



(12) 发明专利申请

(10) 申请公布号 CN 103164659 A

(43) 申请公布日 2013. 06. 19

(21) 申请号 201110415165. 1

(22) 申请日 2011. 12. 13

(71) 申请人 联想(北京)有限公司

地址 100085 北京市海淀区上地信息产业基地创业路 6 号

(72) 发明人 宋祎斐 彭绍平 杨建起

(74) 专利代理机构 北京银龙知识产权代理有限公司 11243

代理人 许静 安利霞

(51) Int. Cl.

G06F 21/62 (2013. 01)

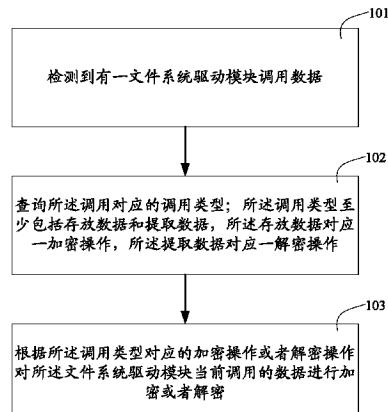
权利要求书2页 说明书6页 附图3页

(54) 发明名称

一种实现数据存储安全性的方法和电子设备

(57) 摘要

本发明实施例提供一种实现数据存储安全性的方法和电子设备，方法应用于电子设备，电子设备中包括：内核单元，为运行于电子设备上的应用程序提供对电子设备硬件的安全访问，支持文件系统驱动模块；文件系统驱动模块支持存取数据；检测到有一文件系统驱动模块调用数据；查询调用对应的调用类型；调用类型中，存放数据对应一加密操作，提取数据对应一解密操作；根据调用类型对应的加密操作或者解密操作对文件系统驱动模块当前调用的数据进行处理。在内核支持一文件系统驱动模块对数据进行调用的过程中，在内核中实现对数据的加密解密操作，且这一加密解密操作对于用户是不可见的，在不影响使用电子设备的其他功能的同时，提高了数据安全性。



1. 一种实现数据存储安全性的方法,应用于电子设备,其特征在于,所述电子设备中包括:

一内核单元,是所述电子设备的操作系统的一部分,为运行于所述电子设备上的应用程序提供对电子设备硬件的安全访问,以及,支持至少一个文件系统驱动模块运行;所述文件系统驱动模块支持以对应的数据组织格式存取数据;

方法包括:

检测到有一文件系统驱动模块调用数据;

查询所述调用对应的调用类型;所述调用类型至少包括存放数据和提取数据,所述存放数据对应一加密操作,所述提取数据对应一解密操作;

根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理。

2. 根据权利要求1所述的方法,其特征在于,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理,具体包括:

在所述加密操作中,接收所述应用程序传输来的明文数据,

调用一加密算法,对所说明文数据进行加密后生成密文数据,

将所述密文数据存放到所述应用程序对应的存储单元中。

3. 根据权利要求1所述的方法,其特征在于,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理,具体包括:

在所述解密操作中,找到所述应用程序对应的存储单元,并调用所述存储单元中的密文数据,

调用一解密算法,对所述密文数据进行解密后生成明文数据;

通知所述应用程序处理所说明文数据。

4. 根据权利要求1所述的方法,其特征在于,检测到有一文件系统驱动模块调用数据,之前还包括:

在所述电子设备上电启动之后,当处于 BOOT LOADER 阶段时,接收输入的密钥,所述密钥是所述加密操作的加密密钥,以及解密操作的解密密钥。

5. 根据权利要求1所述的方法,其特征在于,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理,具体包括:

检测到当前没有可以使用的密钥,

提示需要通过电子设备接口接收来自一 SIM 卡的密钥。

6. 根据权利要求1所述的方法,其特征在于,查询所述调用对应的调用类型还包括:

当查询调用的数据是系统数据时,不执行后续步骤,

当查询调用的数据是应用程序的应用数据时,执行后续步骤。

7. 一种电子设备,其特征在于,具有一操作系统,包括:

内核单元,是所述操作系统的一部分,为运行于所述电子设备上的应用程序提供对电子设备硬件的安全访问,以及,支持至少一个文件系统驱动模块运行;

文件系统驱动模块,用于支持以对应的数据组织格式存取数据;

检测单元,用于检测到有一文件系统驱动模块调用数据;

查询所述调用对应的调用类型;所述调用类型至少包括存放数据和提取数据,所述存

放数据对应一加密操作，所述提取数据对应一解密操作；

数据安全单元，用于根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理。

8. 根据权利要求 7 所述的电子设备，其特征在于，所述数据安全单元包括：

加密模块，用于在所述加密操作中，接收所述应用程序传输来的明文数据，

调用一加密算法，对所述明文数据进行加密后生成密文数据，

将所述密文数据存放到所述应用程序对应的存储单元中。

9. 根据权利要求 7 所述的电子设备，其特征在于，所述数据安全单元包括：

解密模块，用于在所述解密操作中，找到所述应用程序对应的存储单元，并调用所述存储单元中的密文数据，

调用一解密算法，对所述密文数据进行解密后生成明文数据；

通知所述应用程序处理所述明文数据。

10. 根据权利要求 7 所述的电子设备，其特征在于，还包括：

BOOT 单元，用于在所述电子设备上电启动之后，当处于 BOOT LOADER 阶段时，接收输入的密钥，所述密钥是所述加密操作的加密密钥，以及解密操作的解密密钥。

## 一种实现数据存储安全性的方法和电子设备

### 技术领域

[0001] 本发明涉及数据安全技术,特别是指一种实现数据存储安全性的方法和电子设备。

### 背景技术

[0002] 电子设备 - 特别是智能移动终端得到了广泛的应用,很多个人隐私数据都会存储在电子设备内 ;移动互联网技术普及之后,电子设备的安全性显得尤为重要。

[0003] 现有对于电子设备的数据进行安全保护的技术中,对数据的加密几乎都是在应用层实现的。

[0004] 现有技术存在如下问题 :对数据的加密几乎都是在应用层实现,而对于的应用层进行安全性攻击是一个技术相对简单且普遍存在的问题,因此数据的安全性和完整性得不到保证。

### 发明内容

[0005] 本发明要解决的技术问题是提供一种实现数据存储安全性的方法和电子设备,用于解决现有技术中,对数据的加密几乎都是在应用层实现,无法有效防范网络攻击,数据的安全性和完整性得不到保证的缺陷。

[0006] 为解决上述技术问题,本发明的实施例提供一种实现数据存储安全性的方法,应用于电子设备,所述电子设备中包括 :一内核单元,是所述电子设备的操作系统的一部分,为运行于所述电子设备上的应用程序提供对电子设备硬件的安全访问,以及,支持至少一个文件系统驱动模块运行 ;所述文件系统驱动模块支持以对应的数据组织格式存取数据 ;方法包括 :检测到有一文件系统驱动模块调用数据 ;查询所述调用对应的调用类型 ;所述调用类型至少包括存放数据和提取数据,所述存放数据对应一加密操作,所述提取数据对应一解密操作 ;根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理。

[0007] 所述的方法中,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理,具体包括 :在所述加密操作中,接收所述应用程序传输来的明文数据,调用一加密算法,对所说明文数据进行加密后生成密文数据,将所述密文数据存放到所述应用程序对应的存储单元中。

[0008] 所述的方法中,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理,具体包括 :在所述解密操作中,找到所述应用程序对应的存储单元,并调用所述存储单元中的密文数据,调用一解密算法,对所述密文数据进行解密后生成明文数据 ;通知所述应用程序处理所说明文数据。

[0009] 所述的方法中,检测到有一文件系统驱动模块调用数据,之前还包括 :在所述电子设备上电启动之后,当处于 BOOT LOADER 阶段时,接收输入的密钥,所述密钥是所述加密操作的加密密钥,以及解密操作的解密密钥。

[0010] 所述的方法中,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理,具体包括:检测到当前没有可以使用的密钥,提示需要通过电子设备接口接收来自一 SIM 卡的密钥。

[0011] 所述的方法中,查询所述调用对应的调用类型还包括:当查询调用的数据是系统数据时,不执行后续步骤,当查询调用的数据是应用程序的应用数据时,执行后续步骤。

[0012] 一种电子设备,具有一操作系统,包括:内核单元,是所述操作系统的一部分,为运行于所述电子设备上的应用程序提供对电子设备硬件的安全访问,以及,支持至少一个文件系统驱动模块运行;文件系统驱动模块,用于支持以对应的数据组织格式存取数据;检测单元,用于检测到有一文件系统驱动模块调用数据;查询所述调用对应的调用类型;所述调用类型至少包括存放数据和提取数据,所述存放数据对应一加密操作,所述提取数据对应一解密操作;数据安全单元,用于根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行处理。

[0013] 所述的电子设备中,所述数据安全单元包括:加密模块,用于在所述加密操作中,接收所述应用程序传输来的明文数据,调用一加密算法,对所说明文数据进行加密后生成密文数据,将所述密文数据存放到所述应用程序对应的存储单元中。

[0014] 所述的电子设备中,所述数据安全单元包括:解密模块,用于在所述解密操作中,找到所述应用程序对应的存储单元,并调用所述存储单元中的密文数据,调用一解密算法,对所述密文数据进行解密后生成明文数据;通知所述应用程序处理所说明文数据。

[0015] 所述的电子设备中,还包括:BOOT 单元,用于在所述电子设备上电启动之后,当处于 BOOT LOADER 阶段时,接收输入的密钥,所述密钥是所述加密操作的加密密钥,以及解密操作的解密密钥。

[0016] 本发明的上述技术方案的有益效果如下:在内核支持一文件系统驱动模块对数据进行调用的过程中,在内核中实现对数据的加密解密操作,且这一加密解密操作对于用户是不可见的,在不影响使用电子设备的其他功能的同时,提高了数据安全性。

## 附图说明

[0017] 图 1 表示一种实现数据存储安全性的方法流程示意图;

[0018] 图 2 表示电子设备内部功能逻辑分布示意图;

[0019] 图 3 表示一种电子设备的内部结构示意图。

## 具体实施方式

[0020] 为使本发明要解决的技术问题、技术方案和优点更加清楚,下面将结合附图及具体实施例进行详细描述。

[0021] 操作系统(Operating System, OS)是管理电子设备硬件与程序的系统级程序,其管理配置内存,决定系统资源供需的优先次序,控制输入与输出,管理网络与文件系统,提供与系统交互的接口等。

[0022] 内核是操作系统的根本部分,由于直接对硬件操作是非常复杂的,所以内核通常提供一种硬件抽象的方法来完成这些操作,这种硬件抽象隐藏了硬件操作的复杂性,为应用程序和硬件之间提供了简洁统一的接口,使设计应用程序更为简单;内核包括管理存储

器、文件系统、外设和系统资源的各个功能部分,提供硬件抽象层、磁盘及文件系统控制、多任务并行处理等功能;内核支持运行进程,并提供进程间的通信,为应用程序提供对计算机硬件的安全访问,这种安全访问是有限访问,并且内核决定一个应用程序在什么时候对某个硬件操作多长时间。内核不是完整的操作系统,一个基于 Linux 内核的操作系统称为 Linux 操作系统或是 GNU/Linux。

[0023] 本发明实施例提供一种实现数据存储安全性的方法,应用于电子设备,如图 1 所示,电子设备中包括:

[0024] 一内核单元,是所述电子设备的操作系统的一部分,为运行于所述电子设备上的应用程序提供对电子设备硬件的安全访问,以及,支持至少一个文件系统驱动模块运行;所述文件系统驱动模块支持以对应的数据组织格式存取数据;

[0025] 方法包括:

[0026] 步骤 101,检测到有一文件系统驱动模块调用数据;

[0027] 步骤 102,查询所述调用对应的调用类型;所述调用类型至少包括存放数据和提取数据,所述存放数据对应一加密操作,所述提取数据对应一解密操作;

[0028] 步骤 103,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行加密或者解密。

[0029] 应用所提供的技术方案,在内核支持一文件系统驱动模块对数据进行调用的过程中,在内核中实现对数据的加密解密操作,且这一加密解密操作对于用户是不可见的,在不影响使用电子设备的其他功能的同时,提高了数据安全性。

[0030] 电子设备涉及的数据包括:应用数据和系统数据,应用数据中包括 Cache 数据,应用程序使用的数据,以及用户数据;系统数据是系统程序-例如操作系统使用的数据,主要记录了电子设备的各种状态参数的值;其中,未加密的应用数据称为明文数据,加密后的应用数据称为密文数据。文件系统驱动模块支持以对应的数据组织格式存取应用数据和系统数据。

[0031] 在一个优选实施例中,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行加密或者解密,具体包括:

[0032] 在所述加密操作中,接收所述应用程序传输来的明文数据,调用一加密算法,对所说明文数据进行加密后生成密文数据,将所述密文数据存放到所述应用程序对应的存储单元中。

[0033] 在一个优选实施例中,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行加密或者解密,具体包括:

[0034] 在所述解密操作中,找到所述应用程序对应的存储单元,并调用所述存储单元中的密文数据,调用一解密算法,对所述密文数据进行解密后生成明文数据;通知所述应用程序处理所说明文数据。

[0035] 在一个优选实施例中,查询所述调用对应的调用类型还包括:当查询调用的数据是系统数据时,不执行后续步骤;

[0036] 当查询调用的数据是应用程序的应用数据时,执行后续步骤。

[0037] 在电子设备中,存储单元包括若干个分区,其中,有的分区存放应用数据,有的分区存放系统数据。

- [0038] 当查询调用的数据是系统数据时,不对系统数据进行加密或者解密;
- [0039] 当查询调用的数据是应用程序的应用数据时,如果是存放应用数据,则进行加密操作,如果是提取应用数据,则进行解密操作。
- [0040] 在一个优选实施例中,检测到有一文件系统驱动模块调用数据,之前还包括:
- [0041] 在所述电子设备上电启动之后,当处于 BOOT LOADER 阶段时,接收输入的密钥,所述密钥是加密操作的加密密钥,以及解密操作的解密密钥。
- [0042] 在一个优选实施例中,根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块当前调用的数据进行加密或者解密,具体包括:
- [0043] 检测到当前没有可以使用的密钥,提示需要通过电子设备接口接收来自一 SIM 卡的密钥。
- [0044] 在电子设备中,如图 2 所示,电子设备内部的用户区中运行应用程序,不同的应用程序可能使用到不同的文件系统驱动模块,例如 FAT 文件系统、YAFFS 文件系统、EXT 文件系统和 NTFS 文件系统等。
- [0045] 不同的文件系统驱动模块均处于内核单元中运行,加密操作或者解密操作也处于内核单元中运行,即,在内核单元中执行加密操作或者解密操作,文件系统驱动模块均支持加密操作或者解密操作;
- [0046] 当应用程序需要存取应用数据时,会调用处于内核单元中的文件系统驱动模块,任何一个文件系统驱动模块在进行数据存取的过程中,可以对明文数据执行加密操作,或者对密文数据执行解密操作。
- [0047] 在一个应用场景中,电子设备具体是移动终端,移动终端上电后的工作流程包括:
- [0048] 步骤 201,移动终端上电,电源开始向主板和其它器件供电,由于此时电压不稳定,主板上的控制芯片组会向 CPU 发出并保持一个重置 (RESET) 信号,让 CPU 自动恢复到初始状态,但 CPU 此刻不会马上执行指令。
- [0049] 步骤 202,系统引导加载 (BOOT LOADER) 首先进行 CPU、内存、存储控制器等的关键设备初始化操作。其中,BOOT LOADER 是在操作系统内核运行之前运行的一段小程序,这一段小程序可以初始化硬件设备、建立内存空间的映射图,从而将系统的软硬件环境带到一个合适的状态,以便为最终调用操作系统内核准备好正确的环境。
- [0050] 步骤 203,系统 BOOT LOADER,初始化显卡、显示屏及触摸屏设备,此时显卡都会在屏幕上显示出一些初始化厂商 LOGO。
- [0051] 并且,处于这一BOOT LOADER阶段时,显示一输入密钥的界面,提示用户输入密钥;移动终端接收输入的密钥,所述密钥是所述加密操作的加密密钥,解密操作的解密密钥。
- [0052] 步骤 205,系统 BOOT LOADER 加载操作系统的内核单元,准备将移动终端的控制权移交给操作系统;具体包括:
- [0053] 系统 BOOT LOADER 更新传给操作系统内核单元的信息,包括设备信息、内存大小、分区信息等,这些信息通过参数传给内核单元。
- [0054] 步骤 206,系统 BOOT LOADER 的启动代码最后将跳转到内核单元,完成控制权的出让,即将控制权移交给操作系统。
- [0055] 步骤 207,操作系统初始化一些重要的系统数据,然后显示出操作系统的界面,并

继续进行图形用户界面 (GUI) 部分的引导和初始化工作。

[0056] 步骤 208, 启动一个或者多个应用程序, 查询所述调用对应的调用类型, 该应用程序的调用类型具体是调用应用数据。

[0057] 步骤 209, 在解密操作中, 找到应用程序对应的存储单元的用户区, 并调用用户区中的密文数据,

[0058] 调用一解密算法, 对所述密文数据进行解密后生成明文数据; 其中, 所采用的密钥来自步骤 203 中在 BOOT LOADER 阶段由用户输入的密钥;

[0059] 通知应用程序处理所说明文数据。

[0060] 步骤 210, 执行加密操作, 在加密操作中, 接收所述应用程序传输来的明文数据,

[0061] 调用一加密算法, 对明文数据进行加密后生成密文数据, 存放到存储单元的用户区。

[0062] 本发明实施例提供的技术方案, 不仅可以应用在移动终端, 还可以应用在台式的电子设备中, 例如计算机等设备中均可以对应用数据进行加密操作或者解密操作, 在一个应用场景中, 计算机的工作流程包括:

[0063] 步骤 301, 电子设备上电, 电源开始向主板和其它设备供电, 由于此时电压不稳定, 主板上的控制芯片组会向 CPU 发出并保持一个重置 (RESET) 信号, 让 CPU 自动恢复到初始状态, 但 CPU 此刻不会马上执行指令。

[0064] 步骤 302, 系统 BIOS 的启动代码进行上电后自检 (POST), POST 的主要检测电子设备中一些如内存和显卡等的关键设备是否存在和正常工作。

[0065] 步骤 303, 系统 BIOS 查找显卡 BIOS, 例如存放显卡 BIOS 的 ROM 芯片的起始地址通常设在 C0000H 处, 系统 BIOS 在这个起始地址找到显卡 BIOS 之后就调用它的初始化代码, 由显卡 BIOS 来初始化显卡, 此时显卡都会在屏幕上显示出一些初始化信息, 介绍生产厂商、图形芯片类型等内容。

[0066] 并且, 处于这一 BIOS 阶段时, 显示一输入密钥的界面, 提示用户输入密钥; 电子设备接收输入的密钥, 所述密钥是所述加密操作的加密密钥, 解密操作的解密密钥。

[0067] 步骤 304, 系统 BIOS 检测和显示 CPU 的类型和工作频率, 直至所有硬件都已经检测配置完毕。

[0068] 步骤 305, 系统 BIOS 与操作系统的内核单元进行交互, 准备将电子设备的控制权移交给操作系统; 具体包括:

[0069] 系统 BIOS 更新扩展系统配置数据 (ESCD, Extended System Configuration Data), ESCD 是系统 BIOS 用来与操作系统交换硬件配置信息的一种手段, 这些数据被存放在 CMOS 之中。

[0070] 步骤 306, 系统 BIOS 的启动代码将进行最后一项工作, 即根据指定的启动顺序从 USB、硬盘或光驱启动。

[0071] 步骤 307, 操作系统首先初始化一些重要的系统数据, 然后显示出操作系统的界面, 并继续进行图形用户界面 (GUI) 部分的引导和初始化工作。

[0072] 步骤 308, 启动一个或者多个应用程序, 查询所述调用对应的调用类型, 该应用程序的调用类型具体是调用应用数据。

[0073] 步骤 309, 在解密操作中, 找到应用程序对应的存储单元的用户区, 并调用用户区

中的密文数据，

[0074] 调用一解密算法,对密文数据进行解密后生成明文数据 ;其中,所采用的密钥来自步骤 303 中在 BIOS 阶段由用户输入的密钥；

[0075] 通知应用程序处理明文数据。

[0076] 步骤 310,执行加密操作,在加密操作中,接收应用程序传输来的明文数据,调用一加密算法,对明文数据进行加密后生成密文数据,存放到存储单元的用户区。

[0077] 本发明实施例提供一种电子设备,如图 3 所示,具有一操作系统,包括：

[0078] 内核单元 01,是所述操作系统的一部分,为运行于所述电子设备上的应用程序提供对电子设备硬件的安全访问,以及,支持至少一个文件系统驱动模块 02 运行；

[0079] 文件系统驱动模块 02,在所述内核单元 01 中运行,用于支持所述应用程序的数据以对应的数据组织格式进行存取；

[0080] 检测单元 03,用于检测到有一文件系统驱动模块 02 调用数据；

[0081] 查询所述调用对应的调用类型 ;所述调用类型至少包括存放数据和提取数据,所述存放数据对应一加密操作,所述提取数据对应一解密操作；

[0082] 数据安全单元 04,在所述内核单元 01 中运行,用于根据所述调用类型对应的加密操作或者解密操作对所述文件系统驱动模块 02 当前调用的数据进行处理。

[0083] 在一个优选实施例中,电子设备中的数据安全单元 04 包括：

[0084] 加密模块 041,用于在所述加密操作中,接收所述应用程序传输来的明文数据,

[0085] 调用一加密算法,对所述明文数据进行加密后生成密文数据,

[0086] 将所述密文数据存放到所述应用程序对应的存储单元 05 中。

[0087] 在一个优选实施例中,数据安全单元 04 包括：

[0088] 解密模块 042,用于在所述解密操作中,找到所述应用程序对应的存储单元 05,并调用所述存储单元 05 中的密文数据,

[0089] 调用一解密算法,对所述密文数据进行解密后生成明文数据 ;通知所述应用程序处理所说明文数据。

[0090] BOOT 单元,用于在所述电子设备上电启动之后,当处于 BOOT LOADER 阶段时,接收输入的密钥,所述密钥是所述加密操作的加密密钥,以及解密操作的解密密钥。

[0091] 采用本方案之后的优势是 :对电子设备涉及的数据的加解密均在内核中实现,加解密操作对于用户是不可见的,所有的读写数据均由内核中的加解密过滤驱动完成,并且该技术可选的加密应用数据,对于系统数据不进行加解密,在不影响用户使用电子设备的其他体验的同时,提高了数据安全性。

[0092] 以上所述是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明所述原理的前提下,还可以作出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

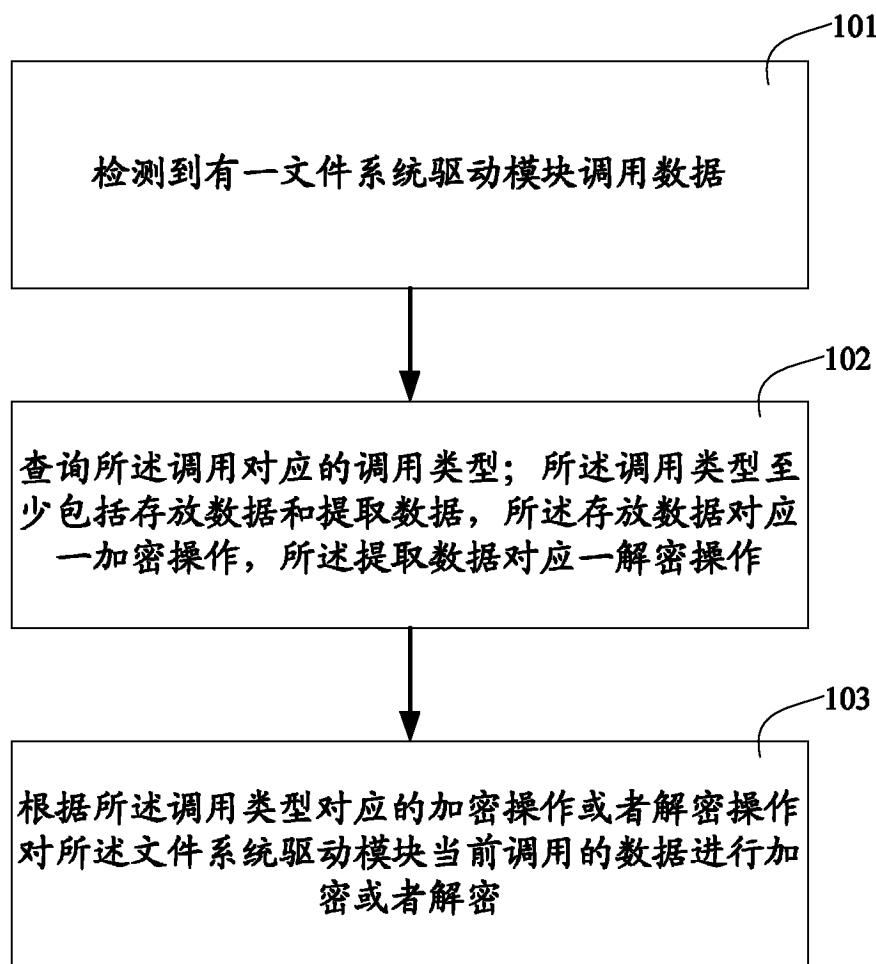


图 1

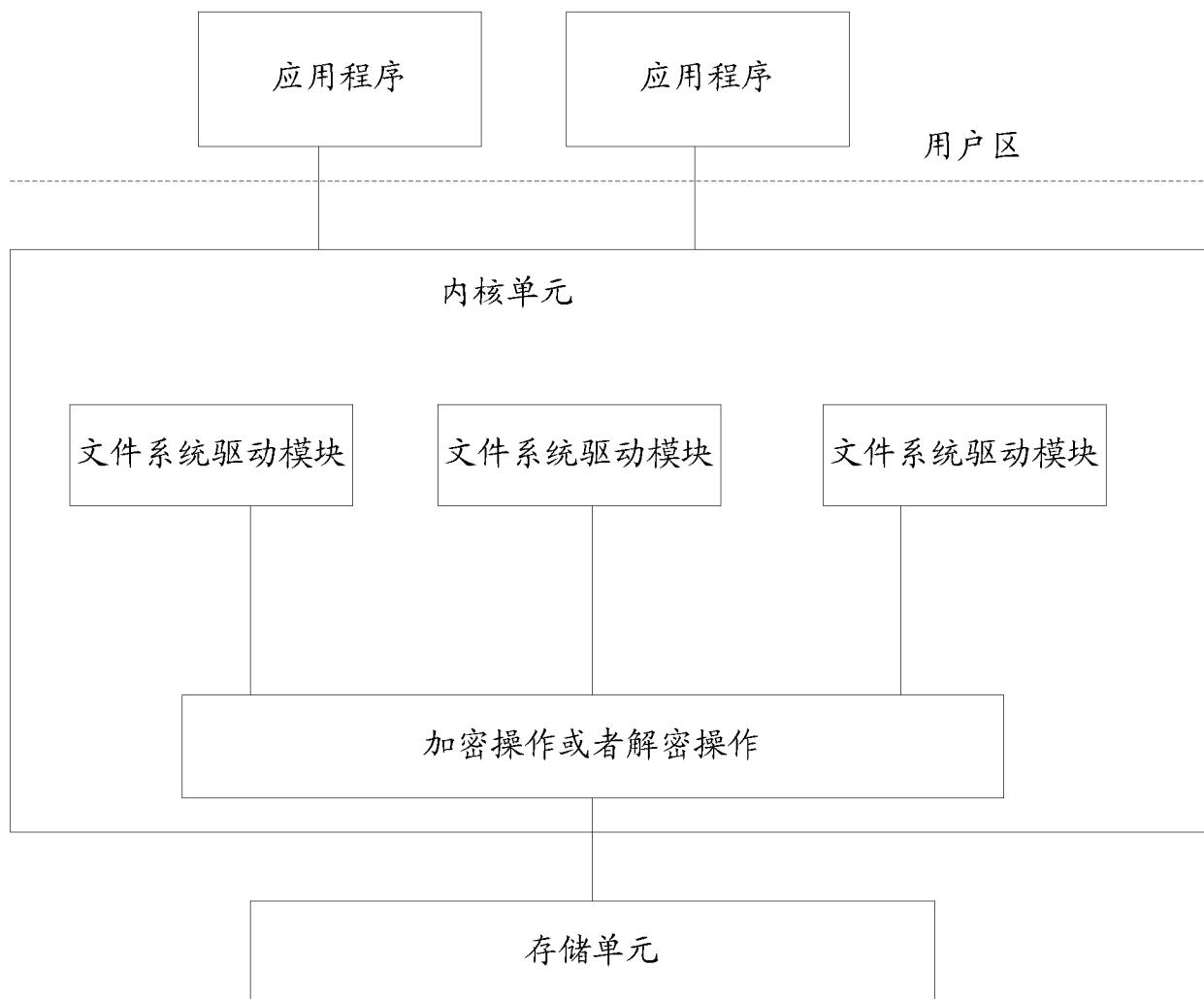


图 2

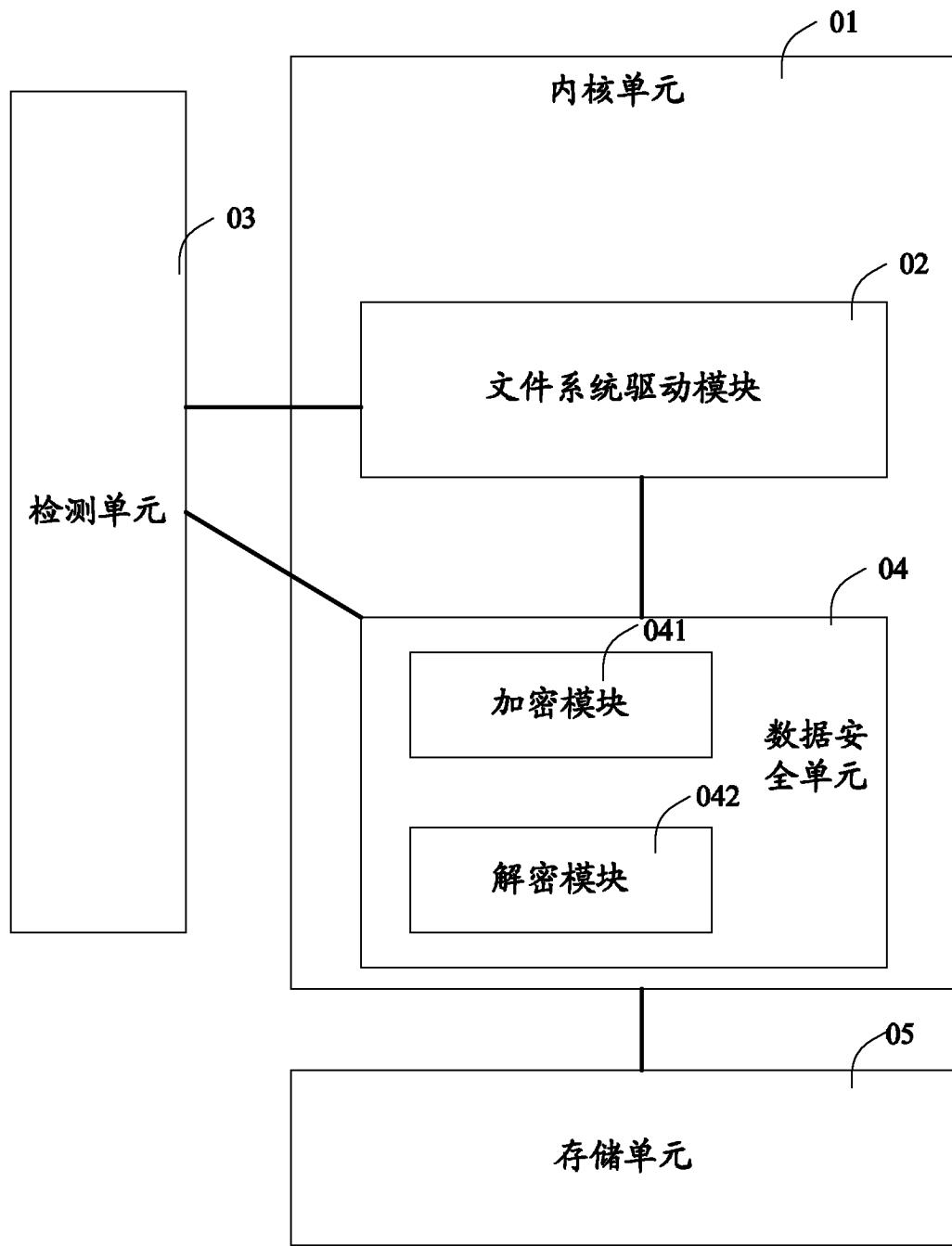


图 3