(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 103369520 A
(43)申请公布日 2013.10.23

(21)申请号 201210084812.X

(22)申请日 2012.03.27

(71)申请人 百度在线网络技术(北京)有限公司
地址 100085 北京市海淀区上地十街 10 号百度大厦三层

(72)发明人 李厚辰 乜聚虎

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 宋合成

(51)Int.Cl.
H04W 12/00(2009.01)
H04L 29/08(2006.01)
G06F 21/56(2013.01)

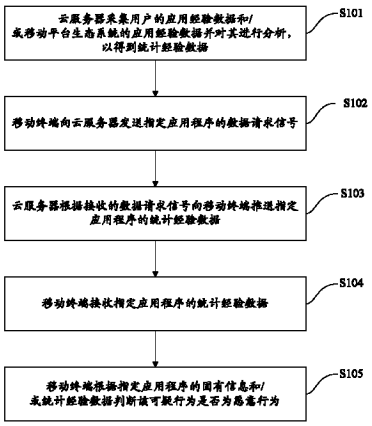
权利要求书4页 说明书11页 附图6页

(54)发明名称

移动终端的应用程序可疑行为的意图预判系统及方法

(57)摘要

本发明提出一种移动终端的应用程序可疑行为的意图预判系统,包括:云服务器,用于采集用户的应用经验数据和/或移动平台生态系统的应用经验数据,并对用户的应用经验数据和/或所述移动平台生态系统的应用经验数据进行分析以得到统计经验数据;移动终端,用于从云服务器下载指定应用程序的统计经验数据,并根据指定应用程序的统计经验数据对所述指定应用程序进行可疑行为的预判。本发明还提出了一种恶意行为检测及判定方法、云服务器及移动终端。本发明可以提高对恶意程序的监测和拦截能力,提升移动终端的安全性。



CN 103369520 A

1. 一种移动终端的应用程序可疑行为的意图预判系统，其特征在于，包括：

云服务器，用于采集用户的应用经验数据和/或移动平台生态系统的应用经验数据，并对所述用户的应用经验数据和/或所述移动平台生态系统的应用经验数据进行分析以得到统计经验数据；以及

移动终端，用于从所述云服务器下载指定应用程序的统计经验数据，并根据所述指定应用程序的统计经验数据对所述指定应用程序进行可疑行为的预判。

2. 如权利要求 1 所述的意图预判系统，其特征在于，所述云服务器包括：

提取模块，用于提取所述移动平台生态系统的应用经验数据和所述用户的应用经验数据，其中，所述移动平台生态系统的应用经验数据包括平台经验数据和平台数据可靠度，所述用户的应用经验数据包括用户经验数据和用户数据可靠度；

比较模块，用于对所述平台数据可靠度和所述用户数据可靠度进行比较；以及

输出模块，用于输出可靠度高的应用经验数据作为所述统计经验数据。

3. 如权利要求 2 所述的意图预判系统，其特征在于，所述云服务器还包括判断模块，所述判断模块用于判断所述用户的应用经验数据和所述移动平台生态系统的应用数据是否为空。

4. 如权利要求 3 所述的意图预判系统，其特征在于，所述输出模块还用于在所述用户的应用经验数据为空且所述移动平台生态系统的应用数据不为空时，将所述移动平台生态系统的应用数据作为所述统计经验数据输出，以及在所述移动平台生态系统的应用经验数据为空且所述用户的应用数据不为空时，将所述用户的应用数据作为所述统计经验数据输出。

5. 如权利要求 1-4 中任一项所述的意图预判系统，其特征在于，所述云服务器还包括：

检测模块，用于检测所述统计经验数据是否发生变化，以及在检测到变化时获取变化的统计经验数据对应的应用程序，并查询所述对应的应用程序的用户列表；

所述输出模块向所述用户列表中的用户推送变化后的统计经验数据。

6. 如权利要求 1 所述的意图预判系统，其特征在于，所述移动终端包括：

存储模块，用于存储应用程序的固有信息；

获取模块，用于向所述云服务器发送指定应用程序的数据请求信号，以及接收来自所述云服务器的所述指定应用程序的统计经验数据；

展示模块，用于向所述用户展示所述指定应用程序的固有信息和/或统计经验数据；

预判模块，用于根据所述指定应用程序的固有信息和/或统计经验数据对所述指定应用程序进行可疑行为的意图预判以判断所述可疑行为是否为恶意行为；

设置模块，用于根据意图判断结果设置所述指定应用程序对可疑行为的执行许可或执行警告。

7. 如权利要求 6 所述的意图预判系统，其特征在于，所述设置模块在所述预判模块判断所述可疑行为为恶意行为时，设置所述指定应用程序对所述可疑行为的执行警告；以及在所述预判模块判断所述可疑行为为非恶意行为时，设置所述指定应用程序对所述可疑行为的执行许可。

8. 如权利要求 1-7 中任一项所述的意图预判系统，其特征在于，所述移动终端还包括：

恶意行为特征模型库，用于存储恶意行为模型；

敏感资源监控模块，用于监控应用程序对敏感资源的访问以获得所述应用程序的行为数据；

行为采集模块，用于对所述敏感资源监控模块监控到的所述行为数据获得所述应用程序对所述敏感资源的可疑行为；

应用行为数据库，用于存储所述行为采集模块检测的所述可疑行为；

应用行为分析中心，用于接收来自所述行为采集模块的所述可疑行为，并调用所述恶意行为特征模型库中的恶意行为模型，以及将所述可疑行为与所述恶意行为模型进行匹配以判断所述可疑行为对应的行为是否为恶意行为；以及

应用安全中心，用于查询所述应用行为数据库中存储的所述可疑行为，以及当判断所述可疑行为为恶意行为后，以恶意程度对所述可疑行为所对应的应用程序访问进行排序，并设置所述应用程序访问的警告级别。

9. 一种移动终端的应用程序可疑行为的意图预判方法，其特征在于，包括如下步骤：

云服务器采集用户的应用经验数据和／或移动平台生态系统的应用经验数据，并对所述用户的应用经验数据和／或所述移动平台生态系统的应用经验数据进行分析以得到统计经验数据；

移动终端向所述云服务器发送指定应用程序的数据请求信号；

所述云服务器根据接收的数据请求信号向所述移动终端推送所述指定应用程序的统计经验数据，其中，所述统计经验数据为用户的应用经验数据或移动平台生态系统的应用经验数据；

所述移动终端接收所述指定应用程序的统计经验数据；以及

所述移动终端根据所述指定应用程序的固有信息和／或统计经验数据对所述指定应用程序进行可疑行为的意图预判以判断所述可疑行为是否为恶意行为。

10. 如权利要求 9 所述的意图预判方法，其特征在于，所述移动平台生态系统的应用经验数据包括平台经验数据和平台数据可靠度，所述用户的应用经验数据包括用户经验数据和用户数据可靠度。

11. 如权利要求 10 所述的意图预判方法，其特征在于，所述对所述用户的应用经验数据和／或所述移动平台生态系统的应用经验数据进行分析得到统计经验数据，还包括如下步骤：

判断所述用户的应用经验数据和所述移动平台生态系统的应用数据是否为空；

当所述用户的应用经验数据和所述移动平台生态系统的应用数据均不为空时，对所述移动平台数据可靠度和所述用户数据可靠度进行比较；

输出可靠度高的应用经验数据作为统计经验数据。

12. 如权利要求 11 所述的意图预判方法，其特征在于，在所述用户的应用经验数据为空且所述移动平台生态系统的应用数据不为空时，所述云服务器将所述移动平台生态系统的应用数据作为所述统计经验数据输出，

在所述移动平台生态系统的应用经验数据为空且所述用户的应用数据不为空时，所述云服务器将所述用户的应用数据作为所述统计经验数据输出。

13. 如权利要求 9-12 中任一项所述的意图预判方法，其特征在于，还包括如下步骤：

检测所述统计经验数据是否发生变化；

在检测到变化时，所述云服务器获取变化的统计经验数据对应的应用程序，并查询所述对应的应用程序的用户列表；

所述云服务器向所述用户列表中的用户推送变化后的统计经验数据。

14. 如权利要求 9 所述的意图预判方法，其特征在于，所述移动终端接收所述指定应用程序的统计经验数据后，还包括如下步骤

将所述指定应用程序的统计经验数据和 / 或所述指定应用程序的固有信息向用户展示。

15. 如权利要求 9 所述的意图预判方法，其特征在于，所述移动终端在判断所述可疑行为为恶意行为时，设置所述指定应用程序对所述可疑行为的执行警告；

在所述预判模块判断所述可疑行为为非恶意行为时，设置所述指定应用程序对所述可疑行为的执行许可。

16. 如权利要求 9-15 中任一项所述的意图预判方法，其特征在于，还包括如下步骤：

所述云服务器收集应用程序的应用行为数据，根据所述应用行为数据获取恶意行为特征数据并更新至移动终端；

所述移动终端监控应用程序对敏感资源的访问以获得所述应用程序的行为数据并根据所述行为数据获得所述应用程序对应的可疑行为，以及将所述可疑行为与预设的恶意行为模型进行匹配以判断所述可疑行为是否为恶意行为，其中，所述敏感资源为恶意行为对应的应用程序访问的资源，所述恶意行为模型根据所述恶意行为特征数据建立；以及

所述移动终端在判断所述可疑行为为恶意行为后，以恶意程度对所述可疑行为所对应的应用程序访问进行排序，并设置所述应用程序访问的警告级别。

17. 一种云服务器，其特征在于，包括：

提取模块，用于提取移动平台生态系统的应用经验数据和所述用户的应用经验数据，其中，所述移动平台生态系统的应用经验数据包括平台经验数据和平台数据可靠度，所述用户的应用经验数据包括用户经验数据和用户数据可靠度；

比较模块，用于对所述平台数据可靠度和所述用户数据可靠度进行比较；以及

输出模块，用于输出可靠度高的应用经验数据作为所述统计经验数据。

18. 如权利要求 17 所述的云服务器，其特征在于，还包括：

判断模块，用于判断所述用户的应用经验数据和所述移动平台生态系统的应用数据是否为空。

19. 如权利要求 18 所述的云服务器，其特征在于，所述输出模块还用于在所述用户的应用经验数据为空且所述移动平台生态系统的应用数据不为空时，将所述移动平台生态系统的应用数据作为所述统计经验数据输出，以及在所述移动平台生态系统的应用经验数据为空且所述用户的应用数据不为空时，将所述用户的应用数据作为所述统计经验数据输出。

20. 如权利要求 17-19 中任一项所述的云服务器，其特征在于，还包括：

检测模块，用于检测所述统计经验数据是否发生变化，以及在检测到变化时获取变化的统计经验数据对应的应用程序，并查询所述对应的应用程序的用户列表，且所述输出模块向所述用户列表中的用户推送变化后的统计经验数据。

21. 一种移动终端，其特征在于，包括：

存储模块，用于存储应用程序的固有信息；

获取模块，用于向所述云服务器发送指定应用程序的数据请求信号，以及接收来自所述云服务器的所述指定应用程序的统计经验数据；

展示模块，用于向所述用户展示所述指定应用程序的固有信息和/或统计经验数据；

预判模块，用于根据所述指定应用程序的固有信息和/或统计经验数据对所述指定应用程序进行可疑行为的意图预判以判断所述可疑行为是否为恶意行为；

设置模块，用于根据意图判断结果设置所述指定应用程序对可疑行为的执行许可或执行警告。

22. 如权利要求 21 所述的移动终端，其特征在于，所述设置模块还用于在所述预判模块判断所述可疑行为为恶意行为时，设置所述指定应用程序对所述可疑行为的执行警告，以及在所述预判模块判断所述可疑行为为非恶意行为时，设置所述指定应用程序对所述可疑行为的执行许可。

23. 如权利要求 21 或 22 所述的移动终端，其特征在于，所述移动终端还包括：

恶意行为特征模型库，用于存储恶意行为模型；

敏感资源监控模块，用于监控应用程序对敏感资源的访问以获得所述应用程序的行为数据；

行为采集模块，用于对所述敏感资源监控模块监控到的所述行为数据获得所述应用程序对所述敏感资源的可疑行为；

应用行为数据库，用于存储所述行为采集模块检测的所述可疑行为；

应用行为分析中心，用于接收来自所述行为采集模块的所述可疑行为，并调用所述恶意行为特征模型库中的恶意行为模型，以及将所述可疑行为与所述恶意行为模型进行匹配以判断所述可疑行为对应的行为是否为恶意行为；以及

应用安全中心，用于查询所述应用行为数据库中存储的所述可疑行为，以及当判断所述可疑行为为恶意行为后，以恶意程度对所述可疑行为所对应的应用程序访问进行排序，并设置所述应用程序访问的警告级别。

移动终端的应用程序可疑行为的意图预判系统及方法

技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种移动终端的应用程序可疑行为的意图预判系统及方法。

背景技术

[0002] 随着智能手机等移动智能终端功能的日益强大，移动智能终端应用软件数量激增，移动智能终端用户数量快速增多。但随之而来的是，带有恶意行为的应用程序也越来越多，令人防不胜防。这些应用程序的恶意行为主要有：恶意扣费或消耗套餐，窃取用户隐私资料，无提示联网下载软件，大量传播恶意软件等。如何防范这些恶意程序已经成为亟待解决的问题。

[0003] 各手机操作系统平台对现有的用程序进行资源访问控制的技术具体包括以下几种：

[0004] (1)Android 平台的资源访问控制机制：

[0005] 在应用安装时，向用户展示应用程序所声明其所需要的权限，用户确定安装该应用则说明用户允许该应用程序使用这些权限，允许应用程序访问这些权限相对应的资源，应用安装成功后，其应用程序信息中就包含了其所声明的权限；

[0006] 应用程序运行时，访问敏感资源时，系统会去判断该应用程序信息中是否包含有相应的权限，若有相应的权限则直接允许应用程序访问该资源，若没有相应的权限则系统抛出安全异常迫使应用程序停止运行来禁止应用程序访问该资源。

[0007] (2)Symbian 系统通过对系统中的敏感资源进行分类，相对应的定义一些能力来控制敏感资源的访问，应用程序通过声明一些能力来请求用户赋予其访问某些敏感信息的能力。这些敏感资源的分类比较粗略，相应的能力指代的可访问资源的范围较广。

[0008] 以上各平台都无法避免以下的技术缺陷：

[0009] (1)Android 暴露给用户应用程序能力信息太粗略，用户只能通过这些暴露出来的应用程序信息对应用程序可能发生的恶意行为进行预判，然而预判的难度非常大并且精确度极低。Android 系统只提供了一种方式，让用户大致了解应用程序的能力，就是应用程序安装包中包含声明需要使用某些权限，并且在安装成功之后可以查看应用程序使用了哪些权限。然而用户很难从粗略的权限描述上了解到应用程序的可疑行为意图。用户在安装应用是和运行应用程序之前很难知道该应用程序是否有可能发生恶意行为。

[0010] (2)Symbian 系统的应用程序能力控制模型与 android 的类似，同样是暴露给用户应用程序能力信息太粗略，用户只能通过这些暴露出来的应用程序信息对应用程序可能发生的恶意行为进行预判，然而预判的难度非常大并且精确度极低。

[0011] 也就是说，现有的手机终端系统，存在着在应用程序执行恶意行为并且被用户发现之前，未能获知应用程序存在恶意行为意图的问题。

发明内容

[0012] 本发明的目的旨在至少解决上述技术缺陷之一。

[0013] 为此，本发明的第一个目的在于提出一种移动终端的应用程序可疑行为的意图预判系统，可以使用户可以在应用程序执行之前，提前获知应用程序的可疑行为信息，并对应用程序进行预判断，提高对恶意程序的监测和拦截能力，提升移动终端的安全性。本发明的第二个目的在于提出一种移动终端的应用程序可疑行为的意图预判方法。本发明的第三个目的在于提出一种云服务器。本发明的第四个目的在于提出一种移动终端。

[0014] 为达到上述目的，本发明第一方面的实施例提出一种移动终端的应用程序可疑行为的意图预判系统，包括：云服务器，用于采集用户的应用经验数据和/或移动平台生态系统的应用经验数据，并对所述用户的应用经验数据和/或所述移动平台生态系统的应用经验数据进行分析以得到统计经验数据；移动终端，用于从所述云服务器下载指定应用程序的统计经验数据，并根据所述指定应用程序的统计经验数据对所述指定应用程序进行可疑行为的预判。

[0015] 根据本发明实施例的移动终端的应用程序可疑行为的意图预判系统，可使用户可以在应用程序执行之前，提前获知应用程序的可疑行为信息，并对应用程序进行预判断，提高对恶意程序的监测和拦截能力，提升移动终端的安全性。另一方面，利用云服务器采集应用程序的应用行为数据，并通过对应用行为数据的分析获取可疑行为特征数据，并且实现云服务器和移动终端的数据同步，从而为移动终端判断应用程序的敏感行为是否为可疑行为提供更充分的依据，提高了移动终端的恶意行为预防和监测能力。

[0016] 本发明第二方面的实施例还提出了一种移动终端的应用程序可疑行为的意图预判方法，包括如下步骤：

[0017] 云服务器采集用户的应用经验数据和/或移动平台生态系统的应用经验数据，并对用户的应用经验数据和/或移动平台生态系统的应用经验数据进行分析以得到统计经验数据；

[0018] 移动终端向云服务器发送指定应用程序的数据请求信号；

[0019] 云服务器根据接收的数据请求信号向所述移动终端推送所述指定应用程序的统计经验数据，其中，统计经验数据为用户的应用经验数据或移动平台生态系统的应用经验数据；

[0020] 移动终端接收指定应用程序的统计经验数据；以及

[0021] 移动终端根据指定应用程序的固有信息和/或统计经验数据对指定应用程序进行可疑行为的意图预判以判断可疑行为是否为恶意行为。

[0022] 根据本发明实施例的移动终端的应用程序可疑行为的意图预判方法，可使用户可以在应用程序执行之前，提前获知应用程序的可疑行为信息，并对应用程序进行预判断，提高对恶意程序的监测和拦截能力，提升移动终端的安全性。另一方面，利用云服务器采集应用程序的应用行为数据，并通过对应用行为数据的分析获取可疑行为特征数据，并且实现云服务器和移动终端的数据同步，从而为移动终端判断应用程序的敏感行为是否为可疑行为提供更充分的依据，提高了移动终端的恶意行为预防和监测能力。

[0023] 本发明第三方面的实施例提出一种云服务器，包括：提取模块，用于提取移动平台生态系统的应用经验数据和所述用户的应用经验数据，其中，所述移动平台生态系统的应用经验数据包括平台经验数据和平台数据可靠度，所述用户的应用经验数据包括用户经验

数据和用户数据可靠度；比较模块，用于对所述平台数据可靠度和所述用户数据可靠度进行比较；以及输出模块，用于输出可靠度高的应用经验数据作为所述统计经验数据。

[0024] 根据本发明实施例的云服务器，采集应用程序的应用行为数据，并通过对应用行为数据的分析获取可疑行为特征数据，并且实现云服务器和移动终端的数据同步，从而为移动终端判断应用程序的敏感行为是否为可疑行为提供更充分的依据。

[0025] 本发明第四方面的实施例提出一种移动终端，包括：存储模块，用于存储应用程序的固有信息；获取模块，用于向所述云服务器发送指定应用程序的数据请求信号，以及接收来自所述云服务器的所述指定应用程序的统计经验数据；展示模块，用于向所述用户展示所述指定应用程序的固有信息和/或统计经验数据；预判模块，用于根据所述指定应用程序的固有信息和/或统计经验数据对所述指定应用程序进行可疑行为的意图预判以判断所述可疑行为是否为恶意行为；设置模块，用于根据意图判断结果设置所述指定应用程序对可疑行为的执行许可或执行警告。

[0026] 根据本发明实施例的移动终端，可使用户可以在应用程序执行之前，提前获知应用程序的可疑行为信息，并对应用程序进行预判断，提高对恶意程序的监测和拦截能力，提升移动终端的安全性。

[0027] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0028] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0029] 图 1 为本发明实施例的移动终端的应用程序可疑行为的意图预判系统的示意图；

[0030] 图 2 为本发明实施例的移动终端的应用程序可疑行为的意图预判方法的流程图；

[0031] 图 3 为本发明实施例的云服务器统计经验数据的流程图；

[0032] 图 4 为本发明实施例的云服务器向移动终端推送统计经验数据的流程图；

[0033] 图 5 为本发明实施例的移动终端向云服务器查询应用程序可疑行为的意图并进行预判的流程图；

[0034] 图 6 为本发明实施的云服务器的示意图；以及

[0035] 图 7 为本发明实施例的移动终端的示意图。

具体实施方式

[0036] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0037] 下文的公开提供了许多不同的实施例或例子用来实现本发明的不同结构。为了简化本发明的公开，下文中对特定例子的部件和设置进行描述。当然，它们仅仅为示例，并且目的不在于限制本发明。此外，本发明可以在不同例子中重复参考数字和/或字母。这种重复是为了简化和清楚的目的，其本身不指示所讨论各种实施例和/或设置之间的关系。此外，本发明提供了的各种特定的工艺和材料的例子，但是本领域普通技术人员可以意识到

其他工艺的可应用于性和 / 或其他材料的使用。另外，以下描述的第一特征在第二特征之“上”的结构可以包括第一和第二特征形成为直接接触的实施例，也可以包括另外的特征形成在第一和第二特征之间的实施例，这样第一和第二特征可能不是直接接触。

[0038] 参照下面的描述和附图，将清楚本发明的实施例的这些和其他方面。在这些描述和附图中，具体公开了本发明的实施例中的一些特定实施方式，来表示实施本发明的实施例的原理的一些方式，但是应当理解，本发明的实施例的范围不受此限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0039] 下面参照附图详细描述根据本发明实施例的移动终端的应用程序可疑行为的意图预判系统。

[0040] 如图 1 所示，本发明实施例的移动终端的应用程序可疑行为的意图预判系统，包括 :云服务器 100 和移动终端 200。其中，云服务器 100 用于采集用户的应用经验数据和 / 或移动平台生态系统的应用经验数据，并对用户的应用经验数据和 / 或移动平台生态系统的应用经验数据进行分析以得到统计经验数据。移动终端 200 用于从云服务器 100 下载指定应用程序的统计经验数据，并根据指定应用程序的统计经验数据对该指定应用程序进行可疑行为的预判。

[0041] 如图 1 所示，云服务器 100 包括 :提取模块 101、比较模块 102 和输出模块 103。其中，提取模块 101 用于提取移动平台生态系统的应用经验数据和用户的应用经验数据。具体地，云服务器 100 提取应用经验数据包括以下两个来源 :

[0042] (1) 移动终端应用程序的审核团队对最新产生的应用进行审核时，对应用程序的安全进行着重审核时，也会得到能够带来安全保障的设置和判定数据，这是数据可以作为移动平台生态系统的应用经验数据。其中，移动平台生态系统的应用经验数据可以包括移动平台生态系统经验数据 e1 和平台数据可靠度 t1。移动平台生态系统经验数据为审核团队在使用应用程序过程中的经验数据，平台数据可靠度为移动生态系统提供的应用经验数据的可靠性程度。

[0043] (2) 其它用户在使用应用程序过程中做出的设置和判定数据，然后这些设置和判定数据作为用户的应用经验数据被同步到云服务器 100 上。其中，用户的应用经验数据可以包括用户经验数据 e2 和用户数据可靠度 t2。用户经验数据为用户在使用应用程序过程中的经验数据，用户数据可靠度为用户提供的应用经验数据的可靠性程度。

[0044] 在本发明的一个实施例中，云服务器 100 还进一步包括 :判断模块 104，用于判断用户的应用经验数据和移动平台生态系统的应用数据是否为空。如果判断模块 104 判断用户的应用经验数据 e2 为空且移动平台生态系统的应用数据 e1 不为空时，即云服务器 100 仅接收到来自移动平台生态系统的应用数据 e1，则输出模块 103 将移动平台生态系统的应用数据 e1 作为统计经验数据输出。

[0045] 如果判断模块 104 判断移动平台生态系统的应用经验数据 e1 为空且用户的应用数据 e2 不为空时，即云服务器 100 仅接收到来自用户的应用经验数据 e2，将输出模块 103 用户的应用数据 e2 作为所述统计经验数据输出。

[0046] 如果用户的应用经验数据 e2 和移动平台生态系统的应用数据 e1 均不为空，则由比较模块 102 对平台数据可靠度 t1 和用户数据可靠度 t2 进行比较。输出模块 103 根据比较结果输出可靠度高的应用经验数据作为统计经验数据。

[0047] 在本发明的一个实施例中，云服务器 100 还进一步包括检测模块 105，检测模块 105 用于检测统计经验数据是否发生变化，在检测到某个应用程序的统计经验数据变化时获取变化的统计经验数据对应的应用程序，并查询对应的应用程序的用户列表。然后由输出模块 103 向用户列表中的用户推送变化后的统计经验数据。移动终端 200 在接收到上述统计经验数据后，可以直接应用云服务器 100 推送的数据到系统中，也可以将上述统计经验数据显示给用户，由用户判断是否需要应用该统计经验数据。

[0048] 由此，云服务器 100 可以在检测到应用程序的统计经验数据变化时，主动向使用该应用程序的用户推送更新信息。便于用户的手机终端可以实时的更新到最新的恶意行为信息，及时地对手机上的应用程序的恶意行为进行判断以及修正。

[0049] 如图 1 所示，移动终端 200 包括 ：存储模块 201、获取模块 202、展示模块 203、预判模块 204 和设置模块 205。其中，存储模块 201 用于存储应用程序的固有信息。在本发明的一个示例中，固有信息包括应用程序的名称、版本号、简介等。获取模块 202 用于向云服务器 100 发送指定应用程序的数据请求信号，以及接收来自云服务器 100 的指定应用程序的统计经验数据。展示模块 203 用于向用户展示指定应用程序的固有信息和 / 或统计经验数据。其中，如果云服务器 100 中未存储有该指定应用程序的统计经验数据，则只向用户展示应用程序的固有信息。

[0050] 预判模块 204 根据指定应用程序的固有信息和 / 或统计经验数据对指定应用程序进行可疑行为的意图预判以判断可疑行为是否为恶意行为。设置模块 205 根据意图判断结果设置指定应用程序对可疑行为的执行许可或执行警告。

[0051] 在本发明的一个实施例中，设置模块 205 在预判模块 204 判断可疑行为为恶意行为时，设置指定应用程序对该可疑行为的执行警告 ；在预判模块 204 判断可疑行为为非恶意行为时，设置指定应用程序对该可疑行为的执行许可。

[0052] 在本发明的一个实施例中，移动终端还进一步包括 ：恶意行为特征模型库、敏感资源监控模块、行为采集模块、应用行为数据库、应用行为分析中心和应用安全中心。其中，恶意行为特征模型库用于存储恶意行为模型。敏感资源监控模块用于监控应用程序对敏感资源的访问以获得应用程序的行为数据。行为采集模块用于对敏感资源监控模块监控到的行为数据获得应用程序对敏感资源的可疑行为。应用行为数据库用于存储行为采集模块检测的可疑行为。应用行为分析中心用于接收来自行为采集模块的可疑行为，并调用恶意行为特征模型库中的恶意行为模型，以及将可疑行为与恶意行为模型进行匹配以判断可疑行为对应的行为是否为恶意行为。应用安全中心用于查询应用行为数据库中存储的可疑行为，以及当判断可疑行为为恶意行为后，按照恶意程度对该可疑行为所对应的应用程序访问进行排序，并设置该应用程序访问的警告级别。

[0053] 其中，预判模块 204 可以集成于应用行为分析中心，根据指定应用程序的固有信息和 / 或统计经验数据对指定应用程序进行可疑行为的意图预判以判断可疑行为是否为恶意行为。设置模块 205 可以集成于应用安全中心，根据意图判断结果设置指定应用程序对可疑行为的执行许可或执行警告。

[0054] 根据本发明实施例的移动终端的应用程序可疑行为的意图预判系统，可使用户可以在应用程序执行之前，提前获知应用程序的可疑行为信息，并对应用程序进行预判断，提高对恶意程序的监测和拦截能力，提升移动终端的安全性。另一方面，利用云服务器采集应

用程序的应用行为数据，并通过对应用行为数据的分析获取可疑行为特征数据，并且实现云服务器和移动终端的数据同步，从而为移动终端判断应用程序的敏感行为是否为可疑行为提供更充分的依据，提高了移动终端的恶意行为预防和监测能力。

[0055] 参见图 2，本发明实施例提出了一种移动终端的应用程序可疑行为的意图预判方法，包括如下步骤：

[0056] S101：云服务器采集用户的应用经验数据和 / 或移动平台生态系统的应用经验数据，并对用户的应用经验数据和 / 或所述移动平台生态系统的应用经验数据进行分析以得到统计经验数据。

[0057] 具体地，云服务器提取应用经验数据包括以下两个来源：

[0058] (1) 移动终端应用程序的审核团队对最新产生的应用进行审核时，对应用程序的安全进行着重审核时，也会得到能够带来安全保障的设置和判定数据，这是数据可以作为移动平台生态系统的应用经验数据。其中，移动平台生态系统的应用经验数据可以包括移动平台生态系统经验数据 e1 和平台数据可靠度 t1。移动平台生态系统经验数据为审核团队在使用应用程序过程中的经验数据，平台数据可靠度为移动生态系统提供的应用经验数据的可靠性程度。

[0059] (2) 其它用户在使用应用程序过程中做出的设置和判定数据，然后这些设置和判定数据作为用户的应用经验数据被同步到云服务器上。其中，用户的应用经验数据可以包括用户经验数据 e2 和用户数据可靠度 t2。用户经验数据为用户在使用应用程序过程中的经验数据，用户数据可靠度为用户提供的应用经验数据的可靠性程度。

[0060] 下面参考图 3 对云服务器获取统计经验数据的过程进行描述。

[0061] S301：判断是否有来自移动平台生态系统的应用经验数据，如果有，则执行步骤 S302，否则执行步骤 S303。

[0062] S302，提取来自移动平台生态系统的应用经验数据，包括移动平台生态系统经验数据 e1 和平台数据可靠度 t1。

[0063] S303：如果没有来自移动平台生态系统的应用经验数据，则判断移动平台生态系统经验数据 e1 为空，然后执行步骤 S304。

[0064] S304：判断是否有来自用户的设置和判定，如果有，则执行步骤 S305，否则执行 S307。

[0065] S305：提取出现几率最高的设置和判断数据，作为来自用户的应用经验数据。

[0066] S306：提取来自用户的应用经验数据，包括：用户经验数据 e2 和用户数据可靠度 t2。

[0067] S307：如果判断没有来自用户的设置和判定，则判断用户经验数据 e2 为空。

[0068] S308：判断移动平台生态系统经验数据 e1 是否不为空，如果是，则执行 S309，否则执行 S313。

[0069] S309：判断用户经验数据 e2 是否不为空，如果是，则执行 S310，否则执行 S311。

[0070] S310：判断平台数据可靠度 t1 是否高于用户数据可靠度 t2，如果是，则执行 S311，否则执行 S313。

[0071] S311：将 e1 作为统计经验数据。

[0072] S312：将 e2 作为统计经验数据。

[0073] S313：输出统计经验数据。

[0074] 如图 4 所示，云服务器还可以在检测到统计经验数据发生变化时，主动向对应的移动终端推送变化的统计经验数据。

[0075] S401：云服务器检测统计经验数据是否发生变化，如果检测到某个应用程序的统计经验数据发生了变化，继续向下执行 S402。

[0076] S402：云服务器获取变化的统计经验数据对应的应用程序，并查询对应的应用程序的用户列表。

[0077] S403：云服务器向用户列表中的指定用户推送变化后的统计经验数据。

[0078] S404：用户终端接收变化后的统计经验数据。

[0079] S405：检查用户设置是否设置为：默认许可云服务器直接将统计经验数据推送至移动终端，如果是，则执行 S407，否则执行 S406。

[0080] S406：移动终端直接对应用程序的指定行为作出预判。

[0081] S407：将指定应用程序的统计经验数据和 / 或指定应用程序的固有信息向用户展示。

[0082] S408：用户查看收到的统计经验数据和 / 或固有信息，并对应用程序的指定行为作出预判。

[0083] 由此，云服务器可以在检测到应用程序的统计经验数据变化时，主动向使用该应用程序的用户推送更新信息。便于用户的手机终端可以实时的更新到最新的恶意行为信息，及时地对手机上的应用程序的恶意行为进行判断以及修正。

[0084] S102：移动终端向云服务器发送指定应用程序的数据请求信号。

[0085] 移动终端在应用程序安装时和用户通过系统软件主动发起请求时，会向云服务器发送应用程序可疑行为的统计经验数据的查询请求，请求获取当前最新的应用程序可疑行为的统计经验数据，便于立即对应用程序潜在的恶意行为进行预判。

[0086] S103：云服务器根据接收的数据请求信号向移动终端推送指定应用程序的统计经验数据。其中，统计经验数据为用户的应用经验数据或移动平台生态系统的应用经验数据。

[0087] S104：移动终端接收指定应用程序的统计经验数据。

[0088] S105：移动终端根据指定应用程序的固有信息和 / 或统计经验数据对指定应用程序进行可疑行为的意图预判，以判断该可疑行为是否为恶意行为。

[0089] 下面参考图 5 对移动终端根据统计经验数据进行安全控制的过程进行说明。

[0090] S501：移动终端向云服务器请求获取指定应用程序的所有统计经验数据。

[0091] S502：判断统计经验数据是否不为空，如果是，则执行 S503，否则执行 S504。

[0092] S503：向用户展示上述统计经验数据和应用程序的固有信息。

[0093] S504：向用户展示应用程序的固有信息。

[0094] S505：对应用程序进行可疑行为意图预判。

[0095] S506：设置应用程序对可疑行为的执行操作。

[0096] 移动终端在判断可疑行为为恶意行为时，设置指定应用程序对所述可疑行为的执行警告；在判断可疑行为为非恶意行为时，设置指定应用程序对所述可疑行为的执行许可。

[0097] 在本发明的一个实施例中的移动终端的应用程序可疑行为的意图预判方法，还进一步包括：云服务器收集应用程序的应用行为数据，根据应用行为数据获取恶意行为特征

数据并更新至移动终端。移动终端监控应用程序对敏感资源的访问以获得应用程序的行为数据并根据行为数据获得应用程序对应的可疑行为，以及将可疑行为与预设的恶意行为模型进行匹配以判断所述可疑行为是否为恶意行为。其中，敏感资源为恶意行为对应的应用程序访问的资源，恶意行为模型根据所述恶意行为特征数据建立。移动终端在判断可疑行为为恶意行为后，以恶意程度对可疑行为所对应的应用程序访问进行排序，并设置应用程序访问的警告级别。

[0098] 根据本发明实施例的可疑行为检测及判定方法，可使用户可以在应用程序执行之前，提前获知应用程序的可疑行为信息，并对应用程序进行预判断，监测和拦截能力，提升移动终端的安全性。另一方面，利用云服务器采集应用程序的应用行为数据，并通过对应用行为数据的分析获取可疑行为特征数据，并且实现云服务器和移动终端的数据同步，从而为移动终端判断应用程序的敏感行为是否为可疑行为提供依据，提高了移动终端的恶意行为预防和监测能力。

[0099] 下面参考图 6 描述根据本发明实施例的云服务器。

[0100] 如图 6 所示，本发明实施例的云服务器 100 包括：提取模块 101、比较模块 102 和输出模块 103。其中，提取模块 101 用于提取移动平台生态系统的应用经验数据和用户的应用经验数据。具体地，云服务器 100 提取应用经验数据包括以下两个来源：

[0101] (1) 移动终端应用程序的审核团队对最新产生的应用进行审核时，对应用程序的安全进行着重审核时，也会得到能够带来安全保障的设置和判定数据，这是数据可以作为移动平台生态系统的应用经验数据。其中，移动平台生态系统的应用经验数据可以包括移动平台生态系统经验数据 e1 和平台数据可靠度 t1。移动平台生态系统经验数据为审核团队在使用应用程序过程中的经验数据，平台数据可靠度为移动生态系统提供的应用经验数据的可靠性程度。

[0102] (2) 其它用户在使用应用程序过程中做出的设置和判定数据，然后这些设置和判定数据作为用户的应用经验数据被同步到云服务器 100 上。其中，用户的应用经验数据可以包括用户经验数据 e2 和用户数据可靠度 t2。用户经验数据为用户在使用应用程序过程中的经验数据，用户数据可靠度为用户提供的应用经验数据的可靠性程度。

[0103] 在本发明的一个实施例中，云服务器 100 还进一步包括：判断模块 104，用于判断用户的应用经验数据和移动平台生态系统的应用数据是否为空。如果判断模块 104 判断用户的应用经验数据 e2 为空且移动平台生态系统的应用数据 e1 不为空时，即云服务器 100 仅接收到来自移动平台生态系统的应用数据 e1，则输出模块 103 将移动平台生态系统的应用数据 e1 作为统计经验数据输出。

[0104] 如果判断模块 104 判断移动平台生态系统的应用经验数据 e1 为空且用户的应用数据 e2 不为空时，即云服务器 100 仅接收到来自用户的应用经验数据 e2，将输出模块 103 用户的应用数据 e2 作为所述统计经验数据输出。

[0105] 如果用户的应用经验数据 e2 和移动平台生态系统的应用数据 e1 均不为空，则由比较模块 102 对平台数据可靠度 t1 和用户数据可靠度 t2 进行比较。输出模块 103 根据比较结果输出可靠度高的应用经验数据作为统计经验数据。

[0106] 在本发明的一个实施例中，云服务器 100 还进一步包括检测模块 105，检测模块 105 用于检测统计经验数据是否发生变化，在检测到某个应用程序的统计经验数据变化时

获取变化的统计经验数据对应的应用程序，并查询对应的应用程序的用户列表。然后由输出模块 103 向用户列表中的用户推送变化后的统计经验数据。移动终端 200 在接收到上述统计经验数据后，可以直接应用云服务器 100 推送的数据到系统中，也可以将上述统计经验数据显示给用户，由用户判断是否需要应用该统计经验数据。

[0107] 由此，云服务器 100 可以在检测到应用程序的统计经验数据变化时，主动向使用该应用程序的用户推送更新信息。便于用户的手机终端可以实时的更新到最新的恶意行为信息，及时地对手机上的应用程序的恶意行为进行判断以及修正。

[0108] 根据本发明实施例的云服务器，采集应用程序的应用行为数据，并通过对应用行为数据的分析获取可疑行为特征数据，并且实现云服务器和移动终端的数据同步，从而为移动终端判断应用程序的敏感行为是否为可疑行为提供更充分的依据。

[0109] 下面参考图 7 描述根据本发明实施例的移动终端。

[0110] 如图 7 所示，本发明实施例的移动终端 200 包括 :存储模块 201、获取模块 202、展示模块 203、预判模块 204 和设置模块 205。其中，存储模块 201 用于存储应用程序的固有信息。在本发明的一个示例中，固有信息包括应用程序的名称、版本号、简介等。获取模块 202 用于向云服务器 100 发送指定应用程序的数据请求信号，以及接收来自云服务器 100 的指定应用程序的统计经验数据。展示模块 203 用于向用户展示指定应用程序的固有信息和 / 或统计经验数据。其中，如果云服务器 100 中未存储有该指定应用程序的统计经验数据，则只向用户展示应用程序的固有信息。

[0111] 预判模块 204 根据指定应用程序的固有信息和 / 或统计经验数据对指定应用程序进行可疑行为的意图预判以判断可疑行为是否为恶意行为。设置模块 205 根据意图判断结果设置指定应用程序对可疑行为的执行许可或执行警告。

[0112] 在本发明的一个实施例中，设置模块 205 在预判模块 204 判断可疑行为为恶意行为时，设置指定应用程序对该可疑行为的执行警告 ;在预判模块 204 判断可疑行为为非恶意行为时，设置指定应用程序对该可疑行为的执行许可。

[0113] 在本发明的一个实施例中，移动终端还进一步包括 :恶意行为特征模型库、敏感资源监控模块、行为采集模块、应用行为数据库、应用行为分析中心和应用安全中心。其中，恶意行为特征模型库用于存储恶意行为模型。敏感资源监控模块用于监控应用程序对敏感资源的访问以获得应用程序的行为数据。行为采集模块用于对敏感资源监控模块监控到的行为数据获得应用程序对敏感资源的可疑行为。应用行为数据库用于存储行为采集模块检测的可疑行为。应用行为分析中心用于接收来自行为采集模块的可疑行为，并调用恶意行为特征模型库中的恶意行为模型，以及将可疑行为与恶意行为模型进行匹配以判断可疑行为对应的行为是否为恶意行为。应用安全中心用于查询应用行为数据库中存储的可疑行为，以及当判断可疑行为为恶意行为后，按照恶意程度对该可疑行为所对应的应用程序访问进行排序，并设置该应用程序访问的警告级别。

[0114] 其中，预判模块 204 可以集成于应用行为分析中心，根据指定应用程序的固有信息和 / 或统计经验数据对指定应用程序进行可疑行为的意图预判以判断可疑行为是否为恶意行为。设置模块 205 可以集成于应用安全中心，根据意图判断结果设置指定应用程序对可疑行为的执行许可或执行警告。

[0115] 根据本发明实施例的移动终端，可使用户可以在应用程序执行之前，提前获知应

用程序的可疑行为信息，并对应用程序进行预判断，提高对恶意程序的监测和拦截能力，提升移动终端的安全性。

[0116] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0117] 在流程图中表示或在此以其他方式描述的逻辑和 / 或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备（如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统）使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，″计算机可读介质″可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例（非穷尽性列表）包括以下 :具有一个或多个布线的电连接部（电子装置），便携式计算机盘盒（磁装置），随机存取存储器 (RAM)，只读存储器 (ROM)，可擦除可编辑只读存储器 (EPROM 或闪速存储器），光纤装置，以及便携式光盘只读存储器 (CDROM)。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

[0118] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现 :具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列 (PGA)，现场可编程门阵列 (FPGA) 等。

[0119] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0120] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0121] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0122] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何

的一个或多个实施例或示例中以合适的方式结合。

[0123] 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同限定。

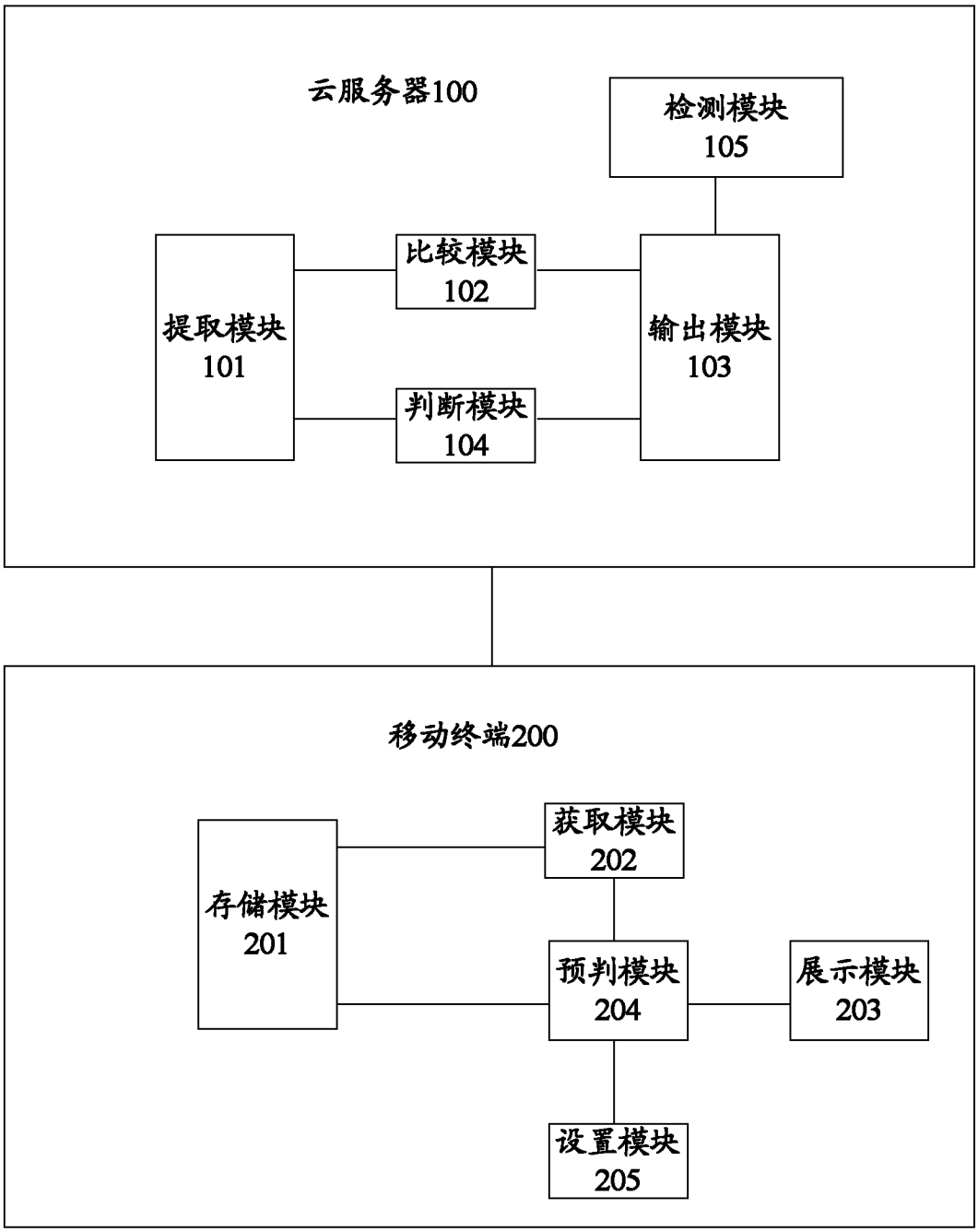

云服务器100
检测模块
105
比较模块
102
提取模块
101
输出模块
103
判断模块
104
移动终端200
获取模块
202
存储模块
201
预判模块
204
展示模块
203
设置模块
205

图 1

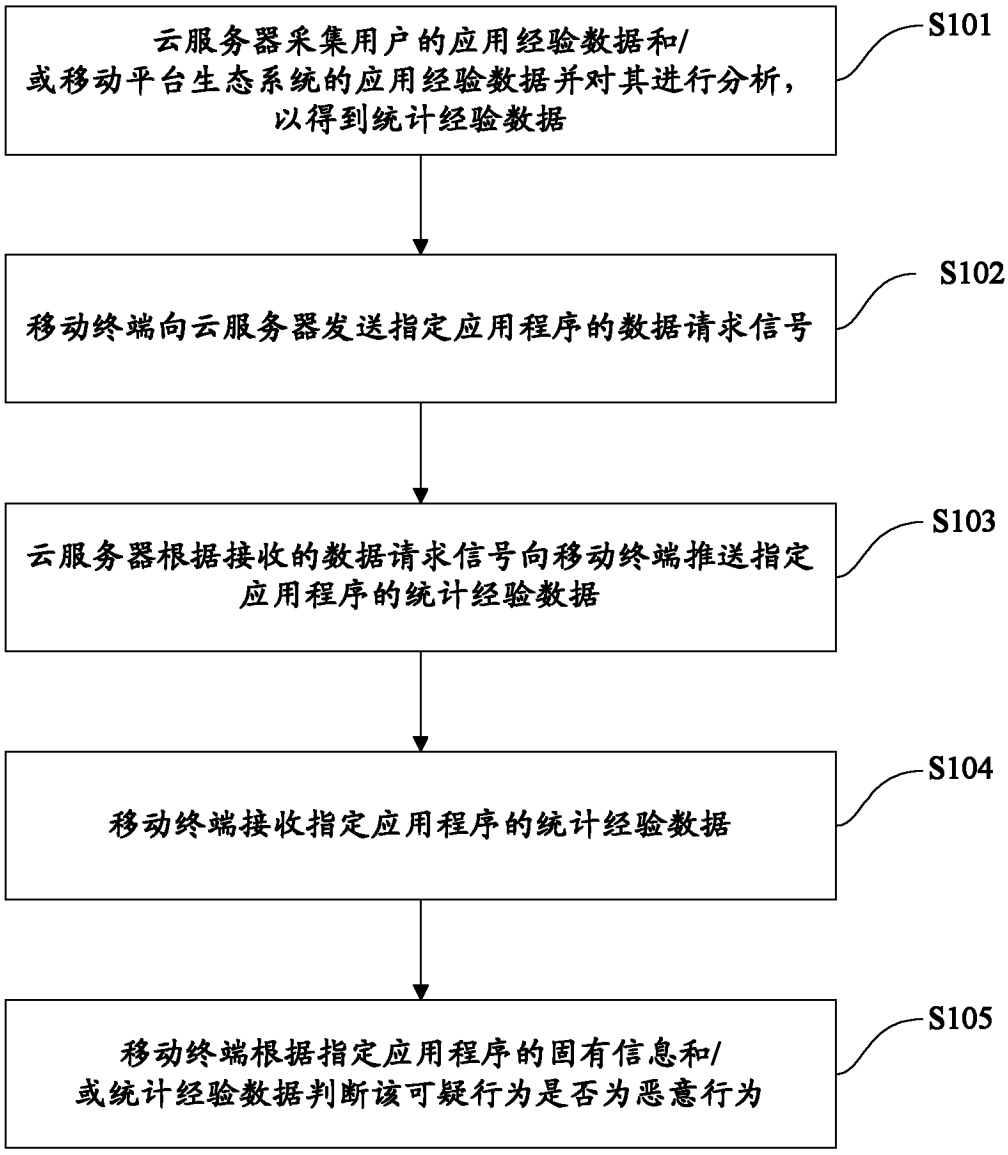

云服务器采集用户的应用经验数据和/
或移动平台生态系统的应用经验数据并对其进行分析，
以得到统计经验数据
S101
移动终端向云服务器发送指定应用程序的数据请求信号
S102
云服务器根据接收的数据请求信号向移动终端推送指定
应用程序的统计经验数据
S103
移动终端接收指定应用程序的统计经验数据
S104
移动终端根据指定应用程序的固有信息和/
或统计经验数据判断该可疑行为是否为恶意行为
S105

图 2

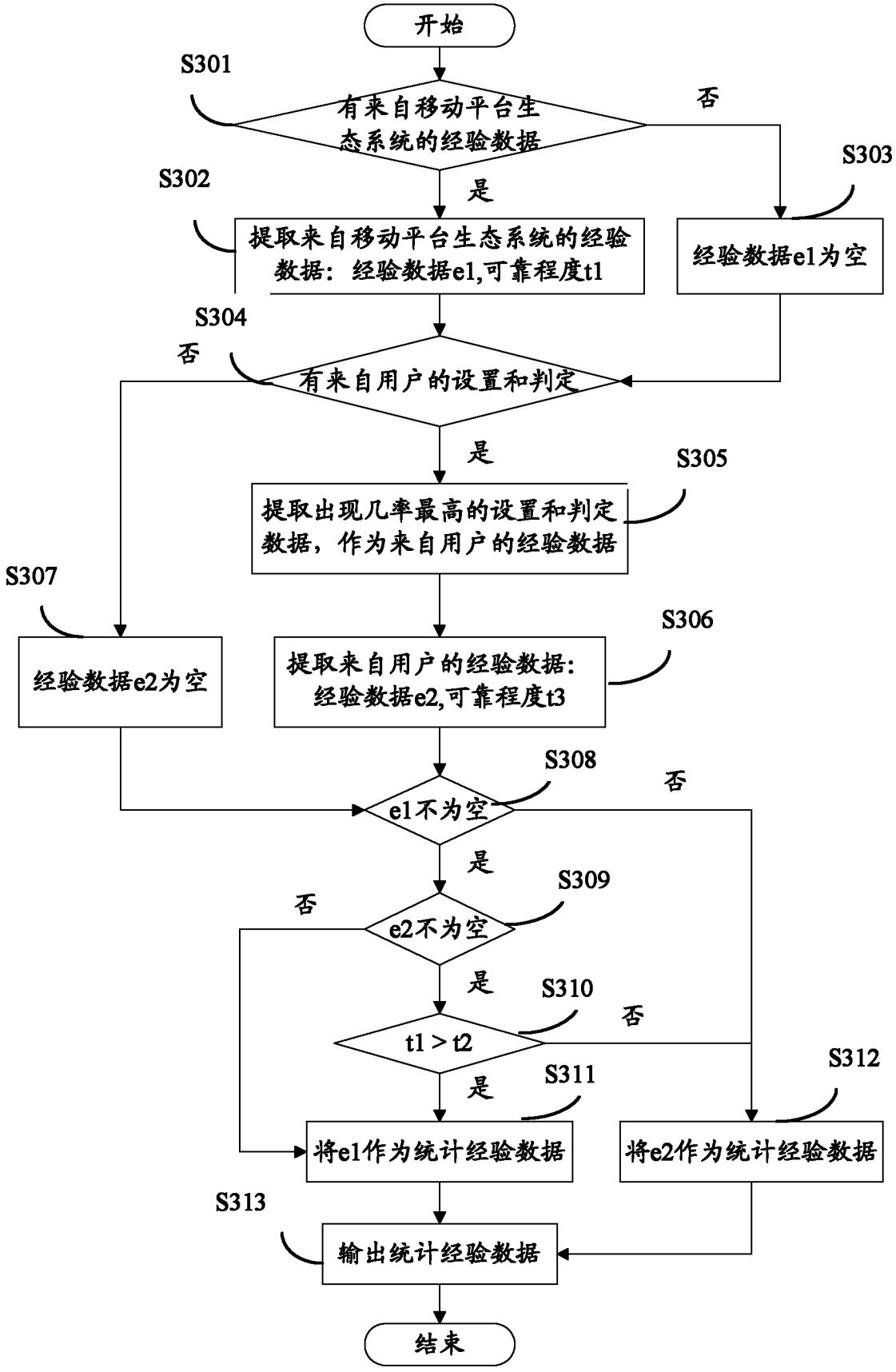

开始
S301
有来自移动平台生态系统的经验数据
否
是
S302
提取来自移动平台生态系统的经验数据：经验数据e1,可靠程度t1
S303
经验数据e1为空
S304
有来自用户的设置和判定
否
是
S305
提取出现几率最高的设置和判定数据，作为来自用户的经验数据
S307
经验数据e2为空
S306
提取来自用户的经验数据：经验数据e2,可靠程度t3
S308
e1不为空
否
是
S309
e2不为空
否
是
S310
t1 > t2
否
是
S311
S312
将e1作为统计经验数据
将e2作为统计经验数据
S313
输出统计经验数据
结束

图 3

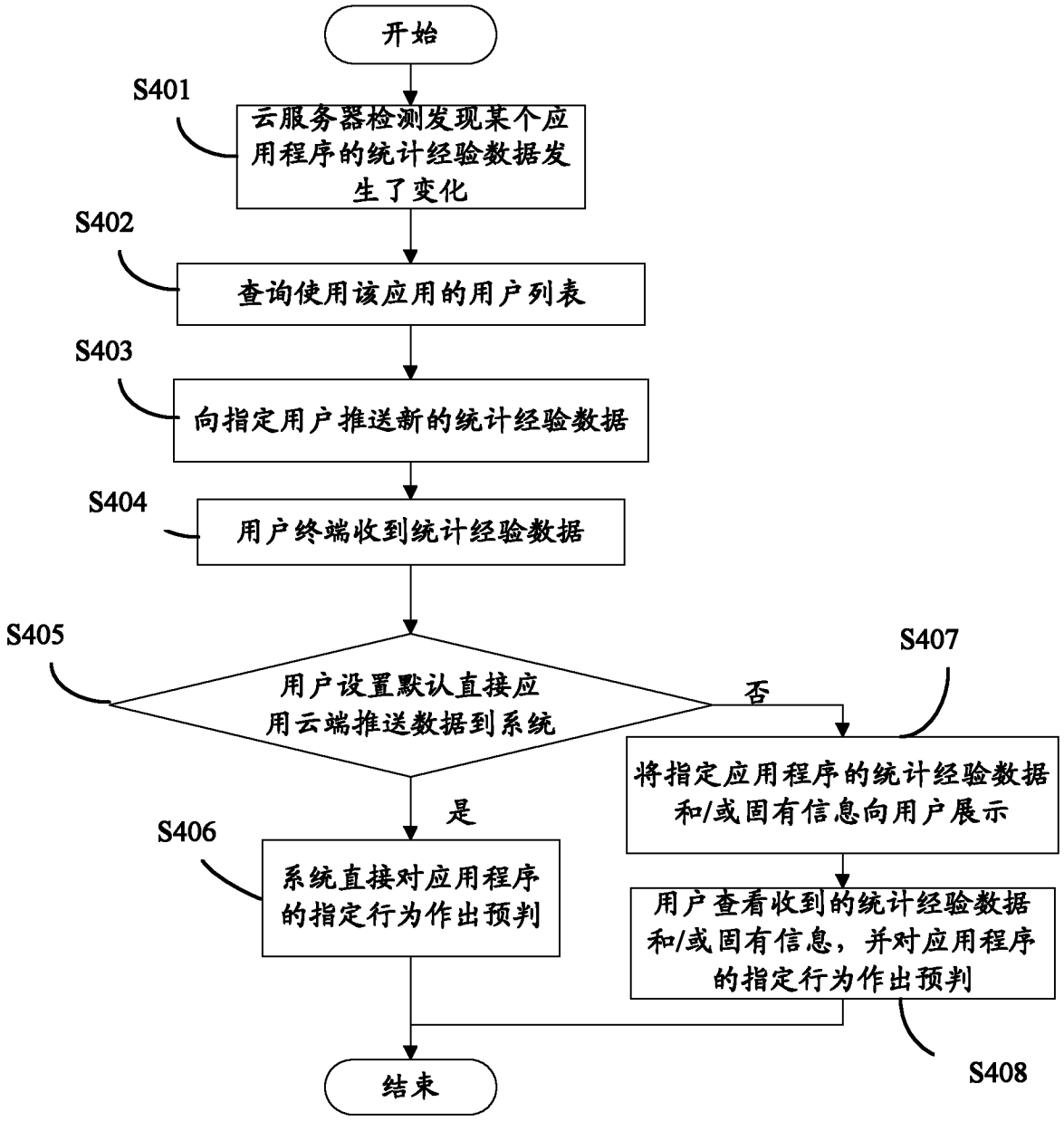

开始
S401
云服务器检测发现某个应用程序的统计经验数据发生了变化
S402
查询使用该应用的用户列表
S403
向指定用户推送新的统计经验数据
S404
用户终端收到统计经验数据
S405
用户设置默认直接应用云端推送数据到系统
否
S407
将指定应用程序的统计经验数据和/或固有信息向用户展示
是
S406
系统直接对应用程序的指定行为作出预判
用户查看收到的统计经验数据和/或固有信息，并对应用程序的指定行为作出预判
S408
结束

图 4

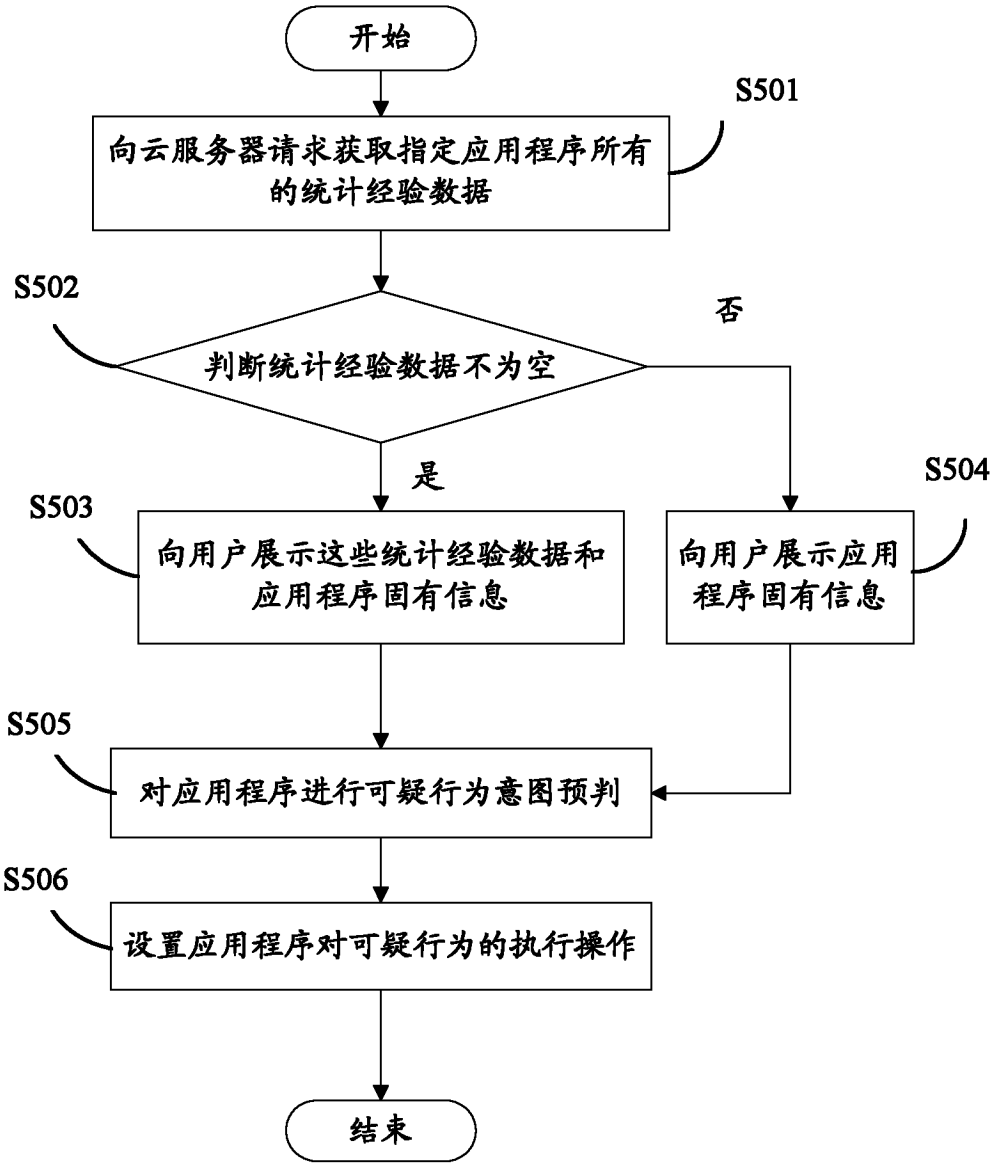

开始
S501
向云服务器请求获取指定应用程序所有的统计经验数据
S502
判断统计经验数据不为空
否
是
S504
S503
向用户展示这些统计经验数据和应用程序固有信息
向用户展示应用程序固有信息
S505
对应用程序进行可疑行为意图预判
S506
设置应用程序对可疑行为的执行操作
结束

图 5

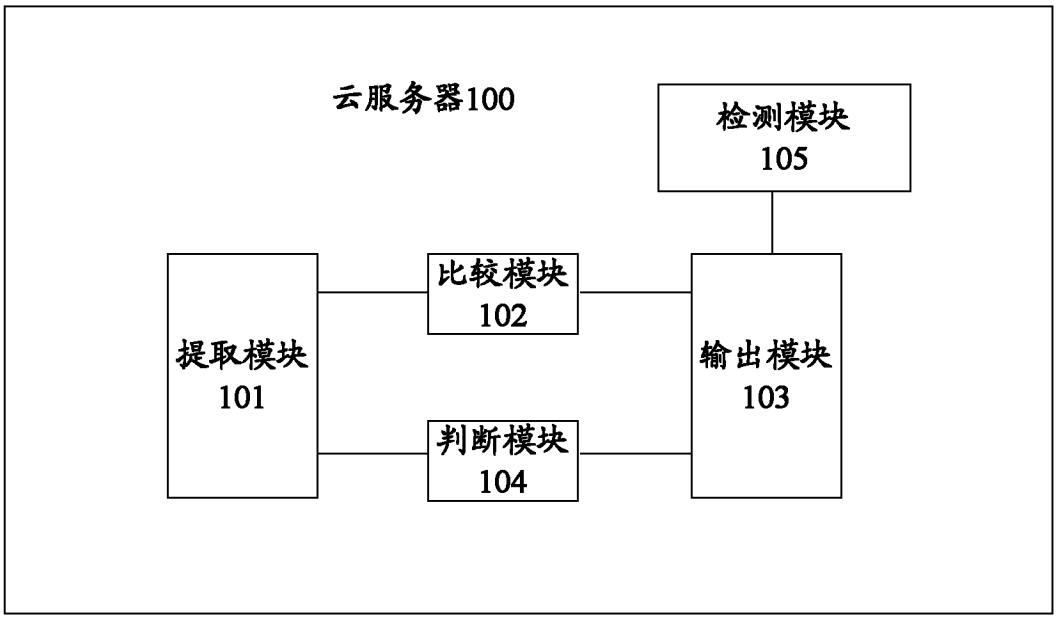

云服务器100
检测模块
105
比较模块
102
提取模块
101
输出模块
103
判断模块
104

图 6

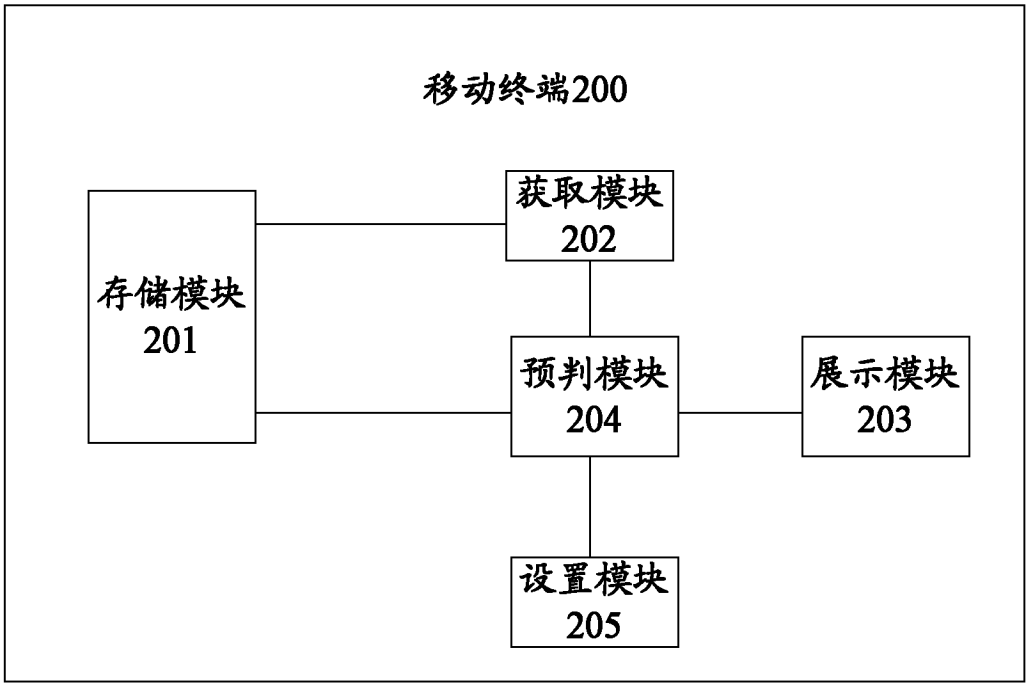

移动终端200
获取模块
202
存储模块
201
预判模块
204
展示模块
203
设置模块
205

图 7