设备环境信息，确定所述待验证设备的可信程度，包括：

当所述设备环境信息中所包含的信息类型与预设信息类型相匹配时，根据所述设备环境信息确定与所述待验证设备相对应的特征向量；

- 15 将所述特征向量输入设备验证模型，利用所述设备验证模型确定所述待验证设备的可信程度；其中，所述设备验证模型用于基于设备的设备环境信息，确定发出核身请求的设备的可信度标签，以及该核身请求被预测为可信请求的概率。

3、根据权利要求 2 所述方法，在将所述特征向量输入设备验证模型，利用所述设备验证模型确定所述待验证设备的可信程度之前，所述方法还包括：

获取历史特征信息，所述历史特征信息与历史设备相对应；

- 20 根据历史特征信息所对应的时间区间，确定第一历史特征信息构成的训练集和第二历史特征信息构成的验证集；

采用第一历史特征信息对所述设备验证模型进行训练，采用第二历史特征信息对所述设备验证模型进行验证。

4、根据权利要求 3 所述方法，根据历史特征信息所对应的时间区间，确定第一历史特征信息构成的训练集和第二历史特征信息构成的验证集，包括：

- 25 根据历史特征信息所对应的时间区间，将生成时间较早的第一历史特征信息分入所述训练集，将生成时间较晚的第二历史特征信息分入所述验证集。

5、根据权利要求 3 所述方法，所述设备验证模型包括逻辑回归 LR 模型和极限梯度提升 XGBoost 模型；则采用第一历史特征信息对所述设备验证模型进行训练，包括：

- 30 根据第一历史特征信息，确定第一历史特征向量、第二历史特征向量，以及与所述第一历史特征信息相对应的历史设备的第一可信度标签；

将第一历史特征向量输入逻辑回归 LR 模型；根据所述第一可信度标签与所述逻辑

回归 LR 模型输出的第一目标标签, 调整所述逻辑回归 LR 模型的模型参数, 直至所述逻辑回归 LR 模型的输出满足预设条件;

根据训练后的所述逻辑回归 LR 模型的输出, 计算第一历史特征信息所对应设备发出的核身请求被预测为可信请求的第一概率;

- 5 将第一概率以及第二历史特征向量输入极限梯度提升 XGBoost 模型; 利用所述极限梯度提升 XGBoost 模型的输出与所述第一可信度标签, 调整所述极限梯度提升 XGBoost 模型的模型参数, 直至所述极限梯度提升 XGBoost 模型的输出满足预设条件; 其中, 所述极限梯度提升 XGBoost 模型的输出, 包括第一历史特征信息所对应历史设备的可信度标签, 以及该历史设备发出的核身请求被预测为可信请求的概率。

- 10 6、根据权利要求 5 所述方法, 采用第二历史特征信息对所述设备验证模型进行验证, 包括:

根据第二历史特征信息, 确定第三历史特征向量、第四历史特征向量, 以及与所述第二历史特征信息相对应的历史设备的第二可信度标签;

- 15 将第三历史特征向量输入训练后的所述逻辑回归 LR 模型; 根据训练后的所述逻辑回归 LR 模型的输出, 计算第二历史特征信息所对应设备发出的核身请求被预测为可信请求的第二概率;

- 20 将第二概率以及第四历史特征向量输入训练后的所述极限梯度提升 XGBoost 模型, 利用训练后的所述极限梯度提升 XGBoost 模型得到所述设备验证模型的输出; 所述设备验证模型的输出, 包括第二历史特征信息所对应历史设备的可信度标签, 以及该历史设备发出的核身请求被预测为可信请求的第三概率;

根据所述设备验证模型的输出和所述第二可信度标签, 利用二分类评估方法, 得到所述设备验证模型的评估数据;

根据所述评估数据调整所述逻辑回归 LR 模型和/或所述极限梯度提升 XGBoost 模型的模型参数, 直至所述设备验证模型的评估数据满足预设条件。

- 25 7、根据权利要求 6 所述方法, 所述设备验证模型的评估数据, 包括 F1 分数和曲线下面积 AUC 值中至少一项。

8、根据权利要求 5~7 之任一所述方法, 所述逻辑回归 LR 模型的模型参数, 包括正则项、正则系数、最大迭代次数中至少一项。

- 30 9、根据权利要求 5~7 之任一所述方法, 第一历史特征向量中分量的数量大于第二历史特征向量中分量的数量。

10、根据权利要求 1~7 之任一所述方法, 所述历史设备, 包括历史登录设备和历史

核身设备中至少一项。

11、根据权利要求 1~7 之任一所述方法,根据历史特征信息以及所述设备环境信息,确定所述待验证设备的可信程度,包括:

5 当所述设备环境信息中所包含的信息类型与预设信息类型不匹配时,确定所述待验证设备不可信。

12、根据权利要求 11 所述方法,所述预设信息类型,包括设备的身份标识 ID,以及设备所对应的无线连接 WIFI、基于位置服务 LBS 和互联网协议 IP 地址中至少一个。

13、根据权利要求 1~7 之任一所述方法,根据所述待验证设备的可信程度,确定对用户进行核身的核身策略,包括:

10 根据所述待验证设备的可信程度,以及核身策略与可信程度区间的对应关系,确定对用户进行核身的核身策略;

其中,所述核身策略所匹配的风险等级与用户所持设备的可信程度负相关。

14、根据权利要求 13 所述方法,所述核身策略中包括核身信息类型、核身信息数量和核身阈值范围中至少一项;

15 则所述核身策略所匹配的风险等级与用户所持设备的可信程度负相关,包括以下至少一项:

当所述核身策略中包括所述核身信息类型时,所述核身策略中核身信息类型的安全等级与用户所持设备的可信程度负相关;

20 当所述核身策略中包括所述核身信息数量时,所述核身策略中的核身信息数量与用户所持设备的可信程度负相关;

当所述核身策略中包括所述核身阈值范围时,所述核身策略中的核身阈值范围与用户所持设备的可信程度正相关。

15、根据权利要求 1 所述方法,按照所述核身策略进行核身,包括:

25 按照所述核身策略确定核身流程、核身所需信息、以及核身所需信息的核身阈值范围;

按照所述核身流程,提示所述待验证设备上报所述核身所需信息;

当接收到所述待验证设备上报的所述核身所需信息时,根据核身所需信息的核身阈值范围进行核身。

16、一种核身装置,包括:

30 请求接收模块,接收来自待验证设备的核身请求,所述核身请求中包括所述待验证设备的设备环境信息,用于请求对待验证设备所对应的用户进行核身;

可信程度确定模块,根据历史特征信息以及所述设备环境信息,确定所述待验证设备的可信程度;所述历史特征信息包括历史设备的设备环境信息;

核身策略确定模块,根据所述待验证设备的可信程度,确定对用户进行核身的核身策略,以便按照所述核身策略进行核身。

5 17、一种电子设备,包括:

处理器;以及

被安排成存储计算机可执行指令的存储器,所述可执行指令在被执行时使所述处理器执行以下操作:

10 接收来自待验证设备的核身请求,所述核身请求中包括所述待验证设备的设备环境信息,用于请求对待验证设备所对应的用户进行核身;

根据历史特征信息以及所述设备环境信息,确定所述待验证设备的可信程度;所述历史特征信息包括历史设备的设备环境信息;

根据所述待验证设备的可信程度,确定对用户进行核身的核身策略,以便按照所述核身策略进行核身。

15 18、一种计算机可读存储介质,所述计算机可读存储介质存储一个或多个程序,所述一个或多个程序当被包括多个应用程序的电子设备执行时,使得所述电子设备执行以下操作:

接收来自待验证设备的核身请求,所述核身请求中包括所述待验证设备的设备环境信息,用于请求对待验证设备所对应的用户进行核身;

20 根据历史特征信息以及所述设备环境信息,确定所述待验证设备的可信程度;所述历史特征信息包括历史设备的设备环境信息;

根据所述待验证设备的可信程度,确定对用户进行核身的核身策略,以便按照所述核身策略进行核身。