(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 7 月 21 日 (21.07.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/151815 A1

(51) 国际专利分类号:
G06F 21/57 (2013.01)

(21) 国际申请号: PCT/CN2021/128867

(22) 国际申请日: 2021 年 11 月 5 日 (05.11.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110053180.X 2021年1月15日 (15.01.2021) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 于文海 (YU, Wenhai); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。祖立军 (ZU, Lijun); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。郭伟 (GUO, Wei); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。乐旭 (LE, Xu); 中国上海市浦东新区含笑路36号银联大厦, Shanghai 200135 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告 (条约第21条(3))。

(54) **Title:** METHOD AND APPARATUS FOR DETERMINING SECURITY STATE OF TERMINAL DEVICE

(54) **发明名称**: 一种终端设备的安全状态判断方法及装置

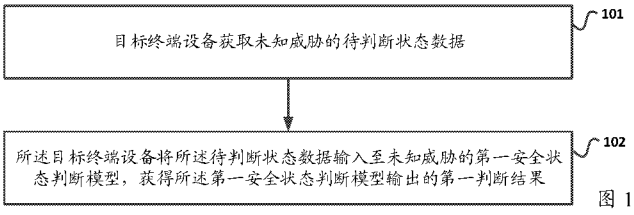

图 1

101 A target terminal device acquires state data to be determined of an unknown threat

102 The target terminal device inputs the state data into a first security state determination model for unknown threats, and obtains a first determination result outputted by the first security state determination model

(57) **Abstract:** A method and apparatus for determining the security state of a terminal device. The method comprises: a target terminal device acquires state data to be determined of an unknown threat (101); the target terminal device inputs the state data into a first security state determination model for unknown threats, and obtains a first determination result outputted by the first security state determination model (102), wherein the first security state determination model is obtained by training when a plurality of terminal devices and servers perform machine learning on the basis of labeling data of unknown threats of the plurality of terminal devices.

(57) **摘要**: 一种终端设备的安全状态判断方法及装置，其中方法为：目标终端设备获取未知威胁的待判断状态数据(101)；所述目标终端设备将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，获得所述第一安全状态判断模型输出的第一判断结果(102)；所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的。

WO 2022/151815 A1

一种终端设备的安全状态判断方法及装置

相关申请的交叉引用

本申请要求在2021年01月15日提交中国专利局、申请号为202110053180.X、申请名称为“一种终端设备的安全状态判断方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及数据安全技术领域，尤其涉及一种终端设备的安全状态判断方法及装置。

背景技术

终端设备涉及许多应用场景。举例来说，中国移动支付的比例逐渐增加，越来越多的终端设备参与到移动支付中。终端设备的状态数据能够反应出当前终端设备的安全状态，所以可通过采集终端设备的状态数据的方法来判定终端设备的安全状态。

目前的方案中，终端设备的已知威胁可以按照相应的安全判断模型检验是否安全，如针对篡改文件的攻击手段，可以通过文件变更的安全判断模型判断终端设备是否安全。然而，对于不确定的攻击手段的未知威胁检测较为局限。目前终端设备的未知威胁检测，是通过大数据统计判断来实现的。目前是先将终端设备的状态数据采集，然后统一传递给服务端，这样以来服务端采集大量的终端设备的状态数据后，才能形成大数据统计，进而进行安全状态判断。然而，服务端获取到大量终端设备的状态数据后，难以保证这些终端设备的状态数据不被滥用。因此，如何在保证终端设备的状态数据隐私安全的情况下，对终端设备的安全状态进行判断便成为了难题。

发明内容

本发明提供一种终端设备的安全状态判断方法及装置，解决了现有技术中如何在保证终端设备的状态数据隐私安全的情况下，对终端设备的安全状态进行判断的问题。

第一方面，本发明提供一种终端设备的安全状态判断方法，包括:

目标终端设备获取未知威胁的待判断状态数据；所述目标终端设备为多个终端设备的任一终端设备;

所述目标终端设备将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，

获得所述第一安全状态判断模型输出的第一判断结果；

所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的；其中，在任一轮机器学习训练中，所述多个终端设备中任一终端设备用于将该轮机器学习训练的本地训练参数发送至服务端，所述服务端用于将该轮机器学习训练中所述多个终端设备的本地训练参数融合，获得融合训练参数，并将所述融合训练参数发送至所述多个终端设备，使得所述多个终端设备基于所述融合训练参数更新或作为所述第一安全状态判断模型的模型参数。

上述方式下，所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的，且在任一轮机器学习训练中，任一终端设备只将该轮机器学习训练的本地训练参数发送至服务端，并由服务端将该轮机器学习训练中所述多个终端设备的本地训练参数融合，获得融合训练参数，从而对使得所述多个终端设备基于所述融合训练参数更新，在该过程中并不需要传递所述多个终端设备的状态数据，所以也不会泄露状态数据的隐私，而每一轮的融合训练参数又都考虑了每个终端设备的本地训练参数，所以也保证第一安全状态判断模型的精确性，因此，目标终端设备获取未知威胁的待判断状态数据后，将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，便可以直接获得所述第一安全状态判断模型输出的第一判断结果，也不需要将待判断状态数据上传至服务端，从而在保证终端设备的状态数据隐私安全的情况下，实现了对终端设备的安全状态的判断。

可选的，所述目标终端设备按照以下方式获得所述目标终端设备的未知威胁的标签化数据：

所述目标终端设备获取所述目标终端设备的未知威胁的无标签数据；

所述目标终端设备基于所述无标签数据获取所述标签化数据。

上述方法中，获取所述目标终端设备的未知威胁的无标签数据后，再基于所述无标签数据获取所述标签化数据，到转换为无标签数据，保留了未知威胁的无标签数据的特性。

可选的，所述目标终端设备基于所述无标签数据获取所述标签化数据，包括：

所述目标终端设备将所述无标签数据输入至已知威胁的至少一个第二安全状态判断模型，获得所述至少一个第二安全状态判断模型输出的至少一个第二判断结果；

所述目标终端设备根据所述至少一个第二判断结果，确定所述无标签数据的标签值，从而将所述无标签数据转换为所述标签化数据。

上述方法中，通过所述至少一个第二安全状态判断模型得到至少一个第二判断结果，从而可以发现相应已知威胁的特性，更准确地得到标签化数据。

可选的，所述目标终端设备基于所述无标签数据获取所述标签化数据，包括：

所述目标终端设备基于所述无标签数据，按照预设聚类算法，获得所述无标签数据的第一簇聚类数据和第二簇聚类数据；所述第一簇聚类数据的数据量小于所述第二簇聚类数据的数据量；

所述目标终端设备将所述第一簇聚类数据的标签值设置为第一标签值，将所述第二簇聚类数据的标签值设置为第二标签值，从而将所述无标签数据转换为所述标签化数据；所述第一标签值表征数据为不安全数据，所述第二标签值表征数据为安全数据。

上述方式下，所述目标终端设备基于所述无标签数据，按照预设聚类算法，获得所述无标签数据的第一簇聚类数据和第二簇聚类数据，从而根据簇聚类数据的数据量自适应地区分出安全数据和不安全数据，并打上标签，提供了一种自动化设置标签的方法。

可选的，所述目标终端设备按照以下方式获得所述第一安全状态判断模型：

在任一轮机器学习训练中，所述目标终端设备基于所述未知威胁的标签化数据和安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数；

所述目标终端设备将所述第二本地训练参数发送至所述服务端；

所述目标终端设备获得来自所述服务端的融合训练参数；所述融合训练参数是所述服务端基于所述多个终端设备发送的本地训练参数得到的；

若所述安全状态训练模型不满足预设收敛条件，则所述目标终端设备将所述融合训练参数重新作为所述第一本地训练参数，返回所述目标终端设备基于所述未知威胁的标签化数据和所述安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数的步骤；

若所述安全状态训练模型满足所述预设收敛条件，则所述目标终端设备将所述融合训练参数作为所述安全状态训练模型的模型参数，将此时的所述安全状态训练模型作为所述第一安全状态判断模型。

可选的，所述获得所述第一安全状态判断模型输出的第一判断结果之后，还包括：

所述目标终端设备将所述第一判断结果发送至所述服务端。

可选的，所述多个终端设备未知威胁的标签化数据均具有相同的数据特征维度。

第二方面，本发明提供一种终端设备的安全状态判断装置，包括：

获取模块，用于获取目标终端设备的未知威胁的待判断状态数据；所述目标终端设备为多个终端设备的任一终端设备；

处理模块，用于将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，获得所述第一安全状态判断模型输出的第一判断结果；

所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的；其中，在任一轮机器学习训练中，所述多个终端设备中任一终端设备用于将该轮机器学习训练的本地训练参数发送至服务端，所述服务端用于将该轮机器学习训练中所述多个终端设备的本地训练参数融合，获得融合训练参数，并将所述融合训练参数发送至所述多个终端设备，使得所述多个终端设备基于所述融合训练参数更新或作为所述第一安全状态判断模型的模型参数。

可选的，所述获取模块按照以下方式获得所述目标终端设备的未知威胁的标签化数据：

获取所述目标终端设备的未知威胁的无标签数据；

基于所述无标签数据获取所述标签化数据。

可选的，所述获取模块具体用于：

将所述无标签数据输入至已知威胁的至少一个第二安全状态判断模型，获得所述至少一个第二安全状态判断模型输出的至少一个第二判断结果；

根据所述至少一个第二判断结果，确定所述无标签数据的标签值，从而将所述无标签数据转换为所述标签化数据。

可选的，所述获取模块具体用于：基于所述无标签数据，按照预设聚类算法，获得所述无标签数据的第一簇聚类数据和第二簇聚类数据；所述第一簇聚类数据的数据量小于所述第二簇聚类数据的数据量；

将所述第一簇聚类数据的标签值设置为第一标签值，将所述第二簇聚类数据的标签值设置为第二标签值，从而将所述无标签数据转换为所述标签化数据；所述第一标签值表征数据为不安全数据，所述第二标签值表征数据为安全数据。

可选的，所述获取模块按照以下方式获得所述第一安全状态判断模型：

在任一轮机器学习训练中，基于所述未知威胁的标签化数据和安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数；将所述第二本地训练参数发送至所述服务端；获得来自所述服务端的融合训练参数；所述融合训练参数是所述服务端基于所述多个终端设备发送的本地训练参数得到的；

若所述安全状态训练模型不满足预设收敛条件，则将所述融合训练参数重新作为所述第一本地训练参数，返回基于所述未知威胁的标签化数据和所述安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数的步骤；

若所述安全状态训练模型满足所述预设收敛条件，则将所述融合训练参数作为所述安全状态训练模型的模型参数，将此时的所述安全状态训练模型作为所述第一安全状态判断模型。

可选的，所述获取模块还用于：将所述第一判断结果发送至所述服务端。

可选的，所述多个终端设备未知威胁的标签化数据均具有相同的数据特征维度。

上述第二方面及第二方面各个可选装置的有益效果，可以参考上述第一方面及第一方面各个可选方法的有益效果，这里不再赘述。

第三方面，本发明提供一种计算机设备，包括程序或指令，当所述程序或指令被执行时，用以执行上述第一方面及第一方面各个可选的方法。

第四方面，本发明提供一种存储介质，包括程序或指令，当所述程序或指令被执行时，用以执行上述第一方面及第一方面各个可选的方法。

本发明的这些方面或其他方面在以下实施例的描述中会更加简明易懂。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例提供的一种终端设备的安全状态判断方法的步骤流程示意图；

图 2 为本发明实施例提供的一种终端设备的安全状态判断方法中终端设备的架构示意图；

图 3 为本发明实施例提供的一种终端设备的安全状态判断方法中所述第一安全状态判断模型的获取示意图；

图 4 为本发明实施例提供的一种终端设备的安全状态判断方法中云端服务的架构示意图；

图 5 为本发明实施例提供的一种终端设备的安全状态判断方法对应的具体流程示意图；

图 6 为本发明实施例提供的一种终端设备的安全状态判断方法中在终端设备的联邦学习的实现示意图；

图 7 为本发明实施例提供的一种终端设备的安全状态判断方法中在服务器端的联邦学习的实现示意图；

图 8 为本发明实施例提供的一种终端设备的安全状态判断方法对应的时序步骤示意图；

图 9 为本发明实施例提供的一种终端设备的安全状态判断装置的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

如图 1 所示，本发明实施例提供一种终端设备的安全状态判断方法。

步骤 101：目标终端设备获取未知威胁的待判断状态数据。

所述目标终端设备为多个终端设备的任一终端设备。

步骤 102：所述目标终端设备将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，获得所述第一安全状态判断模型输出的第一判断结果。

步骤 101~步骤 102 中，举例来说，待判断状态数据可以为 CPU 状态数据、进程状态数据等。

所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的；其中，在任一轮机器学习训练中，所述多个终端设备中任一终端设备用于将该轮机器学习训练的本地训练参数发送至服务端，所述服务端用于将该轮机器学习训练中所述多个终端设备的本地训练参数融合，获得融合训练参数，并将所述融合训练参数发送至所述多个终端设备，使得所述多个终端设备基于所述融合训练参数更新或作为所述第一安全状态判断模型的模型参数。

需要说明的是，特殊地，所述多个终端设备未知威胁的标签化数据均具有相同的数据特征维度。另外，上述机器学习方法不做限定，如可以采用横向联邦学习。

显然，步骤 101~步骤 102 的方法中，为解决隐私数据的使用问题，保证在所述第一安全状态判断模型的训练时，终端设备的隐私数据不会上传云端，仅仅是在终端设备使用。因此，步骤 101~步骤 102 的方法从技术框架上，便保证了隐私数据不会外泄和恶意使用。

另外上述机器学习方法，在解决隐私数据上传问题的同时，也提供了一种终端设备的未知威胁模型迭代的方法，通常而言未知威胁由于采集数据维度较多，并且目的未知难以被捕捉到。那么步骤 101~步骤 102 的方法下，在解决隐私问题的情况下，可以采集更多维度的数据。并且，通过已知威胁的安全状态判断模型的结果对数据进行标签化，可以将模型的训练本地化，从而不断的训练和迭代终端侧的安全状态判断模型。

需要说明的是，传统方案中，未知威胁检测需要大量的辅助数据，因为既然是未知威胁，就需要更多维度的数据去辅助发现和检测。但是随着隐私保护的逐渐重视，大量隐私数据上传云端的进行使用的方式会越来越难以被接受，所以步骤 101~步骤 102 的方法中，

通过上述机器学习方法的引入来解决在终端训练安全状态判断模型的问题，再辅助已知威胁的安全状态判断模型的数据标签化方法，可以使得终端设备安全状态的判断更加的完整。

一种可选实施方式中，所述目标终端设备按照以下方式获得所述目标终端设备的未知威胁的标签化数据：

步骤(1)：所述目标终端设备获取所述目标终端设备的未知威胁的无标签数据。

步骤(2)：所述目标终端设备基于所述无标签数据获取所述标签化数据。

需要说明的是，步骤(2)中可以采用不同方式对所述无标签数据添加标签，从而获取所述标签化数据。

一种可选实施方式中，步骤(2)具体可以为：

所述目标终端设备将所述无标签数据输入至已知威胁的至少一个第二安全状态判断模型，获得所述至少一个第二安全状态判断模型输出的至少一个第二判断结果；

所述目标终端设备根据所述至少一个第二判断结果，确定所述无标签数据的标签值，从而将所述无标签数据转换为所述标签化数据。

举例来说，所述至少一个第二安全状态判断模型为 3 个第二安全状态判断模型，这 3 个第二安全状态判断模型分别用于：检测 A 方面威胁的第二安全状态判断模型，检测 B 方面威胁的第二安全状态判断模型，检测 C 方面威胁的第二安全状态判断模型。

那么对于未知威胁的待判断状态数据，也可能存在 A 方面威胁、B 方面威胁以及 C 方面威胁，所以通过全面的检测，可以定位出未知威胁是否存在相应方面的威胁。

另一种可选实施方式中，步骤(2)具体可以为：

所述目标终端设备基于所述无标签数据，按照预设聚类算法，获得所述无标签数据的第一簇聚类数据和第二簇聚类数据；所述目标终端设备将所述第一簇聚类数据的标签值设置为第一标签值，将所述第二簇聚类数据的标签值设置为第二标签值，从而将所述无标签数据转换为所述标签化数据。

所述第一簇聚类数据的数据量小于所述第二簇聚类数据的数据量；所述第一标签值表征数据为不安全数据，所述第二标签值表征数据为安全数据。

举例来说，所述无标签数据包括 100 万条数据，在聚类后，得到第二簇聚类数据，包括 95 万条数据，以及第一簇聚类数据，包括 4 万条数据，还有 1 万条为孤立的点；那么基于一个原则，较多的数据正常，少数的数据异常，便判断第二簇聚类数据为安全的数据，则标签值设置为第二标签值，以及判断第一簇聚类数据为安全的数据，则标签值设置为第一标签值。

需要说明的是，在步骤 102 之后，还可以执行如下步骤：

所述目标终端设备将所述第一判断结果发送至所述服务端。

需要说明的是，目标终端设备为智能支付设备时，其结构如图 2 所示。

图 2 为终端设备的系统框架图，在终端设备的系统上核心功能主要分为数据采集，模型判定，模型学习，数据上传这四个部分。具体如下：

数据采集：数据采集模块主要负责采集终端设备的数据信息。其中包含已知威胁数据和未知威胁数据。已知威胁数据中包括如 root 检测，hook 框架检测，模拟器环境检测等。未知威胁数据为系统运行时相关数据，这些数据不能明确判定系统的恶意状态，但是当系统遭受攻击时，这些数据会产生变化。未知威胁数据更多是从系统状态变化的角度反映当前终端设备的安全状态。如 CPU 状态数据，内存状态数据，进程状态数据等。

模型判定：模型判定模块主要是利用数据采集模块采集的数据进行安全状态的判定。其中包括已知威胁判定模型（即第二安全判断模型）和未知威胁判定模型（即第一安全判断模型）。而未知威胁判定模型是通过机器学习训练出来的，那么还可以冷启动，如图 2 示出的一个初始模型，这个初始模型是在实验室环境中通过模拟数据模拟出来的。

需要说明的是，以联邦学习为例，上述冷启动的方式如图 3 所示。

图 3 描述的是实验室环境训练初始模型的过程。首先，需要针对实际的安全场景模拟出训练数据，其中包含正常的行为数据和异常行为数据。正常行为数据描述的是在什么状态和数据数值下可以认为终端设备是安全的；相反异常行为数据描述的就是在什么样的终端设备数据数值下终端是不安全的。

进一步地，算法工程师会基于对数据的理解创建一个算法模型，将模拟数据输入到算法模型中，再根据结果调校模型，最终会得到一个符合模拟数据结果的初始未知威胁判定模型。这个模型用于终端设备的冷启动。

模型学习：终端设备中另外一个核心的模块是模型学习模块。这个模块负责联邦学习的终端设备部分。联邦学习很重要的一个环节是模型的迭代，迭代的环节当中终端设备的模型训练为后端的学习提供了模型数据。但若采用联邦学习，具体的机器学习算法必须是有监督的学习算法。所以在模型训练时必须提供数据和对应的标签。

在本发明实施例的方案中，数据模块采集大量数据作为未知威胁的数据输入，这些数据可以分为几个维度，如：环境安全数据（WIFI 地址信息，基站信息，IP 地址信息），硬件安全数据（调试端口使用情况，CPU 使用状态，内存使用状态等），流量安全数据（出口流量数据，进口流量数据）和软件安全数据（系统进程状态，软件业务数据等）。

而标签化的一种方式是通过已知威胁模块的输出进行标签化，已知威胁的输出是一个分值，这种方式相对简单直观，可以直接对未知威胁数据进行训练。

另外还有一种标签化方式需要对未知威胁的持续发现和运营，相对复杂。首先需要对终端设备未知威胁数据先进行无监督聚类，进而可以区分出数据反映出的问题，再通过安全运营对这些问题划分等级或者人工打分。完成等级划分和人工打分之后，再提供给终端设备进行推理和标签化。以上过程因为使用到终端设备隐私数据，所以可以先在实验室环境完成。

上述两种未知威胁的标签化方式，一种属于短期见效，一种需要长期运营不断优化。可以根据实际情况互相结合使用。

数据上传：数据上传模块最主要的作用在于将终端设备训练的未知威胁判定模型上传到云端，另外终端设备也有部分非隐私或者去隐私的数据需要云端帮忙辅助判定。简单来说数据上传模块是终端设备和云端数据交换的通信模块。

一种可选实施方式中，所述目标终端设备按照以下方式获得所述第一安全状态判断模型：

在任一轮机器学习训练中，执行以下步骤：

步骤(a)：所述目标终端设备基于所述未知威胁的标签化数据和安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数。

步骤(b)：所述目标终端设备将所述第二本地训练参数发送至所述服务端。

步骤(c)：所述目标终端设备获得来自所述服务端的融合训练参数。

所述融合训练参数是所述服务端基于所述多个终端设备发送的本地训练参数得到的。

步骤(d)：若所述安全状态训练模型不满足预设收敛条件，则所述目标终端设备将所述融合训练参数重新作为所述第一本地训练参数，返回步骤(a)。

步骤(e)：若所述安全状态训练模型满足所述预设收敛条件，则所述目标终端设备将所述融合训练参数作为所述安全状态训练模型的模型参数，将此时的所述安全状态训练模型作为所述第一安全状态判断模型。

上述过程为终端设备内部的训练学习过程。

另一方面，云端服务的框架图也有配合的功能模块，以联邦学习为例，具体如图 4 所示。

图 4 是云端服务的框架图。包含几个核心功能模块：云端威胁判定模块，联邦学习模块，数据存储模块，对外接口模块。

云端威胁判定模块：由于大量的数据是在终端设备进行判定和训练的，但是依然有少部分的数据终端设备自身是无法完全判定的，比如公网 IP 数据。对于部分设备，设备的移动本身就是一个非常严重的安全问题，如智能自动收货柜。所以需要云端监控终端

设备的公网 IP 信息是否有变动。如上所述，虽然本方案中出于隐私保护的原因，大量的数据通过联邦学习在终端设备进行判定和训练，但是依然会有少量数据必须在云端进行判定。所以从方案的完整性角度考虑，在云端必须要有一个云端威胁判定模块，也就是说云端威胁判定模块用于判断终端设备的状态数据之外的数据，如终端设备的网络数据。

联邦学习模块：终端设备的联邦学习模块主要功能是输入终端设备的数据，输出是对于终端设备数据的判定模型。而云端的联邦学习模块就是对于终端设备上传的模型进行训练。这个模块的输入是终端设备上传的模型，输出是对这些输入模型训练后的新模型。云端的联邦学习模块控制着整个联邦学习的流程。终端设备联邦学习模型的训练并不会实时的进行，一是因为实时训练数据量小，不能有很好的效果，二是因为模型训练会消耗较多的系统资源。所以一般是选择深夜时间，将一天积累的数据集中训练。所以步骤 101~步骤 102 中联邦学习流程的频率是一天一次。并且在每次联邦学习流程开始前，终端设备需要和云端进行协商确认当前终端设备是否加入本轮的联邦学习流程。云端会根据一定的条件进行筛选，选择足够数量的终端设备参与联邦学习流程。

数据存储模块：终端设备的数据，模型，日志，云端的判定结果都会统一结构化存储到数据库中，当然为了使用数据的方便，可以将热数据备份一份到 redis 中方便其他模块的存取。数据存储模块提供相关数据给到对外接口模块使用。

对外接口模块：这个模块的主要作用主要是提供给业务使用方。如业务使用方查询终端设备的安全分值，并获取各个安全维度的详细信息。这个模块通过两种方式对外提供数据，一种可以是页面的形式，直接通过页面展示所有终端设备的状态；另一种是 API 调用的方式，通过 API 查询的方式获取终端设备的安全分值甚至具体的各个安全维度的信息。

另外云端还有一些常规功能，如终端设备日志监控，终端设备崩溃处理等。

需要说明的是，云端的云端判定模块，常规服务模块，存储模块和对外接口模块可以替换或者删除，不影响整个方案的核心功能。云端最核心的功能在于联邦学习，所以云端框架图最极端情况下可以只包括联邦学习模型。

更具体地，本发明实施例提供的一种终端设备的安全状态判断方法具体过程可以如图 5 所示。

步骤 501：在实验室环境中，算法工程师通过模拟的未知威胁数据理解模型构造出模型算法，并通过模拟的正负样本训练出初始的未知威胁判定模型，这个模型用于终端设备未知威胁判定模型的冷启动。

步骤 502：在步骤 501 中生成的未知威胁判定初始模型，需要在终端实际上线使用前部署到每一台终端设备中，保证在安全态势感知功能使用时，未知威胁判定模型可以生效。

步骤 503：该步骤进入终端安全态势感知的循环处理。在终端设备实际运行时，隔一个固定时间就会采集终端数据进行威胁判定。其中一部分数据用于已知威胁判定。其中已知威胁是指如 root 手机，hook 框架等常见的攻击手段。另外一部分数据会进行未知威胁判定，这里未知威胁的判定模型最开始就是第一步中实验室生成的模型。

步骤 504：当到指定时间，并且当前终端被云端选择成为本轮联邦学习流程的终端后，则将当天采集的数据进行处理，训练的数据集是将已知威胁的判定结果作为标签，采集的数据全集作为数据。输入到终端的学习框架中，进行本地未知威胁模型的训练，训练完成后将当天数据进行清除。另外如果当前终端并没有被云端选择成为本轮联邦学习流程的参与终端，则需要立刻将当天存储的数据进行清除处理。

步骤 505：当各个参与联邦学习的终端训练完成后，各个终端将本地训练的模型上传云端，云端则需要等待终端的模型上传。其中会出现终端训练失败，或者终端网络断开无法上传的情况。云端获得的终端模型数量如果不满足一个阈值条件，则本轮的联邦学习失败。如果满足阈值条件则启动云端的联邦学习，由云端服务器的联邦学习模块对终端上传的模型进行训练。

步骤 506：云端的联邦学习模块往往是在一个独立的硬件环境中进行训练，因为机器学习可能需要 CPU 的加速。所以云端中真实的联邦学习训练模块和控制逻辑往往是分离的，控制逻辑将终端上传的未知威胁模型输入到联邦学习训练模块中，学习完成后输出一个优化后的未知威胁判定模型。

步骤 507：完成云端的联邦学习过程后，云端会将优化后的未知威胁判定模型下发给所有在线的终端设备，终端设备获取到云端下发的更新后的未知威胁判定模型后，将新模型替换原本的旧模型，完成新模型的部署使用。

新模型部署完成后，联邦学习模块会进入周期迭代的流程，每天都会将步骤 503~步骤 507 循环执行，一直迭代到模型稳定为止。

进一步地，在终端设备的联邦学习的实现示意图，如图 6 所示。

在手机端，联邦学习的功能以 SDK 形态实现，和检测模块通过 API 进行通信，数据采集和终端威胁判定生成的数据会保存在终端建立的一个数据仓库中，联邦学习 SDK 通过 API 取用数据仓库中的数据，并有状态与流程控制模块控制终端的训练流程。终端模型训练完成后需要通过通信模块上传到云端服务器，不过在传输前，为保证模型数据的安全性，也需要通过加解密模块进行模型加密。

进一步地，在服务器端的联邦学习的实现示意图，如图 7 所示。

联邦学习的服务端通过云端的通信模块接收到终端上传的模型数据后，首先通过加解

密模块解密模型数据，在进行云端聚合之前，需要通过模型验证模块验证终端模型数据是否正确。最后通过联邦学习聚合模块将终端设备的模型进行聚合训练，生成新的未知威胁判定模型。

所以综合上述过程，终端设备与服务器端联合的步骤流程如图 8 所示。

步骤 801：判断数据仓库中的数据是否有更新，并且确认当前终端设备是否满足启动联邦学习的条件。

步骤 802：如果满足启动条件，则终端设备向服务端进行注册，告诉服务端当前终端设备可以进行联邦学习。

步骤 803：当云端判断本轮加入联邦学习的终端设备数量满足阈值要求的情况下，云端（服务器端）会通知终端设备启动本轮的联邦学习流程。

步骤 804：当终端设备接收到云端启动联邦学习的流程指令时，终端设备的联邦学习模块会读取数据仓库中的数据，并在终端设备进行训练。训练完成后终端设备将本轮训练出的未知威胁判定模型上传到云端。

步骤 805：云端在启动联邦学习流程后就会等待终端设备的模型上传，当所有终端设备都已经上传终端设备模型或者超时的情况下终端设备上传的模型数量满足模型聚合的最低要求，则云端会开启模型聚合的过程；否则如果云端等待超时，并且云端收到终端设备回传的模型数量不足以开启模型聚合，则会认为本轮联邦学习失败。

步骤 806：如果云端模型聚合顺利结束，则云端会将聚合后的模型下发给所有终端设备，并通知所有终端设备更新和部署新的未知威胁判定模型。至此一轮联邦学习流程结束。

如图 9 所示，本发明提供一种终端设备的安全状态判断装置，包括：

获取模块 901，用于获取目标终端设备的未知威胁的待判断状态数据；所述目标终端设备为多个终端设备的任一终端设备；

处理模块 902，用于将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，获得所述第一安全状态判断模型输出的第一判断结果；

所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的；其中，在任一轮机器学习训练中，所述多个终端设备中任一终端设备用于将该轮机器学习训练的本地训练参数发送至服务端，所述服务端用于将该轮机器学习训练中所述多个终端设备的本地训练参数融合，获得融合训练参数，并将所述融合训练参数发送至所述多个终端设备，使得所述多个终端设备基于所述融合训练参数更新或作为所述第一安全状态判断模型的模型参数。

可选的，所述获取模块 901 按照以下方式获得所述目标终端设备的未知威胁的标签化

数据：

获取所述目标终端设备的未知威胁的无标签数据；

基于所述无标签数据获取所述标签化数据。

可选的，所述获取模块 901 具体用于：

将所述无标签数据输入至已知威胁的至少一个第二安全状态判断模型，获得所述至少一个第二安全状态判断模型输出的至少一个第二判断结果；

根据所述至少一个第二判断结果，确定所述无标签数据的标签值，从而将所述无标签数据转换为所述标签化数据。

可选的，所述获取模块 901 具体用于：基于所述无标签数据，按照预设聚类算法，获得所述无标签数据的第一簇聚类数据和第二簇聚类数据；所述第一簇聚类数据的数据量小于所述第二簇聚类数据的数据量；

将所述第一簇聚类数据的标签值设置为第一标签值，将所述第二簇聚类数据的标签值设置为第二标签值，从而将所述无标签数据转换为所述标签化数据；所述第一标签值表征数据为不安全数据，所述第二标签值表征数据为安全数据。

可选的，所述获取模块 901 按照以下方式获得所述第一安全状态判断模型：

在任一轮机器学习训练中，基于所述未知威胁的标签化数据和安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数；将所述第二本地训练参数发送至所述服务端；获得来自所述服务端的融合训练参数；所述融合训练参数是所述服务端基于所述多个终端设备发送的本地训练参数得到的；

若所述安全状态训练模型不满足预设收敛条件，则将所述融合训练参数重新作为所述第一本地训练参数，返回基于所述未知威胁的标签化数据和所述安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数的步骤；

若所述安全状态训练模型满足所述预设收敛条件，则将所述融合训练参数作为所述安全状态训练模型的模型参数，将此时的所述安全状态训练模型作为所述第一安全状态判断模型。

可选的，所述获取模块 901 还用于：将所述第一判断结果发送至所述服务端。

可选的，所述多个终端设备未知威胁的标签化数据均具有相同的数据特征维度。

基于同一发明构思，本发明实施例还提供了一种计算机设备，包括程序或指令，当所述程序或指令被执行时，如本发明实施例提供的终端设备的安全状态判断方法及任一可选方法被执行。

基于同一发明构思，本发明实施例还提供了一种计算机可读存储介质，包括程序或指

令，当所述程序或指令被执行时，如本发明实施例提供的终端设备的安全状态判断方法及任一可选方法被执行。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权利要求

1、一种终端设备的安全状态判断方法，其特征在于，包括:

目标终端设备获取未知威胁的待判断状态数据；所述目标终端设备为多个终端设备的任一终端设备;

所述目标终端设备将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，获得所述第一安全状态判断模型输出的第一判断结果;

所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的；其中，在任一轮机器学习训练中，所述多个终端设备中任一终端设备用于将该轮机器学习训练的本地训练参数发送至服务端，所述服务端用于将该轮机器学习训练中所述多个终端设备的本地训练参数融合，获得融合训练参数，并将所述融合训练参数发送至所述多个终端设备，使得所述多个终端设备基于所述融合训练参数更新或作为所述第一安全状态判断模型的模型参数。

2、如权利要求 1 所述的方法，其特征在于，所述目标终端设备按照以下方式获得所述目标终端设备的未知威胁的标签化数据:

所述目标终端设备获取所述目标终端设备的未知威胁的无标签数据;

所述目标终端设备基于所述无标签数据获取所述标签化数据。

3、如权利要求 2 所述的方法，其特征在于，所述目标终端设备基于所述无标签数据获取所述标签化数据，包括:

所述目标终端设备将所述无标签数据输入至已知威胁的至少一个第二安全状态判断模型，获得所述至少一个第二安全状态判断模型输出的至少一个第二判断结果;

所述目标终端设备根据所述至少一个第二判断结果，确定所述无标签数据的标签值，从而将所述无标签数据转换为所述标签化数据。

4、如权利要求 2 所述的方法，其特征在于，所述目标终端设备基于所述无标签数据获取所述标签化数据，包括:

所述目标终端设备基于所述无标签数据，按照预设聚类算法，获得所述无标签数据的第一簇聚类数据和第二簇聚类数据；所述第一簇聚类数据的数据量小于所述第二簇聚类数据的数据量;

所述目标终端设备将所述第一簇聚类数据的标签值设置为第一标签值，将所述第二簇聚类数据的标签值设置为第二标签值，从而将所述无标签数据转换为所述标签化数据；所述第一标签值表征数据为不安全数据，所述第二标签值表征数据为安全数据。

5、如权利要求 1 所述的方法，其特征在于，所述目标终端设备按照以下方式获得所述第一安全状态判断模型：

在任一轮机器学习训练中，所述目标终端设备基于所述未知威胁的标签化数据和安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数；

所述目标终端设备将所述第二本地训练参数发送至所述服务端；

所述目标终端设备获得来自所述服务端的融合训练参数；所述融合训练参数是所述服务端基于所述多个终端设备发送的本地训练参数得到的；

若所述安全状态训练模型不满足预设收敛条件，则所述目标终端设备将所述融合训练参数重新作为所述第一本地训练参数，返回所述目标终端设备基于所述未知威胁的标签化数据和所述安全状态训练模型的第一本地训练参数，获得所述安全状态训练模型的第二本地训练参数的步骤；

若所述安全状态训练模型满足所述预设收敛条件，则所述目标终端设备将所述融合训练参数作为所述安全状态训练模型的模型参数，将此时的所述安全状态训练模型作为所述第一安全状态判断模型。

6、如权利要求 1 至 5 任一项所述的方法，其特征在于，所述获得所述第一安全状态判断模型输出的第一判断结果之后，还包括：

所述目标终端设备将所述第一判断结果发送至所述服务端。

7、如权利要求 1 至 5 任一项所述的方法，其特征在于，所述多个终端设备未知威胁的标签化数据均具有相同的数据特征维度。

8、一种终端设备的安全状态判断装置，其特征在于，包括：

获取模块，用于获取目标终端设备的未知威胁的待判断状态数据；所述目标终端设备为多个终端设备的任一终端设备；

处理模块，用于将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，获得所述第一安全状态判断模型输出的第一判断结果；

所述第一安全状态判断模型是多个终端设备及服务端基于所述多个终端设备未知威胁的标签化数据进行机器学习训练得到的；其中，在任一轮机器学习训练中，所述多个终端设备中任一终端设备用于将该轮机器学习训练的本地训练参数发送至服务端，所述服务端用于将该轮机器学习训练中所述多个终端设备的本地训练参数融合，获得融合训练参数，并将所述融合训练参数发送至所述多个终端设备，使得所述多个终端设备基于所述融合训练参数更新或作为所述第一安全状态判断模型的模型参数。

9、一种计算机设备，其特征在于，包括程序或指令，当所述程序或指令被执行时，

如权利要求 1 至 7 中任意一项所述的方法被执行。

10、一种计算机可读存储介质，其特征在于，包括程序或指令，当所述程序或指令被执行时，如权利要求1至7中任意一项所述的方法被执行。

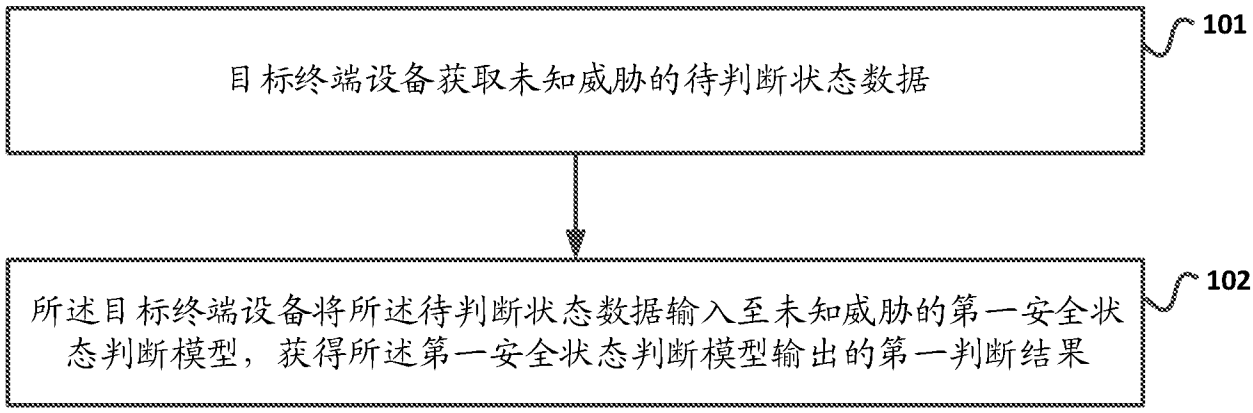
101
目标终端设备获取未知威胁的待判断状态数据
102
所述目标终端设备将所述待判断状态数据输入至未知威胁的第一安全状态判断模型，获得所述第一安全状态判断模型输出的第一判断结果

图 1

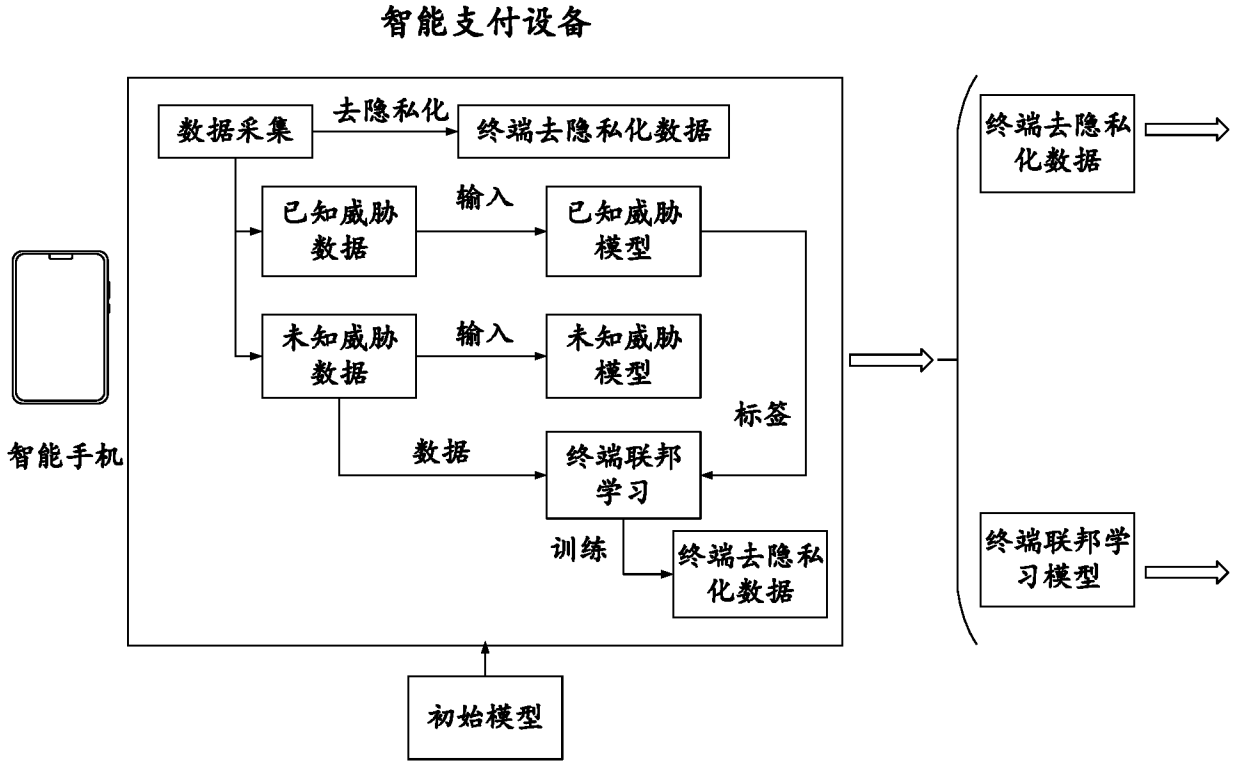
智能支付设备
数据采集
去隐私化
终端去隐私化数据
已知威胁数据
输入
已知威胁模型
未知威胁数据
输入
未知威胁模型
标签
数据
终端联邦学习
训练
终端去隐私化数据
智能手机
初始模型
终端去隐私化数据
终端联邦学习模型

图 2

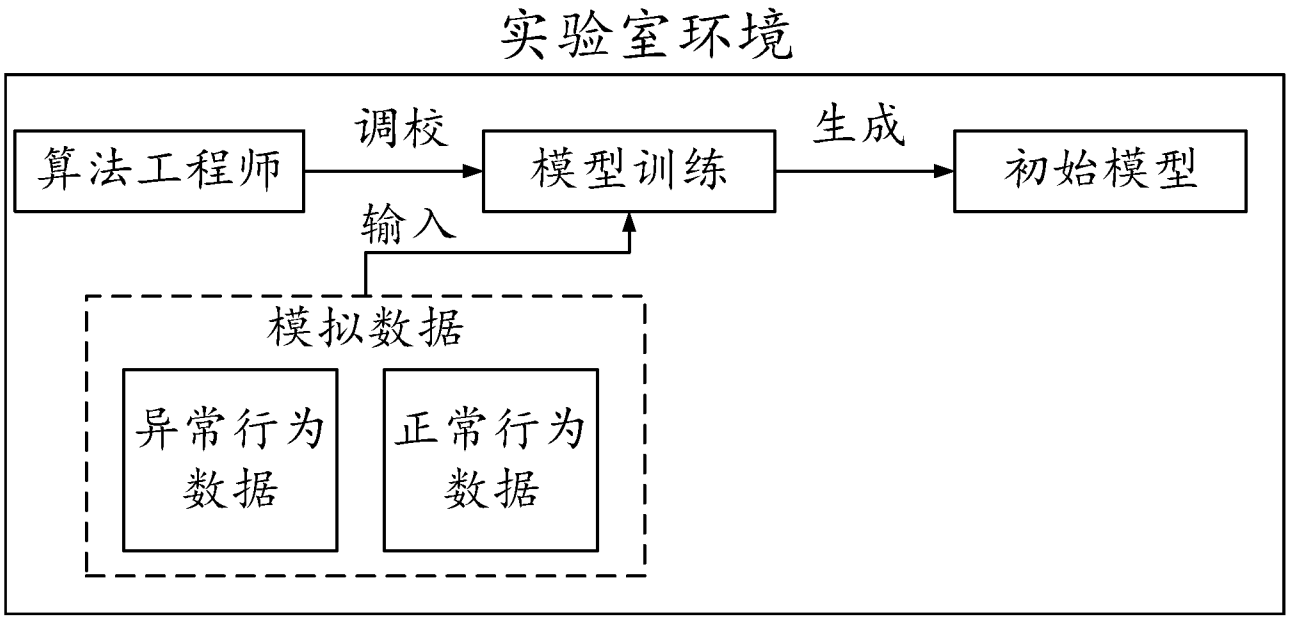
实验室环境
算法工程师
调校
模型训练
生成
初始模型
输入
模拟数据
异常行为数据
正常行为数据

图 3

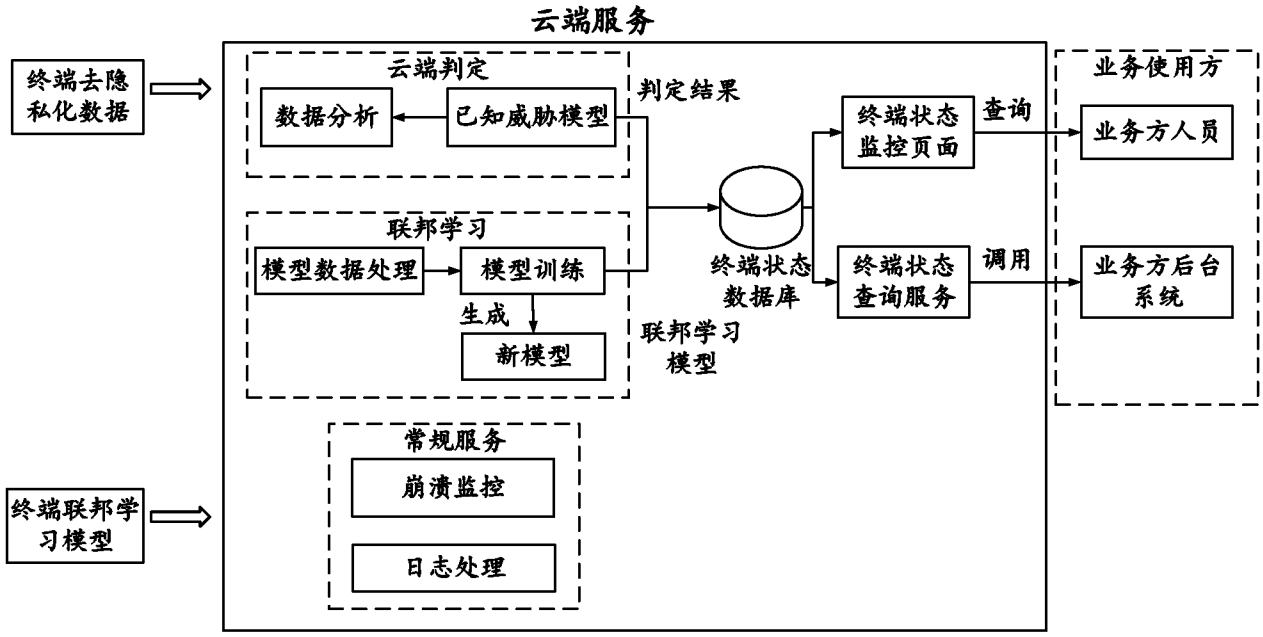
云端服务
终端去隐私化数据
云端判定
数据分析
已知威胁模型
判定结果
联邦学习
模型数据处理
模型训练
生成
新模型
联邦学习模型
终端状态数据库
终端状态监控页面
查询
终端状态查询服务
调用
业务使用方
业务方人员
业务方后台系统
常规服务
崩溃监控
日志处理
终端联邦学习模型

图 4

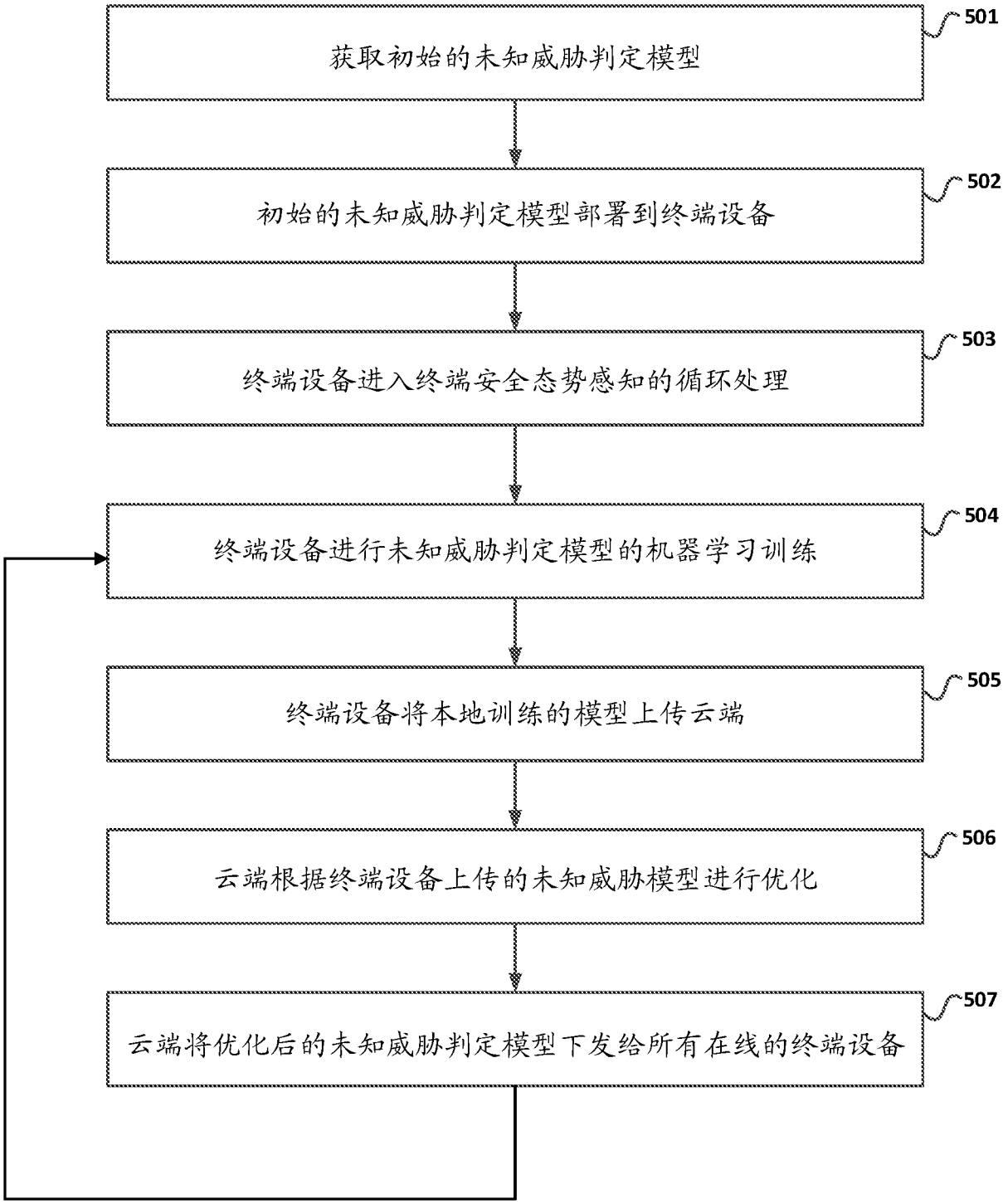
获取初始的未知威胁判定模型
501
初始的未知威胁判定模型部署到终端设备
502
终端设备进入终端安全态势感知的循环处理
503
终端设备进行未知威胁判定模型的机器学习训练
504
终端设备将本地训练的模型上传云端
505
云端根据终端设备上传的未知威胁模型进行优化
506
云端将优化后的未知威胁判定模型下发给所有在线的终端设备
507

图 5

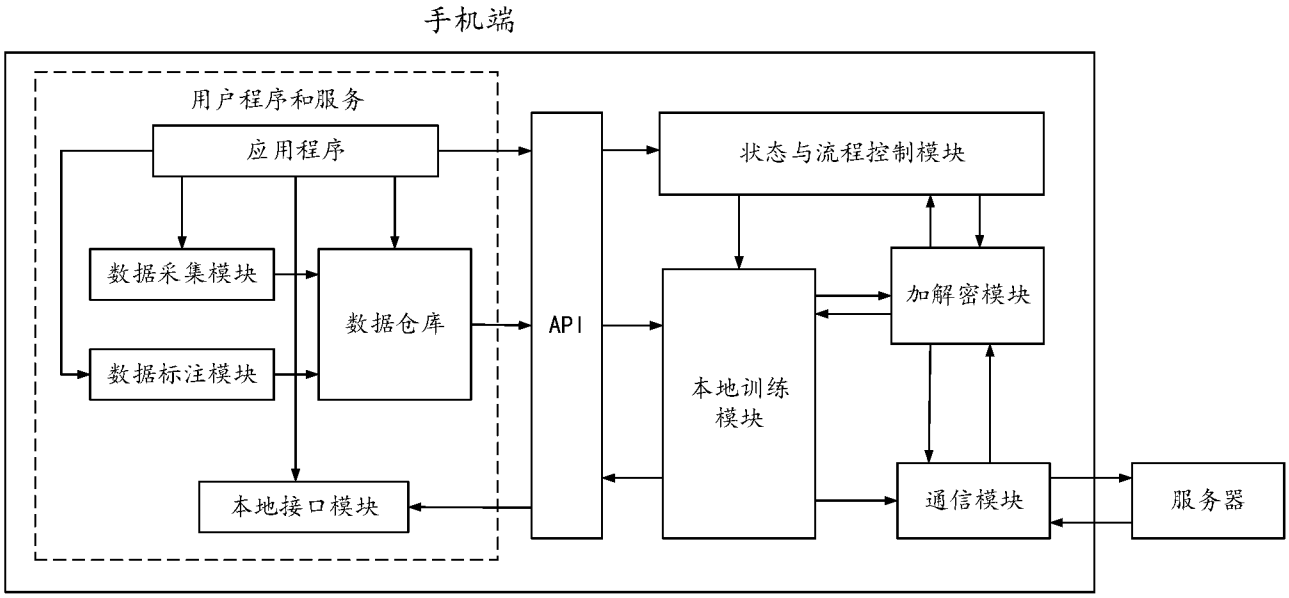
手机端
用户程序和服务
应用程序
数据采集模块
数据标注模块
数据仓库
本地接口模块
API
状态与流程控制模块
本地训练模块
加解密模块
通信模块
服务器

图 6

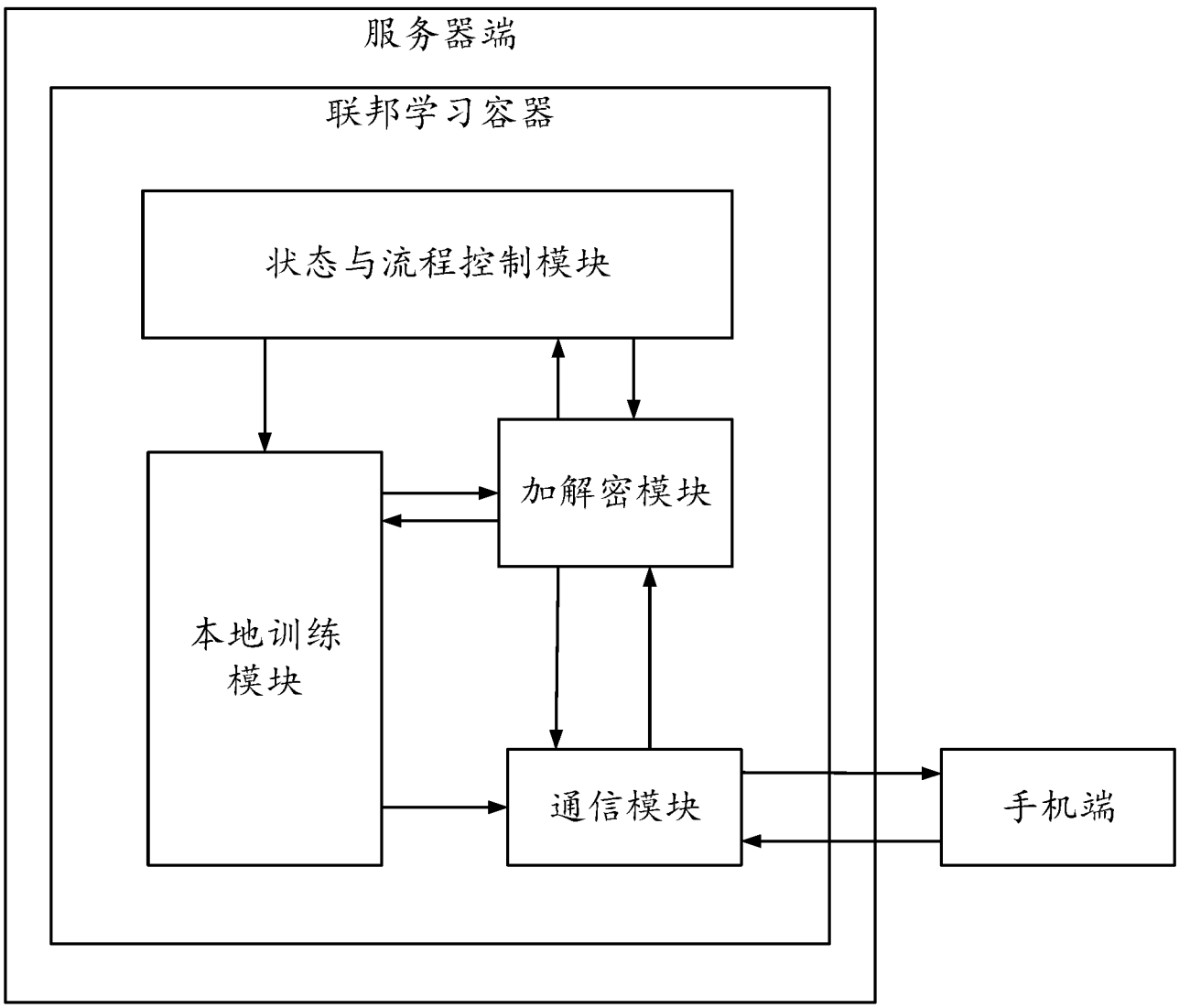
服务器端
联邦学习容器
状态与流程控制模块
加解密模块
本地训练模块
通信模块
手机端

图 7

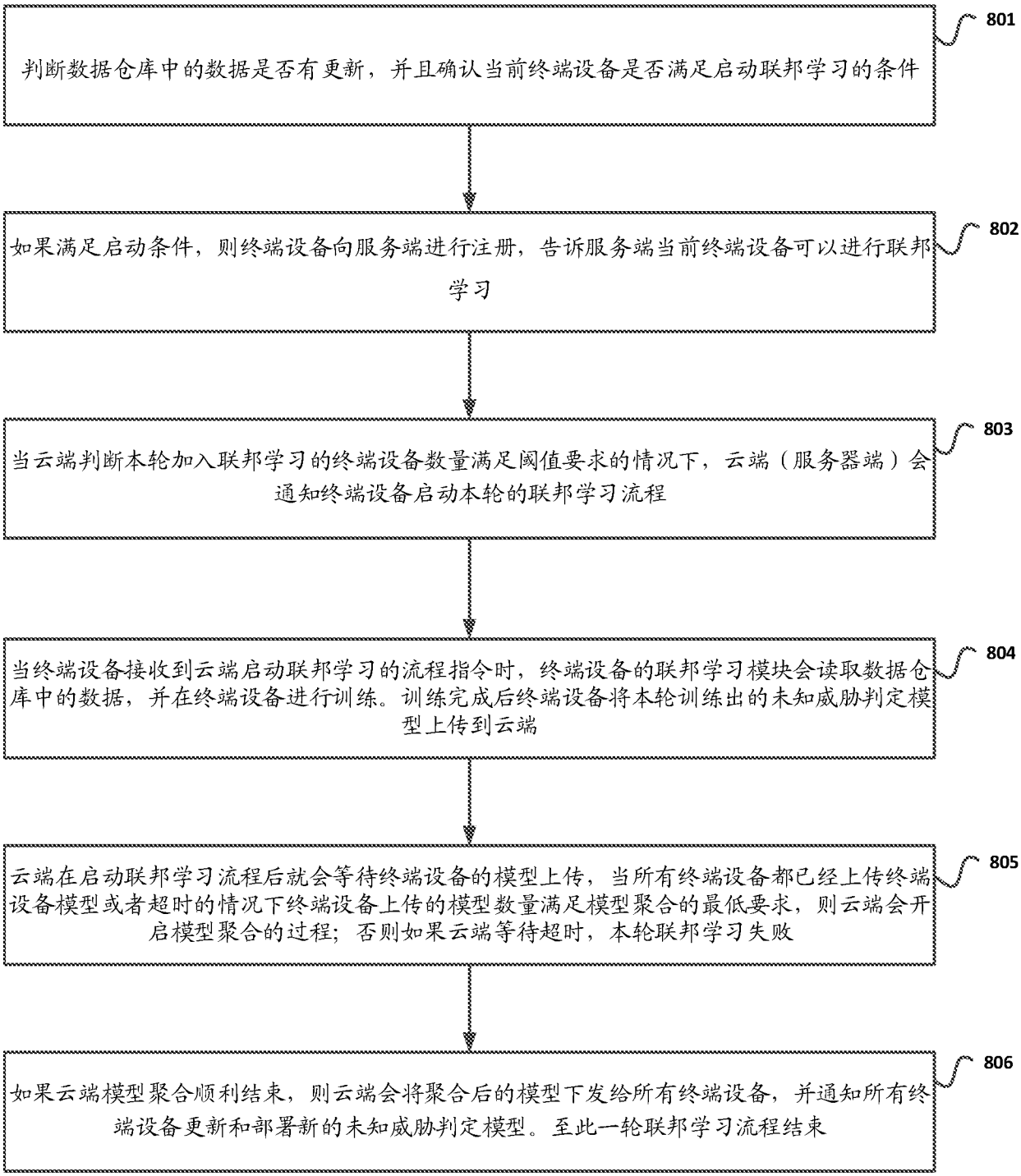
判断数据仓库中的数据是否有更新，并且确认当前终端设备是否满足启动联邦学习的条件
801
如果满足启动条件，则终端设备向服务端进行注册，告诉服务端当前终端设备可以进行联邦学习
802
当云端判断本轮加入联邦学习的终端设备数量满足阈值要求的情况下，云端（服务器端）会通知终端设备启动本轮的联邦学习流程
803
当终端设备接收到云端启动联邦学习的流程指令时，终端设备的联邦学习模块会读取数据仓库中的数据，并在终端设备进行训练。训练完成后终端设备将本轮训练出的未知威胁判定模型上传到云端
804
云端在启动联邦学习流程后就会等待终端设备的模型上传，当所有终端设备都已经上传终端设备模型或者超时的情况下终端设备上传的模型数量满足模型聚合的最低要求，则云端会开启模型聚合的过程；否则如果云端等待超时，本轮联邦学习失败
805
如果云端模型聚合顺利结束，则云端会将聚合后的模型下发给所有终端设备，并通知所有终端设备更新和部署新的未知威胁判定模型。至此一轮联邦学习流程结束
806

图 8

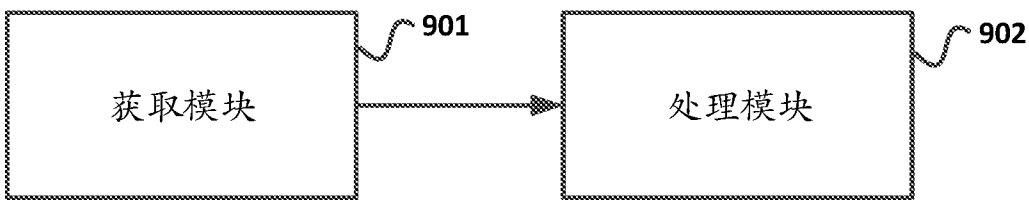
获取模块
901
处理模块
902

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/128867

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: 状态, 安全, 威胁, 判断, 标签, 训练, 模型, 联邦学习, estate, state, position, safety, security, threat, intimidate, estimate, judgement, label, tag, educate, training, model, former, federation, learning, study

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112800428 A (CHINA UNIONPAY CO., LTD.) 14 May 2021 (2021-05-14) claims 1-10	1-10
Y	CN 112070180 A (ELECTRIC POWER RESEARCH INSTITUTE, CHINA SOUTHERN POWER GRID et al.) 11 December 2020 (2020-12-11) claims 1-10, description paragraphs [0042]-[0096]	1-10
Y	CN 111310938 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 19 June 2020 (2020-06-19) claims 1-10, description paragraphs [0049]-[0150]	1-10
A	CN 110113348 A (SICHUAN CHANGHONG ELECTRIC CO., LTD.) 09 August 2019 (2019-08-09) entire document	1-10
A	US 2020125739 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 23 April 2020 (2020-04-23) entire document	1-10

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 January 2022	**28 January 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/128867

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112800428 A	14 May 2021	None	
CN 112070180 A	11 December 2020	None	
CN 111310938 A	19 June 2020	None	
CN 110113348 A	09 August 2019	None	
US 2020125739 A1	23 April 2020	US 10970402 B2	06 April 2021

国际检索报告

国际申请号
PCT/CN2021/128867

A. 主题的分类

G06F 21/57(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, WPI, EPODOC, CNKI, IEEE: 状态，安全，威胁，判断，标签，训练，模型，联邦学习，estate, state, position, safety, security, threat, intimidate, estimate, judgement, label, tag, educate, training, model, former, federation, learning, study

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 112800428 A (中国银联股份有限公司) 2021年5月14日 (2021-05-14) 权利要求1-10	1-10
Y	CN 112070180 A (南方电网科学研究院有限责任公司 等) 2020年12月11日 (2020-12-11) 权利要求1-10，说明书第[0042]-[0096]段	1-10
Y	CN 111310938 A (深圳前海微众银行股份有限公司) 2020年6月19日 (2020-06-19) 权利要求1-10，说明书第[0049]-[0150]段	1-10
A	CN 110113348 A (四川长虹电器股份有限公司) 2019年8月9日 (2019-08-09) 全文	1-10
A	US 2020125739 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2020年4月23日 (2020-04-23) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2022年1月21日	2022年1月28日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 胡贝贝 电话号码 86-(10)-53961415

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/128867

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	112800428	A	2021年5月14日	无			
CN	112070180	A	2020年12月11日	无			
CN	111310938	A	2020年6月19日	无			
CN	110113348	A	2019年8月9日	无			
US	2020125739	A1	2020年4月23日	US	10970402	B2	2021年4月6日