(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 112016078 A
(43)申请公布日 2020.12.01

(21)申请号 202010872545.7

(22)申请日 2020.08.26

(71)申请人 广州市百果园信息技术有限公司
地址 511402 广东省广州市番禺区市桥街兴泰路274号C栋西塔5-13层

(72)发明人 杨景添 苏航

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孟金喆

(51)Int.Cl.
G06F 21/44(2013.01)
G06K 9/62(2006.01)

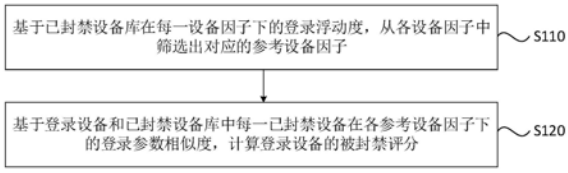
权利要求书2页 说明书10页 附图5页

(54)发明名称

一种登录设备的封禁检测方法、装置、服务器和存储介质

(57)摘要

本发明实施例公开了一种登录设备的封禁检测方法、装置、服务器和存储介质。其中，该方法包括：基于已封禁设备库在每一设备因子下的登录浮动度，从各所述设备因子中筛选出对应的参考设备因子；基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度，计算所述登录设备的被封禁评分。本发明实施例提供的技术方案，确保登录设备面向封禁检测的可靠性，无需对每一使用多开软件的登录设备进行封禁，或者对登录设备进行聚类封禁，在保证登录设备执行任何正常操作的基础上，避免封禁检测的滞后性，从而提高了登录设备面向封禁检测的准确性和封禁及时性。



CN 112016078 A

1.一种登录设备的封禁检测方法,其特征在于,包括:

基于已封禁设备库在每一设备因子下的登录浮动度,从各所述设备因子中筛选出对应的参考设备因子;

基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度,计算所述登录设备的被封禁评分。

2.根据权利要求1所述的方法,其特征在于,所述基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度,计算所述登录设备的被封禁评分,包括:

针对所述已封禁设备库中的每一已封禁设备,基于所述登录设备和该已封禁设备在各所述参考设备因子下的登录参数,计算所述登录设备和该已封禁设备之间的封禁相似度;

将所述登录设备和每一已封禁设备之间的封禁相似度中的最大相似度,作为所述登录设备的被封禁评分。

3.根据权利要求2所述的方法,其特征在于,所述封禁相似度采用杰卡德距离与相似度之间的反向影响来计算。

4.根据权利要求1所述的方法,其特征在于,所述基于已封禁设备库在每一设备因子下的登录浮动度,从各所述设备因子中筛选出对应的参考设备因子,包括:

基于已封禁设备库在每一设备因子下的登录浮动度,确定各所述设备因子的封禁参考置信度,并筛选出所述封禁参考置信度符合指定封禁检测规格的设备因子,作为所述参考设备因子。

5.根据权利要求1所述的方法,其特征在于,在基于已封禁设备库在每一设备因子下的登录浮动度,从各所述设备因子中筛选出对应的参考设备因子之前,还包括:

针对每一设备因子,基于所述已封禁设备库在该设备因子下各历史登录参数的重复频次,计算所述已封禁设备库在该设备因子下的登录浮动度。

6.根据权利要求5所述的方法,其特征在于,所述基于所述已封禁设备库在该设备因子下各历史登录参数的重复频次,计算所述已封禁设备库在该设备因子下的登录浮动度,包括:

对所述已封禁设备库在每一设备因子下各历史登录参数的重复频次进行熵运算,得到所述已封禁设备库在该设备因子下的登录浮动度。

7.根据权利要求1-6任一项所述的方法,其特征在于,在计算所述登录设备的被封禁评分之后,还包括:

如果所述登录设备的被封禁评分超出预设封禁阈值,则对所述登录设备进行封禁。

8.根据权利要求7所述的方法,其特征在于,在对所述登录设备进行封禁之后,还包括:

将完成封禁的登录设备添加至所述已封禁设备库中,并更新所述已封禁设备库在每一设备因子下的登录浮动度。

9.根据权利要求7所述的方法,其特征在于,还包括:

基于完成封禁检测的目标登录设备集合下的封禁准确率和封禁召回率,确定对应的预设封禁阈值。

10.一种登录设备的封禁检测装置,其特征在于,包括:

参考因子筛选模块,用于基于已封禁设备库在每一设备因子下的登录浮动度,从各所

述设备因子中筛选出对应的参考设备因子；

封禁检测模块，用于基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度，计算所述登录设备的被封禁评分。

11.一种服务器，其特征在于，所述服务器包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-9中任一所述的登录设备的封禁检测方法。

12.一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如权利要求1-9中任一所述的登录设备的封禁检测方法。

一种登录设备的封禁检测方法、装置、服务器和存储介质

技术领域

[0001] 本发明实施例涉及互联网技术领域，尤其涉及一种登录设备的封禁检测方法、装置、服务器和存储介质。

背景技术

[0002] 随着互联网技术的快速发展，各种应用程序(Application，APP)平台或者网络社区内基本都会存在一些网络黑色产业链(即网络黑产)和恶意用户等，来传播一些违规信息；因此，为了限制网络黑产和恶意用户的违规行为，通常会预先设置相应的风控处罚逻辑，在网络黑产和恶意用户所使用的违规账号达到一定的封禁级别时，会该违规账号和该违规账号所处的登录设备同时进行封禁。此时，用户在某一设备上请求登录对应的账号时，该风控处罚逻辑主要采用该设备的标识信息来判断该设备是否为已封禁设备，但是网络黑产和恶意用户可以使用各类多开软件来更改本次登录设备的标识信息，以绕过已封禁设备的违规检测，继续执行对应的违规行为，无法保障正常用户的信息浏览安全。

[0003] 目前，通常采用如下两种方式来解决上述问题：1)通过分析登录设备的上报信息，判断是否使用多开软件，进而禁止用户在使用多开软件的登录设备上进行登录；但是，在很多APP网络场景下，支持正常用户使用多开软件对登录设备的标识信息进行更改，此时禁止每一使用多开软件的登录设备上的用户登录，直接影响到正常用户的常规操作而造成大量用户流失。2)采用聚类算法对大量登录设备进行分类，然后存在已封禁设备的类别下的每一登录设备均进行封禁，此时聚类算法仅能初步圈定封禁设备的范围，无法保证封禁设备的准确性，而且由聚类算法初步圈定的封禁设备范围存在一定滞后性，无法保证对存在违规行为的登录设备进行及时封禁。

发明内容

[0004] 本发明实施例提供了一种登录设备的封禁检测方法、装置、服务器和存储介质，在保证登录设备正常操作的基础上，提高登录设备面向封禁检测的准确性和封禁及时性。

[0005] 第一方面，本发明实施例提供了一种登录设备的封禁检测方法，该方法包括：

[0006] 基于已封禁设备库在每一设备因子下的登录浮动度，从各所述设备因子中筛选出对应的参考设备因子；

[0007] 基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度，计算所述登录设备的被封禁评分。

[0008] 第二方面，本发明实施例提供了一种登录设备的封禁检测装置，该装置包括：

[0009] 参考因子筛选模块，用于基于已封禁设备库在每一设备因子下的登录浮动度，从各所述设备因子中筛选出对应的参考设备因子；

[0010] 封禁检测模块，用于基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度，计算所述登录设备的被封禁评分。

[0011] 第三方面，本发明实施例提供了一种服务器，该服务器包括：

[0012] 一个或多个处理器；

[0013] 存储装置，用于存储一个或多个程序；

[0014] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现本发明任意实施例所述的登录设备的封禁检测方法。

[0015] 第四方面，本发明实施例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本发明任意实施例所述的登录设备的封禁检测方法。

[0016] 本发明实施例提供的一种登录设备的封禁检测方法、装置、服务器和存储介质，由于已封禁设备库在每一设备因子下的登录浮动越大，说明该设备因子被篡改的可能性越大，也就是该设备因子对登录设备进行封禁检测的参考价值越低，因此基于已封禁设备库在每一设备因子下的登录浮动度，可以从全部设备因子中筛选出对应的参考设备因子，进而通过分析登录设备和该已封禁设备库中每一已封禁设备在各个参考设备因子下的登录参数相似度，来计算该登录设备的被封禁评分，从而准确判断该登录设备是否需要被封禁的可能性，确保登录设备面向封禁检测的可靠性，无需对每一使用多开软件的登录设备进行封禁，或者对登录设备进行聚类封禁，在保证登录设备执行任何正常操作的基础上，避免封禁检测的滞后性，从而提高了登录设备面向封禁检测的准确性和封禁及时性。

附图说明

[0017] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本发明的其它特征、目的和优点将会变得更明显：

[0018] 图1A为本发明实施例一提供的一种登录设备的封禁检测方法的流程图；

[0019] 图1B为本发明实施例一提供的登录设备的封禁检测过程的原理示意图；

[0020] 图2A为本发明实施例二提供的一种登录设备的封禁检测方法的流程图；

[0021] 图2B为本发明实施例二提供的登录设备的封禁检测过程的原理示意图；

[0022] 图3A为本发明实施例三提供的一种登录设备的封禁检测方法的流程图；

[0023] 图3B为本发明实施例三提供的方法中每一设备因子下的登录浮动度和判断是否封禁时参考的预设封禁阈值的动态更新过程的原理示意图；

[0024] 图4为本发明实施例四提供的一种登录设备的封禁检测装置的结构示意图；

[0025] 图5为本发明实施例五提供的一种服务器的结构示意图。

具体实施方式

[0026] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。此外，在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

[0027] 实施例一

[0028] 图1A为本发明实施例一提供的一种登录设备的封禁检测方法的流程图，本实施例可适用于在任一种登录场景下检测本次的登录设备是否需要被封禁的情况中。本实施例提供的登录设备的封禁检测方法可以由本发明实施例提供的登录设备的封禁检测装置来执行，该装置可以通过软件和/或硬件的方式来实现，并集成在执行本方法的服务器中，该服

务器可以是配置有用户账号注册和登录需求的各类应用程序的后台服务器。

[0029] 具体的,参考图1A,该方法可以包括如下步骤:

[0030] S110,基于已封禁设备库在每一设备因子下的登录浮动度,从各设备因子中筛选出对应的参考设备因子。

[0031] 具体的,为了限制网络黑产和恶意用户的违规行为,而避免在互联网领域内发布的各类违规内容的传播,用户在某一设备上注册或者登录某一应用程序的相应账号时,首先需要判断当前注册登录所采用的该设备是否属于已经被检测出来的已封禁设备,此时通常会将使用多开软件以对当前登录设备的标识信息进行更改的任一登录设备作为封禁设备,来禁止用户在该登录设备上执行任何账号相关操作,但是多开软件除了被网络黑产和恶意用户使用,来更改设备标识信息以绕过封禁检测之外,还会支持正常用户的使用,此时对所有使用多开软件的登录设备进行封禁的方式直接影响到正常用户的常规操作,无法保证登录设备的封禁准确性;或者,通过分析当前登录设备聚类后所属的类别是否为封禁设备类别,来判断当前登录设备是否封禁设备,但是聚类算法属于粗粒度的分类,无法确保登录设备的封禁准确性,而且采用聚类算法后的封禁设备分类存在一定的滞后性,无法保证登录设备封禁检测的及时性。因此,为了避免上述问题,本实施例提供了一种新的封禁检测方式,以在用户使用某个设备注册或登录相应账号时,不用限制用户在登录设备上使用多开软件时的操作,而保证用户在登录设备上执行各类正常操作的同时,还能够准确及时地检测出需要封禁的登录设备,而限制用户在该登录设备上执行任何账号相关操作。

[0032] 此时,由于网络黑产和恶意用户通常会使用多开软件更改登录设备的标识信息来绕过已经检测出的各个封禁设备的违规检测,而在某一设备的各类应用程序上登录相应的用户账号时,该用户账号会处于相应的设备环境里,也就是不同登录设备上的用户账号注册或登录,均会存在对应的设备自适应标识、互联网协议(Internet Protocol,IP)地址、介质访问控制(Media Access Control,MAC)地址、无线网络、客户端版本、操作系统、设备型号和屏幕分辨率等各类设备因子,此时可以理解的是,网络黑产和恶意用户在对某一登录设备上的不同设备因子下的登录参数进行更改时,由于不同设备因子的开发设计难度不同而导致不同设备因子下登录参数的篡改成本也不同,那么各个设备因子被篡改的难度也不同,也就是说设备的全部设备因子中总是会存在登录参数不容易被篡改的设备因子,因此本实施例可以将登录参数不容易被篡改的设备因子作为对登录设备进行封禁检测的参考设备因子,此时登录设备在参考设备因子下所采用的登录参数不容易被恶意篡改,也就更能够代表真实的设备信息,进而通过分别比对登录设备和各个已经检测出的封禁设备在每一参考设备因子下的登录参数之间的相似度,可以准确判断该登录设备是否需要被封禁的可能性,从而确保登录设备面向封禁检测的可靠性。

[0033] 需要说明的是,如果登录设备在某一设备因子下历史登录各种用户账号时所采用的登录参数发生不断变化,说明该设备因子下登录参数的被篡改难度较低,也就是该设备因子下的登录参数容易被篡改,因而不能作为登录设备封禁检测的参考设备因子。

[0034] 在本实施例中,可以通过分析已经检测出的各个已封禁设备在每一设备因子下所采用的登录参数的浮动情况,来判断该设备因子的被篡改难度,此时本实施例中采用登录浮动度来表征各个设备上注册或登录用户账号时在每一设备因子下所采用的历史登录参数的浮动情况;同时,由于在登录设备上注册或登录用户账号时,首先会对该登录设备进行

封禁检测，因此首先需要从全部设备因子中筛选出对封禁检测的参考价值较大的参考设备因子，以提高登录设备进行封禁检测的准确性，此时在已经封禁检测完成的已封禁设备库中，首先会查找出每一已封禁设备在执行任意账号相关操作而被检测出出需要被封禁时在每一设备因子下所采用的历史登录参数，然后通过分析各个已封禁设备在每一设备因子下所采用的历史登录参数的变化情况，来分别计算已封禁设备库在每一设备因子下的登录浮动度，此时如果已封禁设备库在某一设备因子下的登录浮动度越高，说明该设备因子下的登录参数越容易被恶意篡改，也就是该设备因子对于登录设备进行封禁检测的参考价值较低，而如果已封禁设备库在某一设备因子下的登录浮动度越低，说明该设备因子下的登录参数越不容易被恶意篡改，也就是该设备因子对于登录设备进行封禁检测的参考价值较高，因此通过已封禁设备库在每一设备因子下的登录浮动度，可以从全部设备因子中筛选出登录浮动度较低的部分设备因子，作为本实施例中的参考设备因子，此时登录设备在各个参考设备因子下所采用的登录参数不容易被恶意篡改，后续通过分析登录设备与已封禁设备中每一已封禁设备在各个参考设备因子下所采用的登录参数之间的相似度，可以准确判断该登录设备是否为已封禁设备库中的某个已封禁设备，从而准确判断该登录设备是否需要被封禁的可能性，确保登录设备面向封禁检测的可靠性。

[0035] S120，基于登录设备和已封禁设备库中每一已封禁设备在各参考设备因子下的登录参数相似度，计算登录设备的被封禁评分。

[0036] 可选的，在登录设备上注册或登录用户账号，并从各个设备因子中筛选出对应的参考设备因子之后，为了确保登录设备面向封禁检测的可靠性，本实施例首先会查找出该登录设备在执行任意账号相关操作时在每一参考设备因子下所采用的登录参数，同时查找出已封禁设备库中的每一已封禁设备被封禁时在每一参考设备因子下所采用的登录参数，进而分别分析该登录设备与每一已封禁设备在各个参考设备因子下所采用的登录参数之间的相似度，来判断该登录设备是否已封禁设备库中的某一已封禁设备，如果该登录设备与某一已封禁设备在各个参考设备因子下所采用的登录参数之间的相似度较高，说明该登录设备与该已封禁设备极有可能为同一设备，此时按照该登录设备与某一已封禁设备为同一设备的可能性，可以计算出该登录设备的被封禁评分，无需对每一使用多开软件的登录设备进行封禁，或者对登录设备进行聚类封禁，在保证登录设备执行任何正常操作的基础上，避免封禁检测的滞后性，后续采用该被封禁评分可以准确判断该登录设备当前是否需要被封禁，以禁止用户在该登录设备执行任何的账号相关操作。

[0037] 本实施例提供的技术方案，由于已封禁设备库在每一设备因子下的登录浮动越大，说明该设备因子被篡改的可能性越大，也就是该设备因子对登录设备进行封禁检测的参考价值越低，因此基于已封禁设备库在每一设备因子下的登录浮动度，可以从全部设备因子中筛选出对应的参考设备因子，进而通过分析登录设备和该已封禁设备库中每一已封禁设备在各个参考设备因子下的登录参数相似度，来计算该登录设备的被封禁评分，从而准确判断该登录设备是否需要被封禁的可能性，确保登录设备面向封禁检测的可靠性，无需对每一使用多开软件的登录设备进行封禁，或者对登录设备进行聚类封禁，在保证登录设备执行任何正常操作的基础上，避免封禁检测的滞后性，从而提高了登录设备面向封禁检测的准确性和封禁及时性。

[0038] 实施例二

[0039] 图2A为本发明实施例二提供的一种登录设备的封禁检测方法的流程图，图2B为本发明实施例二提供的登录设备的封禁检测过程的原理示意图。本实施例是在上述实施例的基础上进行优化。具体的，如图2A所示，本实施例对于参考设备因子的具体筛选过程以及登录设备的被封禁评分的具体计算过程进行详细的解释说明。

[0040] 可选的，如图2A所示，本实施例中可以包括如下步骤：

[0041] S210，针对每一设备因子，基于已封禁设备库在该设备因子下各历史登录参数的重复频次，计算已封禁设备库在该设备因子下的登录浮动度。

[0042] 可选的，由于已封禁设备库中的各个已封禁设备被封禁时在每一设备因子下所采用的历史登录参数可能会不同，而登录浮动度可以表征已封禁设备库中各个已封禁设备在每一设备因子下所采用的历史登录参数的变化情况，因此本实施例在检测到登录设备需要执行任意账号相关操作(如注册或登录用户账号)时，首先会查找出每一已封禁设备被封禁时在在每一设备因子下所采用的历史登录参数，进而针对每一设备因子，分别计算出各个已封禁设备被封禁时在该设备因子下所采用的每一历史登录参数在已封禁设备库中不断出现的频次，作为本实施例中已封禁设备库在该设备因子下各历史登录参数的重复频次，此时如果某一设备因子下各个历史登录参数的重复频次均比较高，则说明已封禁设备库在该设备因子下所使用的历史登录参数比较稳定，使得已封禁设备库在该设备因子下的浮动较低，因此本实施例可以通过对已封禁设备库在每一设备因子下所采用的各历史登录参数的重复频次进行综合分析，从而计算出已封禁设备库在每一设备因子下的登录浮动度。

[0043] 示例性的，由于信息熵能够准确度量一个系统中信息的有序化程度，系统中信息越是有序，信息熵越低，而系统中信息越是混乱，信息熵越高，因此如图2B所示，本实施例可以通过信息熵来表示已封禁设备在各个设备因子下的登录浮动度，此时针对每一设备因子，基于已封禁设备库在该设备因子下各历史登录参数的重复频次，计算已封禁设备库在该设备因子下的登录浮动度，可以具体包括：对已封禁设备库在每一设备因子下各历史登录参数的重复频次进行熵运算，得到已封禁设备库在该设备因子下的登录浮动度。

[0044] 具体的，在查找出已封禁设备库在每一设备因子下所采用的历史登录参数，并确定出已封禁设备库在每一设备因子下各历史登录参数的重复频次之后，可以对已封禁设备库在每一设备因子下所采用的各个历史登录参数的重复频次进行熵运算，该熵运算公式为：$H=-\sum_{i=1}^{n}p(x_i)\log_2 p(x_i)$，其中，$x_i$为已封禁设备库在每一设备因子下所采用的第i个历史登录参数，$p(x_i)$为已封禁设备库在每一设备因子下的第i个历史登录参数的重复频次下对应的频率；进而将已封禁设备库在每一设备因子下所采用的各个历史登录参数的重复频次进行熵运算的运算结果作为已封禁设备库在该设备因子下的登录浮动度；按照上述熵运算过程，可以得到已封禁设备库在每一设备因子下的登录浮动度。

[0045] S220，基于已封禁设备库在每一设备因子下的登录浮动度，确定各设备因子的封禁参考置信度，并筛选出封禁参考置信度符合指定封禁检测规格的设备因子，作为参考设备因子。

[0046] 可选的，在计算出已封禁设备库在每一设备因子下的登录浮动度之后，由于登录浮动度与设备因子对于封禁检测的参考价值成反比，因此本实施例可以基于已封禁设备库在每一设备因子下的登录浮动度对于封禁检测的参考价值的反向影响程度，来确定各个设

备因子的封禁参考置信度，该封禁参考置信度能够准确表征某一设备因子作为参考设备因子来对登录设备进行封禁检测的可信程度，此时为了准确筛选相应数量的参考设备因子，本实施例会预先设置对应的指定封禁检测规格，该指定封禁检测规格可以为参考设备因子的数量，进而按照各个设备因子的封禁参考置信度，来筛选出符合该指定封禁检测规格的多个设备因子，作为本实施例中的参考设备因子，例如可以采用TopK算法从全部设备因子中筛选出封禁参考置信度为前K项的设备因子，作为对应的参考设备因子。此外，本实施例中也可以将较低登录浮动度下符合该指定封禁检测规格的多个设备因子，作为本实施例中的参考设备因子，而无需计算各个设备因子的封禁参考置信度，从而减少参考设备因子的筛选步骤。

[0047] S230，针对已封禁设备库中的每一已封禁设备，基于登录设备和该已封禁设备在各参考设备因子下的登录参数，计算登录设备和该已封禁设备之间的封禁相似度。

[0048] 可选的，在筛选出对应的参考设备因子之后，可以针对已封禁设备库中的每一已封禁设备，分别查找出该登录设备执行任意的账号相关操作时在每一参考设备因子下所采用的登录参数，以及该已封禁设备被封禁时在每一参考设备因子下所采用的登录参数，然后由分别确定出每一参考设备因子下所采用的登录参数组成的该登录设备和该已封禁设备的设备特征，进而采用相应的相似度算法分析该登录设备和该已封禁设备在每一参考设备因子下所采用的登录参数之间的相似度，并对每一参考设备因子下的登录参数相似度进行综合分析，计算出登录设备和该已封禁设备之间的封禁相似度；此时通过执行上述步骤，可以分别计算出登录设备和每一已封禁设备之间的封禁相似度。

[0049] 需要说明的是，对于所采用的相似度算法不作限定，而本实施例中登录设备和每一已封禁设备之间的封禁相似度可以采用杰卡德距离与相似度之间的反向影响来计算，通过杰卡德距离计算登录设备与已封禁设备的设备距离(也就是登录设备与已封禁设备之间的相异度)，与封禁相似度之间存在反向影响的关系，此时采用杰卡德距离所计算出的登录设备和某一已封禁设备之间的设备距离越大，那么登录设备和该已封禁设备之间的封禁相似度越小。例如，如果参考设备因子为(serial,iid,uuid,eid,mac,aid)，而登录设备在每一参考设备因子下所采用的登录参数为A＝(efd313432,a3bedbd,4cc33ea,78c5b4a,01:01:01:01:01:01,e683acb)，某一已封禁设备在每一参考设备因子下所采用的登录参数为B＝(ABCDFG,a3bedbd,4cc33ea,78c5b4a,02:02:02:02:02:02,c4aabcd5673)，那么登录设备和该已封禁设备之间的封禁相似度可以为$d_j(A,B)=\frac{|A\cup B|-|A\cap B|}{|A\cup B|}$；此时|A∪B|为9，|A∩B|为3，因此登录设备和该已封禁设备之间的设备距离为2/3，所对应的封禁相似度为1/3。

[0050] S240，将登录设备和每一已封禁设备之间的封禁相似度中的最大相似度，作为登录设备的被封禁评分。

[0051] 可选的，如果登录设备和已封禁设备库中任意一个已封禁设备之间相似，那么说明该登录设备需要被封禁，此时只需要判断登录设备和每一已封禁设备之间的封禁相似度中的最大相似度是否达到预设相似阈值即可，如果登录设备和每一已封禁设备之间的封禁相似度中的最大相似度也低于该预设相似阈值，说明该登录设备和每一已封禁设备均不相似，因此本实施例中可以将登录设备和每一已封禁设备之间的封禁相似度中的最大相似

度，作为登录设备的被封禁评分，此时如果最大相似度表示该登录设备于某一已封禁设备之间相似，那么则可以准确确定该登录设备需要被封禁，从而提高通过登录设备的被封禁评分来判定该登录设备是否需要被封禁的全面性。

[0052] 本实施例提供的技术方案，通过熵运算来计算已封禁设备库在每一设备因子下的登录浮动度，能够确保每一设备因子下的登录浮动度的准确性，进而基于已封禁设备库在每一设备因子下的登录浮动度，筛选出符合指定封禁检测规格的设备因子，作为参考设备因子，确保参考设备因子的可靠性；后续通过分析登录设备和该已封禁设备库中每一已封禁设备在各个参考设备因子下的登录参数相似度，来计算该登录设备的被封禁评分，从而准确判断该登录设备是否需要被封禁的可能性，确保登录设备面向封禁检测的可靠性，无需对每一使用多开软件的登录设备进行封禁，或者对登录设备进行聚类封禁，在保证登录设备执行任何正常操作的基础上，避免封禁检测的滞后性，从而提高了登录设备面向封禁检测的准确性和封禁及时性。

[0053] 实施例三

[0054] 图3A为本发明实施例三提供的一种登录设备的封禁检测方法的流程图，图3B为本发明实施例三提供的方法中每一设备因子下的登录浮动度和判断是否封禁时参考的预设封禁阈值的动态更新过程的原理示意图。本实施例是在上述实施例的基础上进行优化。具体的，如图3A所示，本实施例主要对于根据登录设备的被封禁评分判断是否封禁该登录设备时参考的预设封禁阈值以及由于已封禁设备库的变化而使每一设备因子下的登录浮动度发生变化时登录浮动度的动态更新过程进行详细的解释说明。

[0055] 可选的，如图3A所示，本实施例中可以包括如下步骤：

[0056] S310，基于已封禁设备库在每一设备因子下的登录浮动度，从各设备因子中筛选出对应的参考设备因子。

[0057] S320，基于登录设备和已封禁设备库中每一已封禁设备在各参考设备因子下的登录参数相似度，计算登录设备的被封禁评分。

[0058] S330，基于完成封禁检测的目标登录设备集合下的封禁准确率和封禁召回率，确定对应的预设封禁阈值。

[0059] 可选的，为了确保登录设备面向封禁检测的准确性，本实施例可以通过分析采用本实施例中提供的封禁检测方式来判断各个登录设备是否需要被封禁的准确性和召回率，来动态更新对应的预设封禁阈值，此时在对每一登录设备进行封禁检测之后，无论封禁检测结果如何，均可以将采用本实施例提供的封禁检测方式来判断是否需要被封禁的每一登录设备的封禁结果添加到对应的目标登录设备集合中，此时该目标登录设备集合中的各个登录设备均已经完成封禁检测，存在需要封禁的登录设备，也存在不需要封禁的登录设备，因此可以通过判断该目标登录设备集合中每一登录设备的封禁检测具体结果和真实封禁结果，在登录设备的封禁检测过程中，不断计算出对应的封禁准确率和封禁召回率，进而将该封禁准确率和该封禁召回率作为预设封禁阈值的评价指标，来动态更新对应的预设封禁阈值，此时该预设封禁阈值可以表示能够准确区分需要被封禁的登录设备时的评分节点。

[0060] 示例性的，该封禁准确率的计算公式可以为：$precision=\frac{TP}{TP+FP}$；其中，TP为目标登录设备集合内将需要被封禁的登录设备预测为需要被封禁的设备数量，FP为目标登录设

备集合内将不需要被封禁的登录设备预测为需要被封禁的设备数量;而该封禁召回率的计算公式可以为:$recall=\frac{TP}{TP+FN}$;其中,FN为目标登录设备集合内将需要被封禁的登录设备预测为不需要被封禁的设备数量。

[0061] 此时,可以将封禁准确率达到相应准确性要求,且封禁召回率达到相应的召回要求下对应的登录设备的被封禁评分作为当前的预设封禁阈值,例如本实施例对于封禁准确率要求较高,而对于封禁召回率要求能够达到某一范围即可,因此可以将目标登录设备集合下封禁召回率达到某一召回范围的要求时的多个登录设备中,封禁准确率最高时的该登录设备的被封禁评分作为当前的预设封禁阈值,此时该预设封禁阈值能够在保证相对高的封禁召回的基础上,使封禁检测的准确性达到最高。

[0062] S340,如果登录设备的被封禁评分超出预设封禁阈值,则对登录设备进行封禁。

[0063] 可选的,在计算出登录设备的被封禁评分之后,可以通过比对该登录设备的被封禁评分与预设封禁阈值之间的大小,来判断该登录设备是否需要被封禁,如果登录设备的被封禁评分超出该预设封禁阈值,则说明该登录设备极有可能需要被封禁,因此可以对该登录设备进行封禁,以避免各个用户在该登录设备上执行任何的账号相关操作,从而降低违规内容的广泛传播,提高正常用户浏览信息的安全健康性。

[0064] S350,将完成封禁的登录设备添加至已封禁设备库中,并更新已封禁设备库在每一设备因子下的登录浮动度。

[0065] 可选的,在对登录设备进行封禁之后,可以直接将该登录设备作为已封禁设备,添加至已封禁设备库中,以便后续基于已封禁设备库在每一设备因子下的登录浮动度,来准确筛选出对应的参考设备因子,此时由于不断对登录设备进行封禁检测之后,会使已封禁设备库发生动态变化,那么已封禁设备库在每一设备因子下的登录浮动度也会随着发生动态变化,因此本实施例在将完成封禁的登录设备添加至已封禁设备库中,还需要采用与上述实施例中提供的对已封禁设备库在每一设备因子下的登录浮动度进行计算时的相同方式,来重新计算已封禁设备库在每一设备因子下的登录浮动度,以对每一设备因子下的登录浮动度进行动态更新,从而提高参考设备因子的筛选准确性。

[0066] 本实施例提供的技术方案,基于已封禁设备库在每一设备因子下的登录浮动度,可以从全部设备因子中筛选出对应的参考设备因子,进而通过分析登录设备和该已封禁设备库中每一已封禁设备在各个参考设备因子下的登录参数相似度,来计算该登录设备的被封禁评分,从而准确判断该登录设备是否需要被封禁的可能性,确保登录设备面向封禁检测的可靠性,无需对每一使用多开软件的登录设备进行封禁,或者对登录设备进行聚类封禁,在保证登录设备执行任何正常操作的基础上,避免封禁检测的滞后性,从而提高了登录设备面向封禁检测的准确性和封禁及时性;同时,参考完成封禁检测的目标登录设备集合下的封禁准确率和封禁召回率,动态更新对应的预设封禁阈值,进一步确保登录设备面向封禁检测的准确性,同时将完成封禁的登录设备不断添加至已封禁设备库中,并动态更新已封禁设备库在每一设备因子下的登录浮动度,进一步提高参考设备因子的筛选准确性。

[0067] 实施例四

[0068] 图4为本发明实施例四提供的一种登录设备的封禁检测装置的结构示意图,具体的,如图4所示,该装置可以包括:

[0069] 参考因子筛选模块410,用于基于已封禁设备库在每一设备因子下的登录浮动度,从各所述设备因子中筛选出对应的参考设备因子;

[0070] 封禁检测模块420,用于基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度,计算所述登录设备的被封禁评分。

[0071] 本实施例提供的技术方案,由于已封禁设备库在每一设备因子下的登录浮动越大,说明该设备因子被篡改的可能性越大,也就是该设备因子对登录设备进行封禁检测的参考价值越低,因此基于已封禁设备库在每一设备因子下的登录浮动度,可以从全部设备因子中筛选出对应的参考设备因子,进而通过分析登录设备和该已封禁设备库中每一已封禁设备在各个参考设备因子下的登录参数相似度,来计算该登录设备的被封禁评分,从而准确判断该登录设备是否需要被封禁的可能性,确保登录设备面向封禁检测的可靠性,无需对每一使用多开软件的登录设备进行封禁,或者对登录设备进行聚类封禁,在保证登录设备执行任何正常操作的基础上,避免封禁检测的滞后性,从而提高了登录设备面向封禁检测的准确性和封禁及时性。

[0072] 本实施例提供的登录设备的封禁检测装置可适用于上述任意实施例提供的登录设备的封禁检测方法,具备相应的功能和有益效果。

[0073] 实施例五

[0074] 图5为本发明实施例五提供的一种服务器的结构示意图,如图5所示,该服务器包括处理器50、存储装置51和通信装置52;服务器中处理器50的数量可以是一个或多个,图5中以一个处理器50为例;服务器中的处理器50、存储装置51和通信装置52可以通过总线或其他方式连接,图5中以通过总线连接为例。

[0075] 本实施例提供的一种服务器可用于执行上述任意实施例提供的登录设备的封禁检测方法,具备相应的功能和有益效果。

[0076] 实施例六

[0077] 本发明实施例六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可实现上述任意实施例中的登录设备的封禁检测方法。该方法具体可以包括:

[0078] 基于已封禁设备库在每一设备因子下的登录浮动度,从各所述设备因子中筛选出对应的参考设备因子;

[0079] 基于登录设备和所述已封禁设备库中每一已封禁设备在各所述参考设备因子下的登录参数相似度,计算所述登录设备的被封禁评分。

[0080] 当然,本发明实施例所提供的一种包含计算机可执行指令的存储介质,其计算机可执行指令不限于如上所述的方法操作,还可以执行本发明任意实施例所提供的登录设备的封禁检测方法中的相关操作。

[0081] 通过以上关于实施方式的描述,所属领域的技术人员可以清楚地了解到,本发明可借助软件及必需的通用硬件来实现,当然也可以通过硬件实现,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,该计算机软件产品可以存储在计算机可读存储介质中,如计算机的软盘、只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、闪存(FLASH)、硬盘或光盘等,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)执行本发明各个实施例所述的方法。

[0082] 值得注意的是,上述登录设备的封禁检测装置的实施例中,所包括的各个单元和模块只是按照功能逻辑进行划分的,但并不局限于上述的划分,只要能够实现相应的功能即可;另外,各功能单元的具体名称也只是为了便于相互区分,并不用于限制本发明的保护范围。

[0083] 以上所述仅为本发明的优选实施例,并不用于限制本发明,对于本领域技术人员而言,本发明可以有各种改动和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

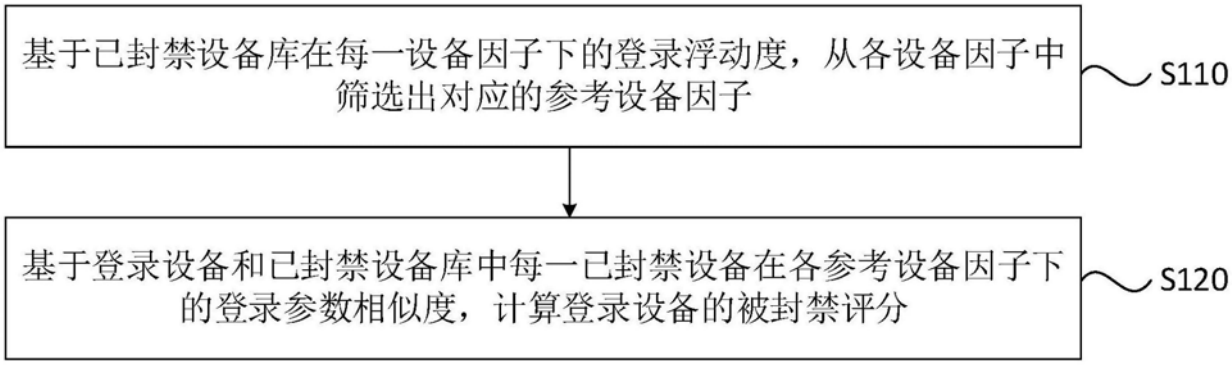

基于已封禁设备库在每一设备因子下的登录浮动度，从各设备因子中筛选出对应的参考设备因子
S110
基于登录设备和已封禁设备库中每一已封禁设备在各参考设备因子下的登录参数相似度，计算登录设备的被封禁评分
S120

图1A

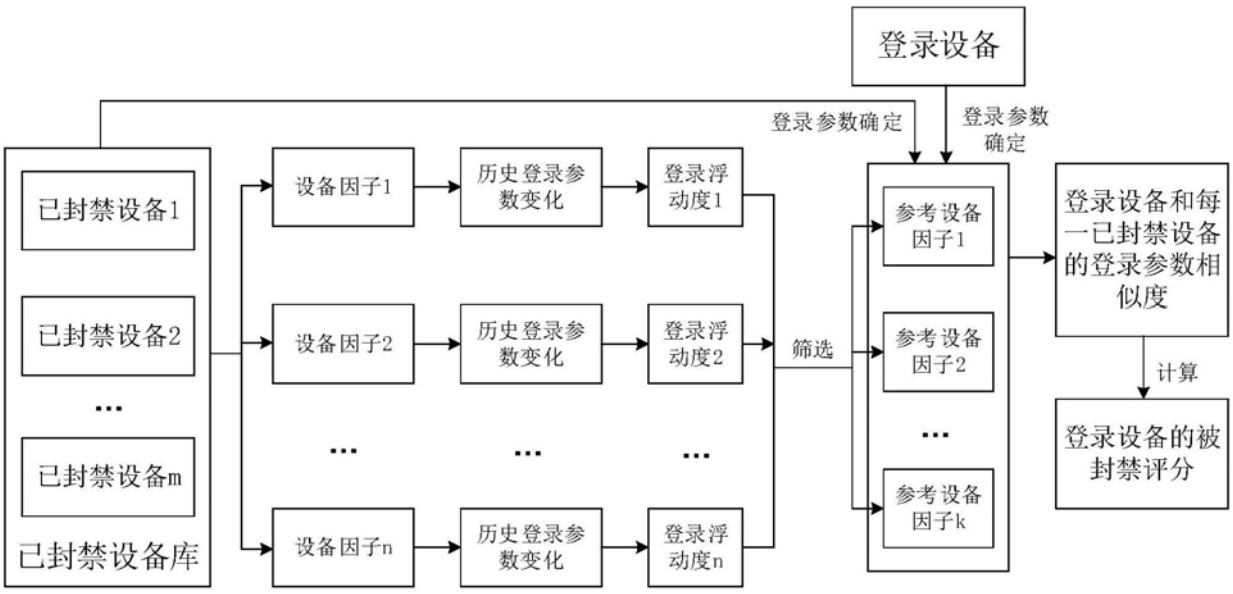

登录设备
登录参数确定
登录参数确定
已封禁设备1
已封禁设备2
...
已封禁设备m
已封禁设备库
设备因子1
设备因子2
...
设备因子n
历史登录参数变化
历史登录参数变化
...
历史登录参数变化
登录浮动度1
登录浮动度2
...
登录浮动度n
筛选
参考设备因子1
参考设备因子2
...
参考设备因子k
登录设备和每一已封禁设备的登录参数相似度
计算
登录设备的被封禁评分

图1B

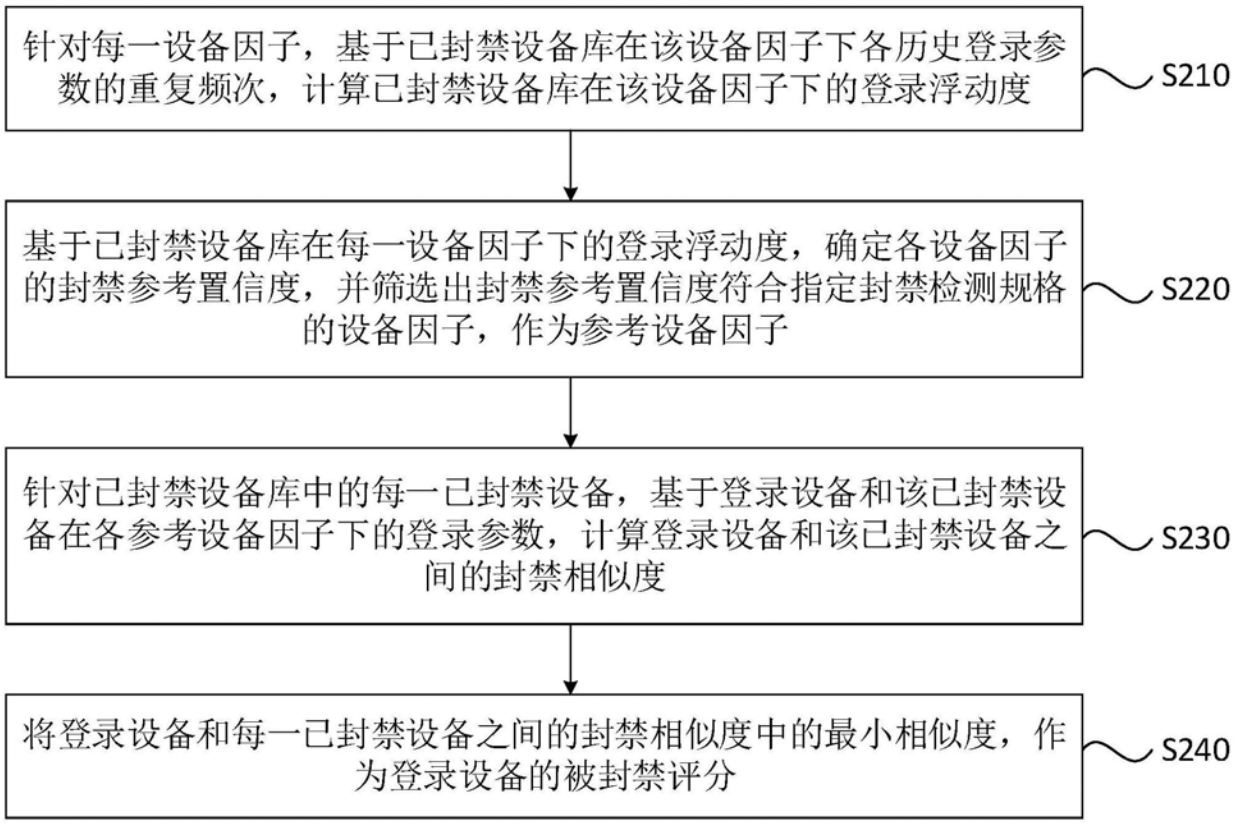

针对每一设备因子，基于已封禁设备库在该设备因子下各历史登录参数的重复频次，计算已封禁设备库在该设备因子下的登录浮动度
S210
基于已封禁设备库在每一设备因子下的登录浮动度，确定各设备因子的封禁参考置信度，并筛选出封禁参考置信度符合指定封禁检测规格的设备因子，作为参考设备因子
S220
针对已封禁设备库中的每一已封禁设备，基于登录设备和该已封禁设备在各参考设备因子下的登录参数，计算登录设备和该已封禁设备之间的封禁相似度
S230
将登录设备和每一已封禁设备之间的封禁相似度中的最小相似度，作为登录设备的被封禁评分
S240

图2A

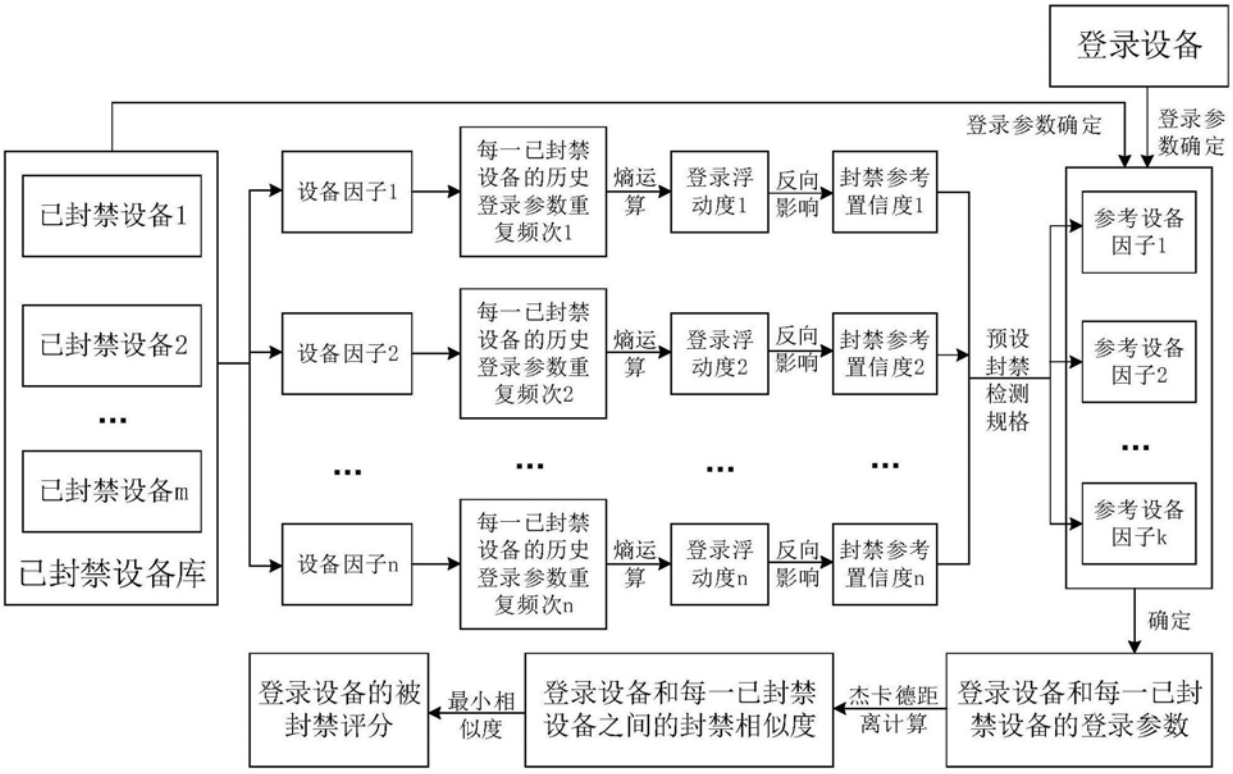

登录设备
登录参数确定
登录参数确定
已封禁设备1
已封禁设备2
...
已封禁设备m
已封禁设备库
设备因子1
设备因子2
...
设备因子n
每一已封禁设备的历史登录参数重复频次1
每一已封禁设备的历史登录参数重复频次2
每一已封禁设备的历史登录参数重复频次n
熵运算
登录浮动度1
登录浮动度2
登录浮动度n
反向影响
封禁参考置信度1
封禁参考置信度2
封禁参考置信度n
预设封禁检测规格
参考设备因子1
参考设备因子2
参考设备因子k
确定
登录设备和每一已封禁设备的登录参数
杰卡德距离计算
登录设备和每一已封禁设备之间的封禁相似度
最小相似度
登录设备的被封禁评分

图2B

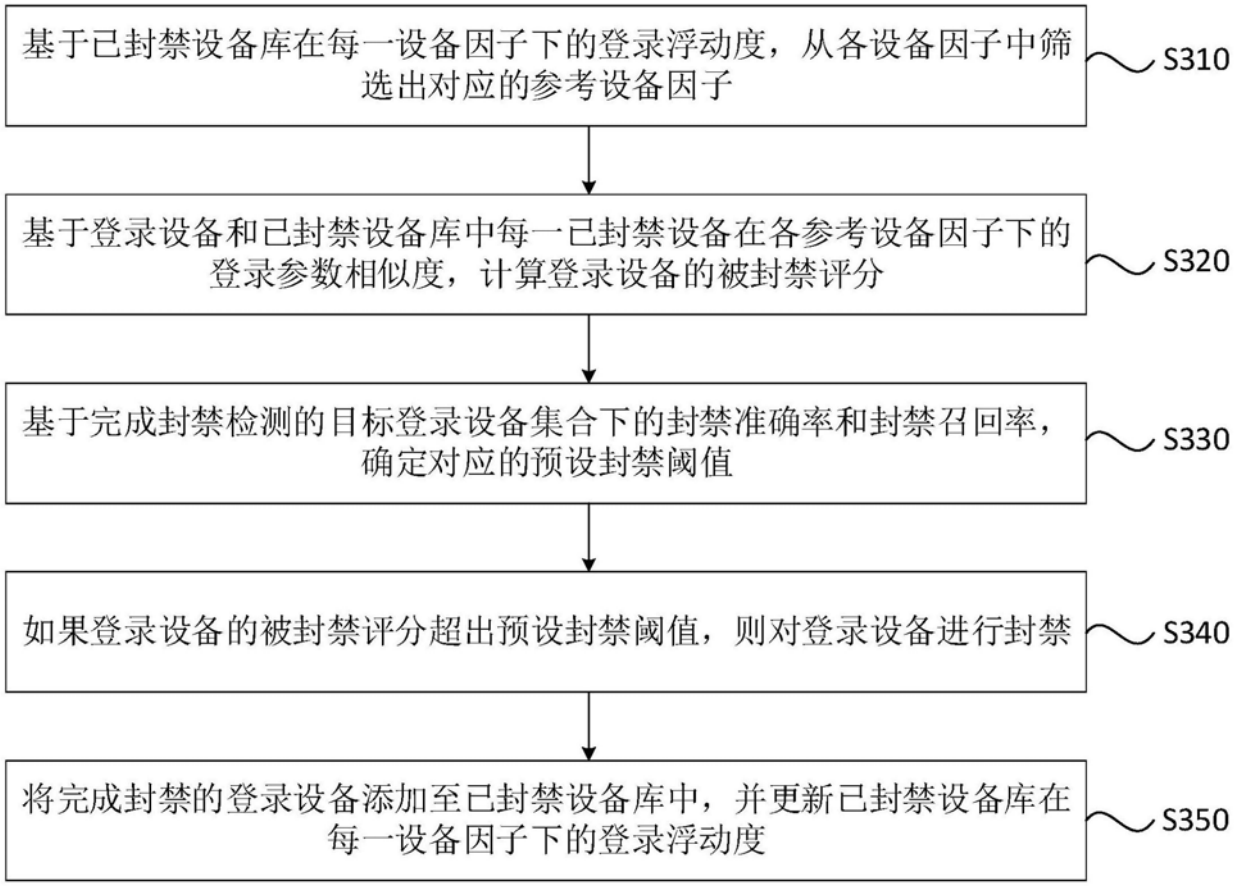

基于已封禁设备库在每一设备因子下的登录浮动度，从各设备因子中筛选出对应的参考设备因子
S310
基于登录设备和已封禁设备库中每一已封禁设备在各参考设备因子下的登录参数相似度，计算登录设备的被封禁评分
S320
基于完成封禁检测的目标登录设备集合下的封禁准确率和封禁召回率，确定对应的预设封禁阈值
S330
如果登录设备的被封禁评分超出预设封禁阈值，则对登录设备进行封禁
S340
将完成封禁的登录设备添加至已封禁设备库中，并更新已封禁设备库在每一设备因子下的登录浮动度
S350

图3A

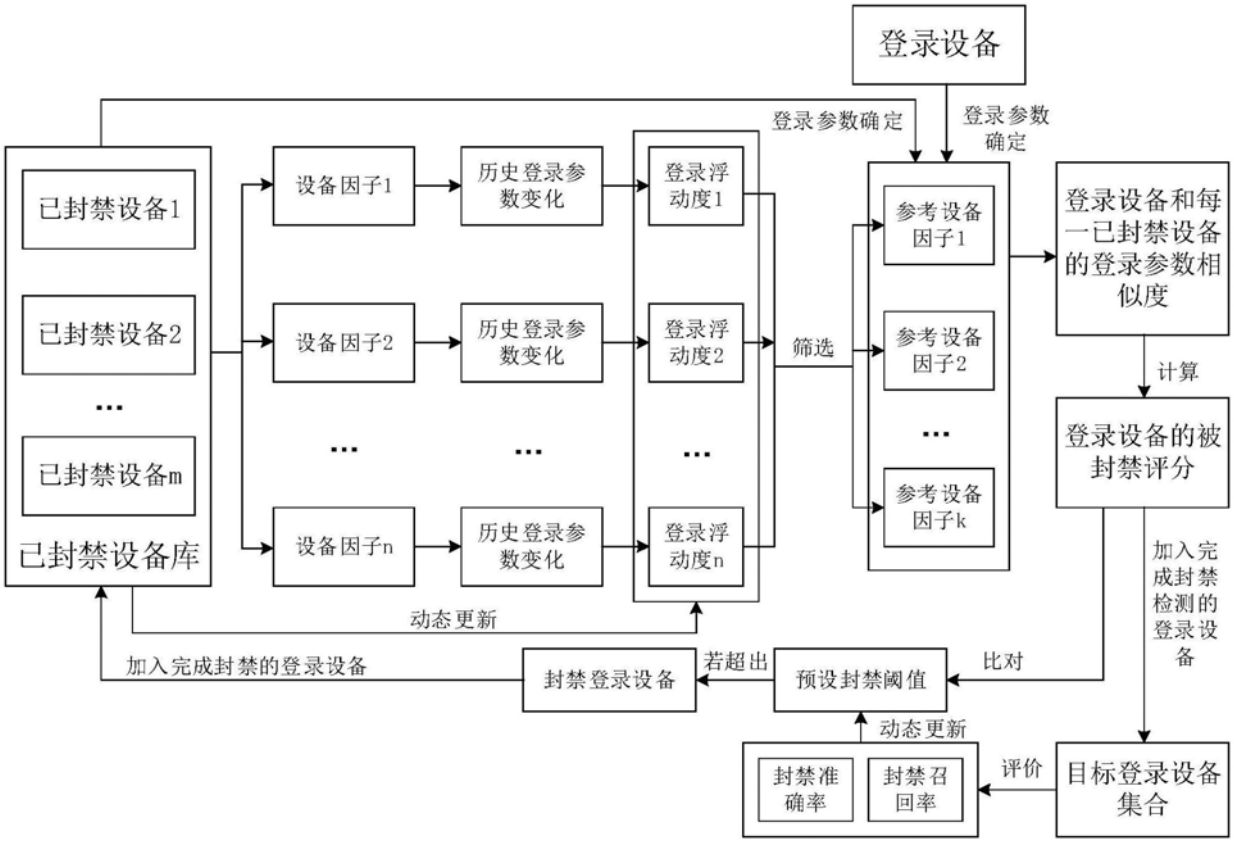

登录设备
登录参数确定
登录参数确定
已封禁设备1
已封禁设备2
...
已封禁设备m
已封禁设备库
设备因子1
设备因子2
...
设备因子n
历史登录参数变化
历史登录参数变化
...
历史登录参数变化
登录浮动度1
登录浮动度2
...
登录浮动度n
筛选
参考设备因子1
参考设备因子2
...
参考设备因子k
登录设备和每一已封禁设备的登录参数相似度
计算
登录设备的被封禁评分
加入完成封禁检测的登录设备
目标登录设备集合
评价
比对
预设封禁阈值
若超出
封禁登录设备
加入完成封禁的登录设备
动态更新
动态更新
封禁准确率
封禁召回率

图3B

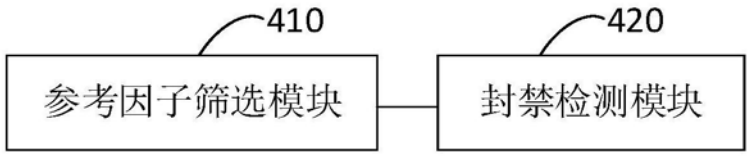

410
420
参考因子筛选模块
封禁检测模块

图4

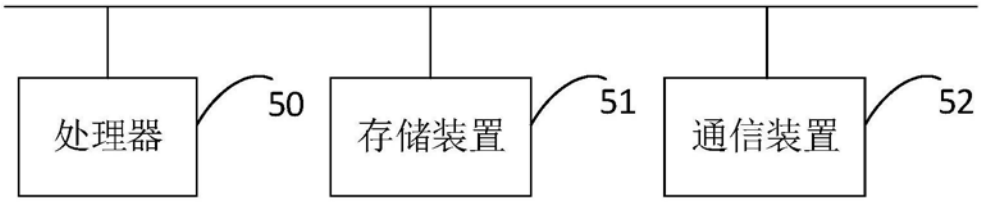

处理器
50
存储装置
51
通信装置
52

图5