[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 9/445 (2006.01)
G06F 21/22 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710031200.3

[43] 公开日 2009 年 5 月 6 日

[11] 公开号 CN 101425016A

[22] 申请日 2007.11.1
[21] 申请号 200710031200.3
[71] 申请人 珠海金山软件股份有限公司
地址 519015 广东省珠海市珠海吉大景山路莲山巷 8 号金山电脑大厦
[72] 发明人 朱熠锷
[74] 专利代理机构 广州华进联合专利商标代理有限公司
代理人 李双皓

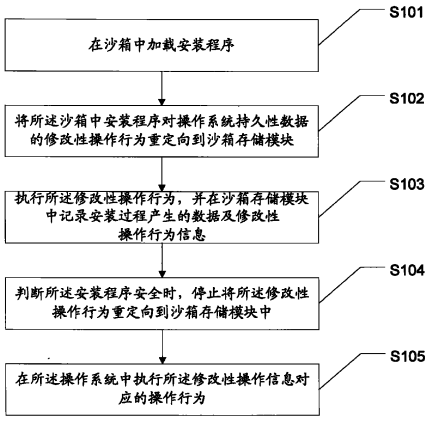
权利要求书 3 页 说明书 8 页 附图 2 页

[54] 发明名称

运行安装软件的方法和系统

[57] 摘要

本发明公开了一种运行安装软件的方法和系统。所述方法包括：在沙箱中加载安装程序；将所述安装程序对操作系统持久性数据的修改性操作行为重定向到沙箱存储模块；执行所述修改性操作行为，并在所述沙箱存储模块中记录相应的修改性操作行为信息以及在安装过程中所产生的数据；判断所述安装程序安全时，停止将所述修改性操作行为重定向到沙箱存储模块中；在所述操作系统中执行所述修改性操作信息对应的操作行为。通过本发明技术方案，安装程序合并到操作系统之后，达到在操作系统真实安装的效果，在保证安装过程安全的同时，提高了安装程序的实用性。



1、一种运行安装软件的方法，其特征在于，包括:

在沙箱中加载安装程序;

将所述安装程序对操作系统持久性数据的修改性操作行为重定向到沙箱存储模块;

执行所述修改性操作行为，并在所述沙箱存储模块中记录相应的修改性操作行为信息以及在安装过程中所产生的数据;

判断所述安装程序安全时，停止将所述修改性操作行为重定向到沙箱存储模块中;

在所述操作系统中执行所述修改性操作信息对应的操作行为。

2、根据权利要求 1 所述的运行安装软件的方法，其特征在于，所述修改性操作信息对应的操作行为包括对操作系统持久性数据的创建和/或修改，所述执行修改性操作信息对应的操作行为具体过程包括:

根据所述修改性操作信息和所述沙箱与操作系统之间的双向映射规则，获取所述沙箱存储模块中所述安装软件在安装过程中所产生的数据对应的操作系统路径;

调用所述操作系统的应用程序编程接口，将所述数据复制到所述操作系统路径。

3、根据权利要求 1 或 2 所述的运行安装软件的方法，其特征在于，所述修改性操作信息对应的操作行为包括删除操作系统持久性数据，所述删除行为的具体过程包括:

获得所述修改性操作信息中记录的所述安装程序试图删除的持久性数据信息;

将所述持久性数据信息作为参数传给所述操作系统中的删除函数，将所述操作系统中对应的持久性数据删除。

4、根据权利要求 3 所述的运行安装软件的方法，其特征在于，通过安全判断模块对所述存储模块进行扫描，或者采用人工的方式，判断所述安装程序是

否安全。

5、根据权利要求 3 所述的运行安装软件的方法，其特征在于，安装程序运行完毕之后还包括步骤：判断所述安装程序具有恶意行为时，提示是否删除所述沙箱存储模块记录的修改性操作行为信息以及所存储安装程序的数据。

6、一种运行安装软件的系统，其特征在于，包括：

沙箱外壳程序模块，用于将安装软件在沙箱中进行加载；

系统调用拦截模块，识别沙箱中运行的安装程序的调用，用于执行所述沙箱系统中安装程序对操作系统持久性数据的修改性操作行为，并重定向到存储模块；

沙箱存储模块，用于记录修改性操作行为信息以及在安装过程中所产生的数据；

提交模块，用于判断所述安装程序安全时，通知所述系统调用拦截模块停止将所述修改性操作行为重定向到沙箱存储模块中；将所述安装过程中所产生的数据结合修改性操作行为信息提交到所述操作系统进行合并。

7、根据权力要求 6 所述的运行安装软件的系统，其特征在于，所述提交模块包括：

复制模块，用于根据所述修改性操作信息以及所述沙箱与操作系统之间的双向映射规则，获取沙箱存储模块中所述安装软件在安装过程中所产生的数据对应的操作系统路径；调用操作系统的应用程序编程接口，将所述数据复制到对应的操作系统路径。

8、根据权利要求 6 或 7 所述的运行安装软件的系统，其特征在于，所述提交模块包括：

删除模块，用于根据所述修改性操作信息中记录的所述安装程序试图删除的持久性数据信息；将所述持久性数据信息作为参数传给所述操作系统中的删除函数，将所述操作系统中对应的持久性数据删除。

9、根据权利要求 8 所述的运行安装软件的系统，其特征在于，还包括：

安全判断模块，用于对所述沙箱存储模块进行扫描，或采用人工方式，判断所述安装程序是否安全。

10、根据权利要求 8 所述的运行安装软件的系统，其特征在于，所述提交模块还用于判断所述安装程序具有恶意行为时，提示是否删除沙箱存储模块所记录的修改性操作行为信息和所存储安装程序的数据。

运行安装软件的方法和系统

【技术领域】

本发明涉及计算机技术领域，尤其涉及运行安装软件的方法和系统。

【背景技术】

由于安装程序的特殊性，安装程序中可能被置入病毒、木马或恶意程序（以下统称为恶意软件），如果直接运行该程序可能会对操作系统造成损坏。

对于这些可能包含恶意软件的安装程序，传统的处理方法是，预先用杀毒软件扫描，没有发现问题再运行安装软件。但是，由于杀毒软件的杀毒能力存在一定的滞后性，且含恶意软件的安装软件可能进行了特殊的加密和伪装，这使得杀毒软件识别起来较为困难，将可能导致操作系统安装上恶意软件，对操作系统造成巨大损坏。

目前，还有一种运行安装软件的方法是在操作系统中构造虚拟机（VM），模拟真实操作系统的运行环境，通过虚拟机将安装程序封闭在一个虚拟的环境里运行，也仅在虚拟机中应用该程序。由于虚拟机的环境与真实的操作系统是完全隔离的，因此安装程序的修改性操作作用不到真实操作系统中，也就不会对真实操作系统造成影响。

但是，如果要在虚拟机中实现完全模拟真实操作系统的环境，需要进行大量的数据复制，虚拟机本身占用的资源较多，性能开销也大，建立虚拟机会影响整个操作系统的处理能力，这从实用性的角度是难以实现的，因而虚拟机难以实现对真实操作系统完全的模拟，也就是说，虚拟机难以实现精确的环境再造。因此，虚拟机所模拟的环境和真实环境是不同的，在其中进行安全的评估得到的结果对真实环境而言不具有较大的实用意义。此外，虚拟机环境与真实操作系统完全隔离的特性导致难以实现数据的修改提交。

【发明内容】

本发明的发明目的是提供一种运行安装软件的方法和系统，以达到提高软件安装的安全性和实用性的目的。

为达到上述发明目的，本发明提出以下的技术方案:

本发明提供一种运行安装软件的方法，首先在沙箱中加载安装程序;

将所述安装程序对操作系统持久性数据的修改性操作行为重定向到沙箱存储模块;

执行所述修改性操作行为，并在所述沙箱存储模块中记录相应的修改性操作行为信息以及在安装过程中所产生的数据;

判断所述安装程序安全时，停止将所述修改性操作行为重定向到沙箱存储模块中;

在所述操作系统中执行所述修改性操作信息对应的操作行为。

另外，本发明还提供一种运行安装软件的系统，包括:

沙箱外壳程序模块，用于将安装软件在沙箱中进行加载;

系统调用拦截模块，识别沙箱中运行的安装程序的调用，用于执行所述沙箱中安装程序对操作系统持久性数据的修改性操作行为，并重定向到沙箱存储模块;

沙箱存储模块，记录修改性操作行为信息以及在安装过程中所产生的数据;

提交模块，用于判断所述安装程序安全时，通知所述系统调用拦截模块停止将所述修改性操作行为重定向到沙箱存储模块中；将所述安装过程中所产生的数据结合修改性操作行为信息提交到所述操作系统进行合并。

从以上技术方案可以看出，本发明带来的有益效果：首先，本发明的技术方案在沙箱虚拟环境中运行安装程序，对其修改性操作进行拦截并进行处理，将其重定向到沙箱存储模块中进行相应记录，当判断处理结果安全之后，将记录内容提交到操作系统中进行合并，从而使安装程序可以脱离沙箱直接运行。被确认安全的程序合并到操作系统之后，达到了在操作系统真实环境下安装的效果。既能有效地防止安装程序对操作系统进行恶意修改，避免操作系统遭到

不可修复的损害，安装后的软件程序还可在真实的操作系统中正常运行，达到安全的软件程序在操作系统中直接安装的效果，具有完全的实用性。

其次，通过共享操作系统的资源（文件、注册表等）轻松实现精确的环境再造，为沙箱中运行的程序提供与在操作系统中直接运行的相同环境。

另外，由于本发明中的沙箱相比传统的虚拟机而言，具有轻量级虚拟化的优点，因此其占用的资源和性能开销较小，使并行运行多个虚拟环境成为可能。

【附图说明】

图 1 为本发明方法的基本流程图;

图 2 为本发明系统的结构框图。

【具体实施方式】

本发明是基于沙箱提供的虚拟环境进行的，本发明中的沙箱与传统的虚拟机相比具有轻量级虚拟化（Light-weight virtualization）和单向隔离的优点。本发明中的沙箱能够针对在沙箱中运行的程序对操作系统持久性数据的修改操作（包括文件和注册表操作）建立一个基于改写时复制（Copy On Write）策略的私有存储创建机制，以及实际存储和私有存储之间的路径双向映射机制。沙箱中的系统调用拦截模块，接管了操作系统中的文件操作和注册表操作的应用程序编程接口（Application Programming Interface，API）。换句话说，沙箱中程序调用文件操作（或注册表操作）的 API 时，实际执行的是沙箱中系统调用拦截模块中的对应操作行为。这些操作行为会根据沙箱系统调用中所请求的操作行为类型是否为修改类操作来调用不同的子处理流程。

本发明所描述的沙箱方案，是从程序的持久性数据入手，提供一个单向隔离的虚拟化执行环境，用于软件的安装和测试。本发明将沙箱内运行的程序对操作系统持久性数据的修改类操作（创建文件、修改文件、删除文件、创建、修改、删除注册表项等）进行拦截，并重定向到一沙箱私有的存储模块。因为是单向隔离，所以在保留隔离特性（防止持久性伤害）的同时，提供精确的环

境再造能力和将沙箱中的修改提交到操作系统中的能力。

图 1 为本发明提供的运行安装软件的方法的具体过程，如图 1 所示，首先创建或加载沙箱，然后在沙箱中加载安装程序（S101）。当安装程序运行后，将所述沙箱中安装程序对操作系统持久性数据的修改性操作行为重定向到沙箱存储模块（S102），所述操作系统持久性数据包括但不限于文件以及注册表项。接着，执行所述操作行为，并在所述沙箱存储模块中记录相应的操作行为信息以及在安装过程中所产生的数据，所述数据包含但不限于文件以及注册表项，操作行为一般包括修改性操作行为和读取性操作行为，在本发明中，对操作系统持久性数据的修改性操作行为进行重定向即可（S103）。至此，安装过程结束。然后利用设置的安全判断模块，通过扫描私有存储区或根据运行所安装的程序并对其行为进行人工判定的方式，来确定此安装程序是否带有恶意行为。当判断所述安装程序安全时，停止将所述操作行为重定向到沙箱存储模块中（S104）。最后，在所述操作系统中执行所述修改性操作信息对应的操作行为（S105），将沙箱存储模块中的数据结合操作行为信息提交并合并到真实的操作系统中去。

具体工作过程和原理是：

安装软件程序时，首先创建或加载一个沙箱，并将安装程序加载进该沙箱，在沙箱中运行该程序。安装程序运行时对操作系统提出操作请求，在执行相应的操作时通常会包括一些修改性操作，比如对文件和注册表的操作，此时沙箱可识别出安装程序对操作系统持久性数据提出的修改性操作，并对其进行拦截，将其重定向到一个沙箱存储模块。由于修改类操作被拦截，实际上并没有修改操作系统中任何实际的数据，因此即使是运行的恶意软件也不会对操作系统造成持久性的损害。

接着，执行所述操作行为，并记录相应的操作行为信息以及在安装过程中所产生的数据，所述操作行为一般包括删除类操作、读取类操作和改写类操作。一般而言，上述三种操作行为中，删除类操作和改写类操作如果直接运行于操作系统当中，将会对操作系统的持久性数据进行删除、修改和/或创建，因此有可能会对操作系统的安全性造成影响。本发明将改写类操作中的创建和/或修改

过程，以及删除类操作中的删除过程定义为修改性操作。在本实施例中，通过日志系统来记录相应的修改性操作行为信息。

对于删除类操作而言，首先根据沙箱与操作系统之间双向映射的规则，将原始路径名映射为沙箱存储模块中的路径名，然后搜索沙箱存储模块，若此路径所指示的对象存在，则直接将此对象在沙箱存储模块中的副本删除，并将该操作行为信息进行记录。通过上述操作在沙箱存储模块中存储文件和注册表项的修改结果及操作行为的记录，以备需要时将安装结果提交到操作系统中进行合并。若不存在则不进行真正的删除操作，而是在日志系统中记录一条删除日志，包括了该安装程序试图删除的原始路径名。

对于读取类操作而言，首先根据沙箱与操作系统之间双向映射的规则，将原始路径名映射为沙箱存储模块中的路径名，并检查此路径是否存在于沙箱的删除日志中，是则返回路径找不到的错误并结束此流程。否则接着搜索沙箱存储模块，若此路径所指示的对象存在，则将此对象在沙箱存储模块中的副本打开并返回给沙箱，以供沙箱中的安装程序读取；若所指示的对象不存在则按原始路径打开所指定的对象再返回。

对于改写类操作而言，首先根据沙箱与操作系统之间双向映射的规则，将原始路径名映射为沙箱存储模块中的路径名，并检查此路径是否存在于沙箱的删除日志中，是则返回路径找不到的错误并结束此流程。若不存在于删除日志，则接着搜索沙箱存储模块，若此路径所指示的对象存在，则将此对象在沙箱存储模块中的副本打开并返回给沙箱，以供沙箱中的安装程序改写；若所指示的对象不存在，则要将原始路径所指示的对象复制一份副本到沙箱存储模块中，然后打开此副本再将其返回给沙箱。

举例来说，若沙箱中运行的安装程序要在 C:\Windows\目录下写入一个 a.txt 文件，通过使用本发明的方法，实际上并没有新文件被写到 C:\Windows\下，而是将该修改性操作重定向到沙箱存储模块，在沙箱存储模块中创建了 a.txt 文件并将其句柄返回给沙箱中运行的安装程序。对该程序而言，其所操作的仍然是 C:\Windows\a.txt，但对于操作系统或其它不在沙箱中运行的程序而言，这个文件的实际位置可能是在例如 C:\MySandbox\C\Windows\a.txt 这样的

路径下。

步骤S103之后，沙箱内整个安装过程对操作系统所有持久性数据所进行的操作动作被完整地记录在日志中，在安装过程中产生的实际数据（包括文件、目录、注册表项等具体内容）被保存到沙箱存储模块中。根据沙箱存储模块存储的安装程序产生的实际数据，可以判断该安装文件是否安全，即该安装程序是否具有恶意行为。所述判断过程可以利用一个安全判断模块，通过对沙箱存储模块里存储的数据进行扫描的方式来判断，并提供扫描结果报告。当然，也可以通过人工的方式进行判断。当判断所述安装程序不存在恶意软件即安全时，停止将所述操作行为重定向到沙箱存储模块中。

当通过判断，确认安装程序安全之后，再将沙箱存储模块所存储安装程序的数据结合日志系统所记录的修改性操作行为信息提交到操作系统进行合并。所述操作行为信息一般可以包括，安装程序运行过程中在沙箱存储模块产生的文件名和/或目录名和/或注册表项信息，以及包含删除日志的日志系统，所述提交的具体过程一般包括复制和/或删除过程。

对于复制过程，首先根据记录的修改性操作信息和所述沙箱与操作系统之间的双向映射规则，获取沙箱存储模块中所述安装软件在安装过程中所产生的数据对应的操作系统路径；然后调用操作系统的应用程序编程接口 API，将所述数据复制到所述操作系统相应路径，所述数据包含文件和/或目录和/或注册表项。

对于删除过程，首先需要取出删除日志的记录信息，该记录信息包含安装程序试图进行删除的持久性数据信息；然后将所述持久性数据信息作为参数传给操作系统 API 中的删除函数，将所述操作系统中对应的持久性数据删除。所述持久性数据信息包括文件名和/或目录名和/或注册表项名信息；所述持久性数据包括文件和/或目录和/或注册表项。

作为本发明的进一步改进，安装程序在沙箱中运行完毕之后，在判断当所述安装程序具有恶意行为时，提示用户选择是否删除沙箱存储模块中记录的操作行为信息以及所存储安装程序的数据。用户可以根据需要，选择删除日志所

记录的修改性操作行为信息和沙箱存储模块所存储安装程序产生的数据，或者选择保留所述日志和数据。

基于本发明方法的工作过程和基本原理，本发明还提供一种运行安装软件的系统，如图 2 所示，包括:

沙箱外壳程序模块 1，将安装软件在沙箱中进行加载;

系统调用拦截模块 2，识别沙箱中运行的安装程序的调用，用于执行所述沙箱中安装程序对操作系统持久性数据的修改性操作行为，并重定向到沙箱存储模块 3;

沙箱存储模块 3，记录操作行为信息以及数据，所述操作行为信息包括修改性操作行为信息，所述数据包括所述安装软件在安装过程中所产生的数据;

提交模块 4 判断所述安装程序安全时，通知所述系统调用拦截模块 2 停止将所述修改性操作行为重定向到沙箱存储模块 3 中；在所述操作系统中执行所述修改性操作信息对应的操作行为，即将所述沙箱存储模块所存储安装程序的数据结合修改性操作行为信息提交到所述操作系统进行合并。

其中，所述提交模块 4 包括复制模块和删除模块:

复制模块根据所述修改性操作行为信息以及沙箱与操作系统之间的双向映射规则，获取沙箱存储模块中所述安装软件在安装过程中所产生的数据对应的操作系统路径；调用操作系统的应用程序编程接口 API，将所述数据复制到对应的操作系统路径，所述数据包含文件和/或目录和/或注册表项。

删除模块根据所述修改性操作信息中记录的所述安装程序试图删除的持久性数据信息；将所述持久性数据信息作为参数传给所述操作系统中的删除函数，将所述操作系统中对应的持久性数据删除。所述持久性数据信息包括文件名和/或目录名和/或注册表项名信息；所述持久性数据包括文件和/或目录和/或注册表项。

作为本发明的进一步改进，为提高判断安装程序过程是否安全，本发明的

系统还包括：安全判断模块 5，该模块对所述沙箱存储模块 3 进行恶意软件扫描，或采用人工的方式，判断所述安装程序是否安全。

作为本发明的进一步改进，所述提交模块 4 还可以在判断所述安装程序具有恶意行为时，提示用户选择是否删除沙箱存储模块中所记录的操作行为信息和所存储安装程序的数据。

本发明系统的工作过程、基本原理与本发明方法的基本一致，此处不再赘述。

以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

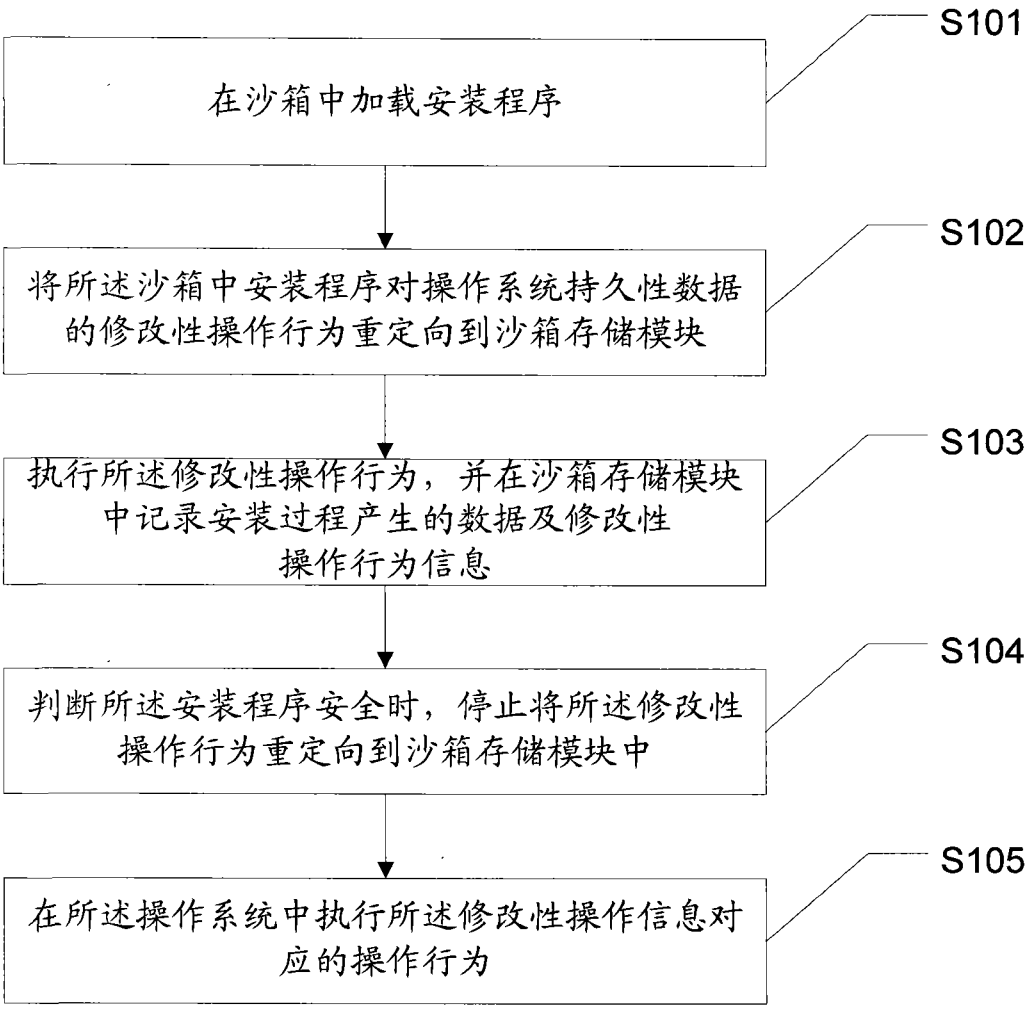

S101
在沙箱中加载安装程序
S102
将所述沙箱中安装程序对操作系统持久性数据的修改性操作行为重定向到沙箱存储模块
S103
执行所述修改性操作行为，并在沙箱存储模块中记录安装过程产生的数据及修改性操作行为信息
S104
判断所述安装程序安全时，停止将所述修改性操作行为重定向到沙箱存储模块中
S105
在所述操作系统中执行所述修改性操作信息对应的操作行为

图 1

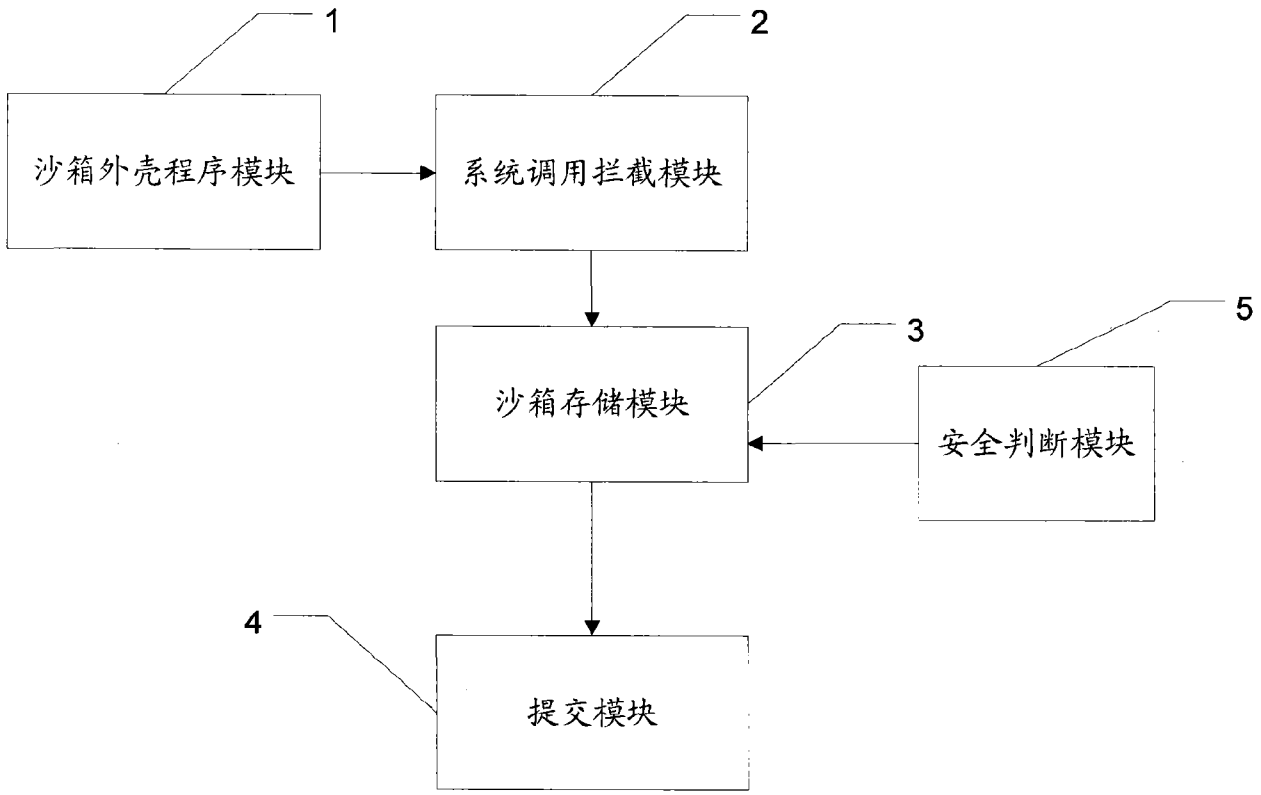


图 2