(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104866761 B
(45)授权公告日 2017.10.31

(21)申请号 201510292398.5

(22)申请日 2015.06.01

(65)同一申请的已公布的文献号
申请公布号 CN 104866761 A

(43)申请公布日 2015.08.26

(73)专利权人 成都中科创达软件有限公司
地址 610041 四川省成都市高新区交子大道88号中航国际广场1幢4层401-408号

(72)发明人 劳亚奇 曾俊汉 陈刚

(74)专利代理机构 北京天奇智新知识产权代理有限公司 11340
代理人 郭霞

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

(56)对比文件
CN 102222194 A,2011.10.19,
CN 103368904 A,2013.10.23,
CN 104318176 A,2015.01.28,
CN 104182688 A,2014.12.03,
CN 104182688 A,2014.12.03,
US 2010/0293615 A1,2010.11.18,
CN 102508768 A,2012.06.20,
CN 103259806 A,2013.08.21,
CN 101866407 A,2010.10.20,
褚力行.基于数据签名的Linux兼容内核上应用程序的安全机制.《中国优秀硕士学位论文全文数据库 信息科技辑》.2007,

审查员 张立丽

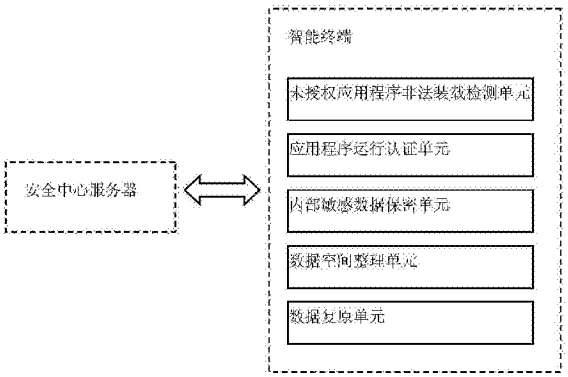
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种高安全性安卓智能终端

(57)摘要

本发明的高安全性安卓智能终端包括依次设置的未授权应用程序非法装载检测单元、应用程序运行认证单元、内部敏感数据保密单元、数据空间整理单元以及数据复原单元;通过各单元的设置,对安卓操作系统中的应用程序和内存数据进行了有效的保护,降低了设备损耗、提高了用户使用体验。



CN 104866761 B

1.一种高安全性安卓智能终端，所述智能终端包括依次设置的未授权应用程序非法装载检测单元、应用程序运行认证单元、内部敏感数据保密单元、数据空间整理单元以及数据复原单元；其中，

所述未授权应用程序非法装载检测单元用于未授权应用程序非法装载的检测；

所述应用程序运行认证单元用于运行智能终端内应用程序时的认证；

所述内部敏感数据保密单元用于应用程序可调用内部敏感数据的保密处理；

所述数据空间整理单元用于数据读写存储空间的管理；以及

所述数据复原单元用于安卓操作系统的数据复原；

所述未授权应用程序非法装载检测单元包括：程序非标准检测单元、第一交互单元、预分析单元、动作配准单元、自适应反应单元以及第二传输单元；其中，

所述程序非标准检测单元用于检测智能终端中的非正常现象；

所述预分析单元用于获得系统所在智能终端中安装的应用程序信息，同时将预分类的非法动作通过数据库运作建立待判定程序组；

所述未授权应用程序非法装载检测单元通过第一交互单元调用程序非标准检测单元的检测结果，所得到的非标准检测结果发送至动作配准单元；

所述动作配准单元将安卓操作系统程序非标准检测单元检测到的非正常现象与待判定程序组中的动作做比对；

所述动作配准单元将程序非标准检测单元检测到的非正常现象与预分析单元在初始化阶段已经完成的待判定程序组中的动作做比对，得到该非正常现象涉及到的运作权限后，再将这些运作权限所对应的程序从待判定程序组中取出，最后根据得到的程序数目的差异将信息进行相应的处理，如果得到仅一个程序被比对为待判定程序，则直接作为非法程序进入自适应反应单元执行相应运作，所述自适应反应单元根据比对信息中的非法级别决定相应类型；否则通过第二传输单元将待判定程序信息发送至安全中心服务器进行进一步判定，将待判定程序交由安全中心服务器进行被动分析。

2.一种如权利要求1所述的终端，所述未授权应用程序非法装载检测单元还可以设有运作权限判定单元和第一提示单元，运作权限判定单元从安装的应用程序中取出含有开机自动运行权限的应用程序，以提示的形式将这些应用程序信息显示给用户，并让用户选择信任为安全的程序，然后将用户选择的安全程序从待判定程序组中去除，不再进行后续的判定。

3.一种如权利要求2所述的终端，所述应用程序运行认证单元包括：标识码获得单元、密钥获得单元、第一加密单元、第二加密单元、以及认证请求发送单元；所述标识码获得单元、密钥获得单元分别连接第一加密单元，所述第一加密单元连接第二加密单元，以及第二加密单元连接认证请求发送单元，其中，

所述标识码获得单元用于当运行待运行的程序时，获得智能终端的移动设备国际标识码和移动终端电话号码；

所述密钥获得单元用于获得第一加密算法密钥、第二加密算法密钥和当前的时间标识序列；

所述第一加密单元用于根据第二加密算法密钥和所述当前的时间标识序列对所述移动设备国际标识码、移动终端电话号码和待运行的程序的签名序列进行加密；

所述第二加密单元用于根据所述第一加密算法密钥对所述第二加密算法密钥进行复合加密；

所述认证请求发送单元用于向安全中心服务器发送认证请求消息。

4.一种如权利要求3所述的终端，所述内部敏感数据保密单元包括：权限档案建立单元、独立控制单元、以及确定单元，其中，

所述权限档案建立单元，用于在安卓操作系统最下层建立用于存储应用权限记录表的权限档案，并将敏感数据分类存储在应用权限记录表中；

所述独立控制单元，用于在安卓操作系统最下层生成独立应用编程接口，通过独立应用编程接口设置应用权限记录表的内容；

所述确定单元，用于当应用程序读取敏感数据时，在安卓操作系统本地框架层根据应用权限记录表确定该应用是否有权限获得敏感数据。

5.一种如权利要求4所述的终端，所述数据复原单元包括：程序移除单元、加载类别去除单元、以及程序重构单元，其中

所述程序移除单元，用于遍历安卓操作系统的数据存储区中第一程序指引文档记录的应用的加载类别，移除加载类别为用户新加载应用的应用，所述第一程序指引文档中携带系统当前已安装的所有应用的加载类别，所述加载类别用于标识所述应用为用户新加载应用或原始设置应用；

所述加载类别去除单元，用于去除所述第一程序指引文档中已移除应用对应的加载类别；

所述程序重构单元，用于比较安卓操作系统的系统分区中第二程序指引文档和去除已移除应用对应的加载类别后的第一程序指引文档，根据所述第二程序指引文档记录的加载类别拷贝并重构所述第一程序指引文档没有记录的加载类别对应的应用，所述第二程序指引文档用于记录安卓操作系统首次安装时安装的应用的加载类别。

一种高安全性安卓智能终端

技术领域

[0001] 本发明涉及移动通信领域，尤其涉及一种高安全性安卓智能终端。

背景技术

[0002] 随着移动设备(智能终端、平板电脑)的普及和性能增加，移动设备上的应用也越来越多，范围也越来越广，不仅涉及娱乐、工具，更有网银等应用。移动设备中的软件程序保护和隐私数据保护也越发重要。

[0003] 由于智能终端中存有大量的用户隐私信息，因此吸引了大量的欺诈应用程序涌入应用程序市场，窃取用户的隐私信息；加之各个应用程序市场的监督管理制度和检测方法尚不完善，无法对应用程序的欺诈性进行甄别，因此使用户隐私信息大量外泄，应用程序的使用者蒙受很大损失。

[0004] 现有技术中，移动应用程序保护只在软件的安装流程方面进行了有限的控制，这很难给破解者造成障碍。目前安卓操作系统中对应用程序和内存数据的保护缺少有效的保护方案。因此亟需提供相应的安全保护安卓操作系统应用程序和内部数据的技术方案。

发明内容

[0005] 本发明的目的是通过以下技术方案实现的。

[0006] 根据本发明的实施方式，提出一种高安全性安卓智能终端，所述智能终端包括依次设置的未授权应用程序非法装载检测单元、应用程序运行认证单元、内部敏感数据保密单元、数据空间整理单元以及数据复原单元；其中，

[0007] 所述未授权应用程序非法装载检测单元用于未授权应用程序非法装载的检测；

[0008] 所述应用程序运行认证单元用于运行智能终端内应用程序时的认证；

[0009] 所述内部敏感数据保密单元用于应用程序可调用内部敏感数据的保密处理；

[0010] 所述数据空间整理单元用于数据读写存储空间的管理；以及

[0011] 所述数据复原单元用于安卓操作系统的数据复原。

[0012] 根据本发明的实施方式，所述未授权应用程序非法装载检测单元包括：程序非标准检测单元、第一交互单元、预分析单元、动作配准单元、自适应反应单元以及第二传输单元；其中，

[0013] 所述程序非标准检测单元用于检测智能终端中的非正常现象；

[0014] 所述预分析单元用于获得系统所在智能终端中安装的应用程序信息，同时将预分类的非法动作通过数据库运作建立待判定程序组；

[0015] 所述未授权应用程序非法装载检测单元通过第一交互单元调用程序非标准检测单元的检测结果，所得到的非标准检测结果发送至动作配准单元；

[0016] 所述动作配准单元将安卓操作系统程序非标准检测单元检测到的非正常现象与待判定程序组中的动作做比对；

[0017] 所述动作配准单元将程序非标准检测单元检测到的非正常现象与预分析单元在

初始化阶段已经完成的待判定程序组中的动作做比对，得到该非正常现象涉及到的运作权限后，再将这些运作权限所对应的程序从待判定程序组中取出，最后根据得到的程序数目的差异将信息进行相应的处理，如果得到仅一个程序被比对为待判定程序，则直接作为非法程序进入自适应反应单元执行相应运作，即，所述自适应反应单元根据比对信息中的非法级别决定相应类型；否则通过第二传输单元将待判定程序信息发送至安全中心服务器进行进一步判定，将待判定程序交由安全中心服务器进行被动分析。

[0018] 根据本发明进一步的实施方式，所述未授权应用程序非法装载检测单元还可以设有运作权限判定单元和第一提示单元，运作权限判定单元从安装的应用程序中取出含有开机自动运行权限的应用程序，以提示的形式将这些应用程序信息显示给用户，并让用户选择信任为安全的程序，然后将用户选择的安全程序从待判定程序组中去除，不再进行后续的判定。

[0019] 根据本发明的一个实施方式，所述应用程序运行认证单元包括：标识码获得单元、密钥获得单元、第一加密单元、第二加密单元、以及认证请求发送单元。

[0020] 根据本发明的实施方式，所述内部敏感数据保密单元包括：权限档案建立单元、独立控制单元、以及确定单元，其中，

[0021] 所述权限档案建立单元，用于在安卓操作系统最下层建立用于存储应用权限记录表的权限档案，并将敏感数据分类存储在应用权限记录表中；

[0022] 所述独立控制单元，用于在安卓操作系统最下层生成独立应用编程接口，通过独立应用编程接口设置应用权限记录表的内容；

[0023] 所述确定单元，用于当应用程序读取敏感数据时，在安卓操作系统本地框架层根据应用权限记录表确定该应用是否有权限获得敏感数据。

[0024] 根据本发明的实施方式，所述数据复原单元包括：程序移除单元、加载类别去除单元、以及程序重构单元，其中

[0025] 所述程序移除单元，用于遍历安卓操作系统的数据存储区中第一程序指引文档记录的应用的加载类别，移除加载类别为用户新加载应用的应用，所述第一程序指引文档中携带系统当前已安装的所有应用的加载类别，所述加载类别用于标识所述应用为用户新加载应用或原始设置应用；

[0026] 所述加载类别去除单元，用于去除所述第一程序指引文档中已移除应用对应的加载类别；

[0027] 所述程序重构单元，用于比较安卓操作系统的系统分区中第二程序指引文档和去除已移除应用对应的加载类别后的第一程序指引文档，根据所述第二程序指引文档记录的加载类别拷贝并重构所述第一程序指引文档没有记录的加载类别对应的应用，所述第二程序指引文档用于记录安卓操作系统首次安装时安装的应用的加载类别。

[0028] 本发明的高安全性安卓智能终端包括依次设置的未授权应用程序非法装载检测单元、应用程序运行认证单元、内部敏感数据保密单元、数据空间整理单元以及数据复原单元；通过各单元的设置，对安卓操作系统中的应用程序和内存数据进行了有效的保护，降低了设备损耗、提高了用户使用体验。

附图说明

[0029] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0030] 附图1示出了根据本发明实施方式的高安全性安卓智能终端结构示意图；

[0031] 附图2示出了根据本发明实施方式的未授权应用程序非法装载检测单元结构示意图；

[0032] 附图3示出了根据本发明实施方式的应用程序运行认证单元结构示意图；

[0033] 附图4示出了根据本发明实施方式的内部敏感数据保密单元结构示意图；

[0034] 附图5示出了根据本发明实施方式的数据空间整理单元结构示意图；

[0035] 附图6示出了根据本发明实施方式的数据复原单元结构示意图。

具体实施方式

[0036] 下面将参照附图更详细地描述本公开的示例性实施方式。虽然附图中显示了本公开的示例性实施方式，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0037] 根据本发明的实施方式，提出一种高安全性安卓智能终端，如附图1所示，所述智能终端包括依次设置的未授权应用程序非法装载检测单元、应用程序运行认证单元、内部敏感数据保密单元、数据空间整理单元以及数据复原单元；其中，

[0038] 所述未授权应用程序非法装载检测单元用于未授权应用程序非法装载的检测；

[0039] 所述应用程序运行认证单元用于运行智能终端内应用程序时的认证；

[0040] 所述内部敏感数据保密单元用于应用程序可调用内部敏感数据的保密处理；

[0041] 所述数据空间整理单元用于数据读写存储空间的管理；以及

[0042] 所述数据复原单元用于安卓操作系统的数据复原。

[0043] 根据本发明的实施方式，所述高安全性安卓智能终端与设置于云端的安全中心服务器通信，所述安全中心服务器包括依次设置的第一传输单元、被动解析单元、第一解密单元、第二解密单元以及云端认证单元；其中，

[0044] 所述第一传输单元用于传输与安全防护单元的交互数据；

[0045] 所述被动解析单元用于对智能终端应用程序的被动分析；

[0046] 所述第一解密单元和所述第二解密单元用于执行安全防护单元的应用程序运行认证单元发送数据的解密；以及

[0047] 所述云端认证单元用于执行智能终端应用程序的云端认证。

[0048] 根据本发明的一个实施方式，如附图2所示，所述未授权应用程序非法装载检测单元包括：程序非标准检测单元、第一交互单元、预分析单元、动作配准单元、自适应反应单元以及第二传输单元；其中，

[0049] 所述程序非标准检测单元用于检测智能终端中的非正常现象；

[0050] 所述预分析单元用于获得系统所在智能终端中安装的应用程序信息，同时将预分类的非法动作通过数据库运作建立待判定程序组；

[0051] 所述未授权应用程序非法装载检测单元通过第一交互单元调用程序非标准检测

单元的检测结果，所得到的非标准检测结果发送至动作配准单元；

[0052] 所述动作配准单元将安卓操作系统程序非标准检测单元检测到的非正常现象与待判定程序组中的动作做比对；

[0053] 所述动作配准单元将程序非标准检测单元检测到的非正常现象与预分析单元在初始化阶段已经完成的待判定程序组中的动作做比对，得到该非正常现象涉及到的运作权限后，再将这些运作权限所对应的程序从待判定程序组中取出，最后根据得到的程序数目的差异将信息进行相应的处理，如果得到仅一个程序被比对为待判定程序，则直接作为非法程序进入自适应反应单元执行相应运作，即，所述自适应反应单元根据比对信息中的非法级别决定相应类型；否则通过第二传输单元将待判定程序信息发送至安全中心服务器进行进一步判定，将待判定程序交由安全中心服务器进行被动分析。

[0054] 所述被动解析单元用于对智能终端应用程序exe文件的被动分析；所述被动解析单元处于线程控制运行状态，当消息队列中有未授权应用程序非法装载检测单元请求被动分析的消息时，被动解析单元便开始执行，首先从消息中获得exe文件，然后调用被动分析函数对exe文件进行分析，分析时用到已经建立完成的正常程序调用函数库及非标准程序调用函数库，最后根据分析函数返回的结果设置安全中心服务器向未授权应用程序非法装载检测单元的返回消息。

[0055] 根据本发明进一步的实施方式，所述未授权应用程序非法装载检测单元还可以设有运作权限判定单元和第一提示单元，运作权限判定单元从安装的应用程序中取出含有开机自动运行权限的应用程序，以提示的形式将这些应用程序信息显示给用户，并让用户选择信任为安全的程序，然后将用户选择的安全程序从待判定程序组中去除，不再进行后续的判定。

[0056] 根据本发明的一个实施方式，如附图3所示，所述应用程序运行认证单元包括：标识码获得单元、密钥获得单元、第一加密单元、第二加密单元、以及认证请求发送单元，其中，

[0057] 所述标识码获得单元用于当运行待运行的程序时，获得智能终端的移动设备国际标识码和移动终端电话号码；

[0058] 所述密钥获得单元用于获得第一加密算法密钥、第二加密算法密钥和当前的时间标识序列；所述第一加密算法可以是但不限于非对称加密算法，所述第二加密算法可以是但不限于对称加密算法；

[0059] 所述第一加密单元用于根据第二加密算法密钥和所述当前的时间标识序列对所述移动设备国际标识码、移动终端电话号码和待运行的程序的签名序列进行加密；

[0060] 所述第二加密单元用于根据所述第一加密算法密钥对所述第二加密算法密钥进行复合加密，

[0061] 所述认证请求发送单元用于向安全中心服务器发送认证请求消息，所述认证请求消息携带加密的所述移动设备国际标识码、移动终端电话号码、待运行的程序的签名序列和第二加密算法密钥；

[0062] 所述安全中心服务器通过第一传输单元接收所述认证请求消息；

[0063] 所述第一解密单元根据第一加密算法密钥对所述加密的第二加密算法密钥进行解密，获得当前的时间标识序列；

[0064] 所述第二解密单元根据所述解密的第二加密算法密钥和所述当前的时间标识序列对所述加密的移动设备国际标识码、移动终端电话号码和待运行的程序的签名序列进行解密；

[0065] 所述云端认证单元根据所述解密的移动设备国际标识码、移动终端电话号码和待运行的程序的签名序列对所述智能终端及待运行的应用程序进行认证。

[0066] 根据本发明的一个实施方式，如附图4所示，所述内部敏感数据保密单元包括：权限档案建立单元、独立控制单元、以及确定单元，其中，

[0067] 所述权限档案建立单元，用于在安卓操作系统最下层建立用于存储应用权限记录表的权限档案，并将敏感数据分类存储在应用权限记录表中；

[0068] 所述独立控制单元，用于在安卓操作系统最下层生成独立应用编程接口，通过独立应用编程接口设置应用权限记录表的内容；

[0069] 所述确定单元，用于当应用程序读取敏感数据时，在安卓操作系统本地框架层根据应用权限记录表确定该应用是否有权限获得敏感数据。

[0070] 根据本发明的实施方式，所述独立控制单元包括：

[0071] 独立应用编程接口生成单元，用于设置应用安装权限，在安卓操作系统最下层生成独立应用编程接口；

[0072] 权限管理单元，用于通过独立应用编程接口访问应用权限记录表，修改应用权限记录表中有获得权限的应用程序类型、以及该应用程序有权限获得的敏感数据的内容；以及

[0073] 第一存储单元，用于保存修改后的应用权限记录表。

[0074] 根据本发明的实施方式，所述确定单元包括：

[0075] 权限记录表读取单元，用于当应用程序读取敏感数据时，该应用程序调用标准应用编程接口访问独立应用编程接口，读取应用权限记录表；

[0076] 一致确定单元，用于在安卓操作系统本地框架层确定当前应用是否与应用权限记录表中的应用一致；以及

[0077] 执行单元，用于当确定结果为一致时，在应用权限记录表中查询当前应用有权限获得的敏感数据的类型，通过标准应用编程接口获得该类型对应的信息数据并显示。

[0078] 根据本发明的一个实施方式，如附图5所示，所述数据空间整理单元包括：空间整理方案设置单元、出入接口请求第一传送单元、出入接口请求截取单元、目的修改单元、以及出入接口请求第二传送单元，其中，

[0079] 所述空间整理方案设置单元，用于预先设置智能终端内的数据读写存储方案；

[0080] 所述出入接口请求第一传送单元，用于当安卓操作系统的应用层访问智能终端上的数据时，先将出入接口请求传送到安卓操作系统的内核层的虚拟文件开关层；

[0081] 所述出入接口请求截取单元，用于在安卓操作系统的内核层的虚拟文件开关层截取出入接口请求；

[0082] 所述目的修改单元，根据空间整理方案，修改或保留出入接口请求的目的数据库，将出入接口请求传送给真实的数据空间；以及

[0083] 所述出入接口请求第二传送单元，用于通过真实的数据空间将出入接口请求传送到智能终端的驱动程序中。

[0084] 根据本发明的实施方式，所述预先设置智能终端内的数据读写存储方案具体为：将可读写数据存储空间划分为安全区和暂存区，处于安全保障状态时，在内核层的虚拟文件开关层截取文件读写运作请求，将对安全区的写运作重定向到暂存区中；处于非安全保障状态时，直接下发所有文件读写运作请求；还原系统时，放弃暂存区中的数据；备份系统时，将暂存区中的数据回写到安全区。

[0085] 根据本发明的一个实施方式，如附图6所示，所述数据复原单元包括：程序移除单元、加载类别去除单元、以及程序重构单元，其中

[0086] 所述程序移除单元，用于遍历安卓操作系统的数据存储区中第一程序指引文档记录的应用的加载类别，移除加载类别为用户新加载应用的应用，所述第一程序指引文档中携带系统当前已安装的所有应用的加载类别，所述加载类别用于标识所述应用为用户新加载应用或原始设置应用；

[0087] 所述加载类别去除单元，用于去除所述第一程序指引文档中已移除应用对应的加载类别；

[0088] 所述程序重构单元，用于比较安卓操作系统的系统分区中第二程序指引文档和去除已移除应用对应的加载类别后的第一程序指引文档，根据所述第二程序指引文档记录的加载类别拷贝并重构所述第一程序指引文档没有记录的加载类别对应的应用，所述第二程序指引文档用于记录安卓操作系统首次安装时安装的应用的加载类别。

[0089] 根据本发明的实施方式，所述数据复原单元还可以包括：

[0090] 第一判断单元，用于在安卓操作系统首次运行时，判断数据存储区是否存在第一程序指引文档；

[0091] 首次安装加载类别添加单元，用于在第一程序指引文档不存在时，复制系统分区的第二程序指引文档到数据存储区，将复制的系统分区的第二程序指引文档作为数据存储区的第一程序指引文档；

[0092] 新加载类别添加单元，用于接收第三方应用安装完成的指令，并在数据存储区的第一程序指引文档中记录所述第三方应用的加载类别。

[0093] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

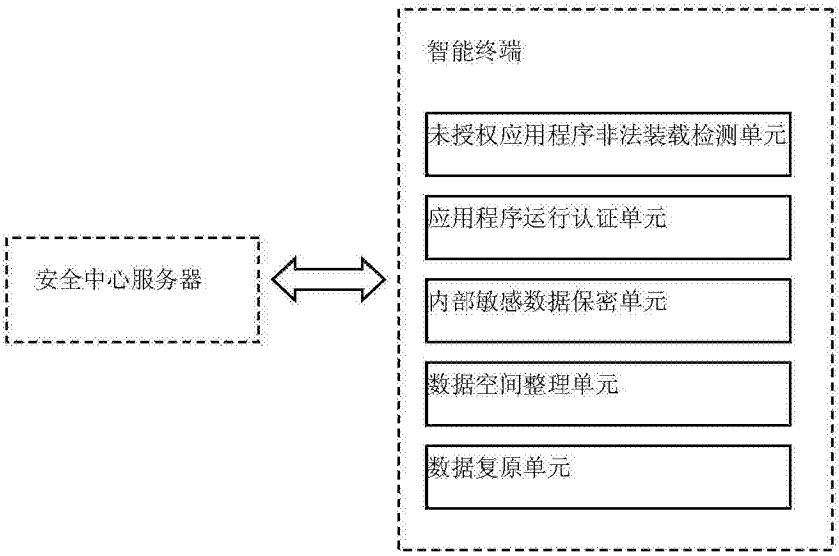

智能终端
未授权应用程序非法装载检测单元
应用程序运行认证单元
内部敏感数据保密单元
数据空间整理单元
数据复原单元
安全中心服务器

图1

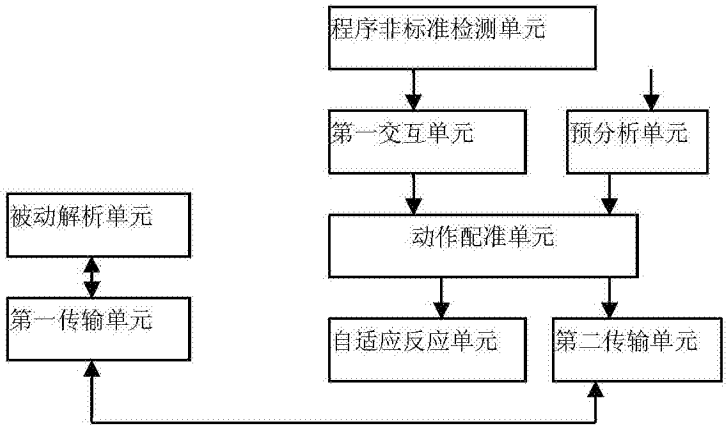

程序非标准检测单元
第一交互单元
预分析单元
被动解析单元
动作配准单元
第一传输单元
自适应反应单元
第二传输单元

图2

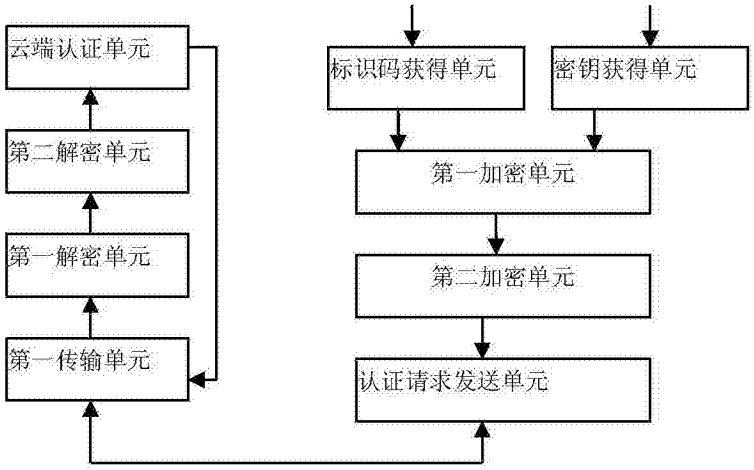

云端认证单元
第二解密单元
第一解密单元
第一传输单元
标识码获得单元
密钥获得单元
第一加密单元
第二加密单元
认证请求发送单元

图3

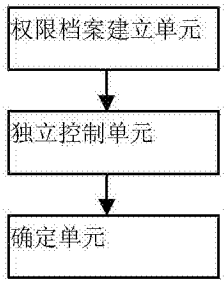

权限档案建立单元
独立控制单元
确定单元

图4

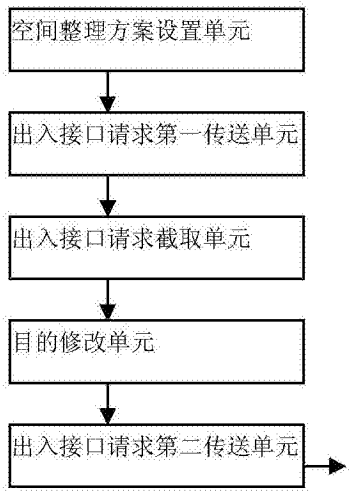

空间整理方案设置单元
出入接口请求第一传送单元
出入接口请求截取单元
目的修改单元
出入接口请求第二传送单元

图5

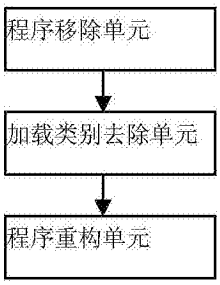


图6