(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 108718313 A
(43)申请公布日 2018.10.30

(21)申请号 201810544822.4

(22)申请日 2018.05.31

(71)申请人 深圳市文鼎创数据科技有限公司
地址 518000 广东省深圳市南山区粤海街道科丰路2号特发信息港大厦A栋七楼南701-708单元

(72)发明人 冯灼坤

(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 官建红

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/12(2013.01)

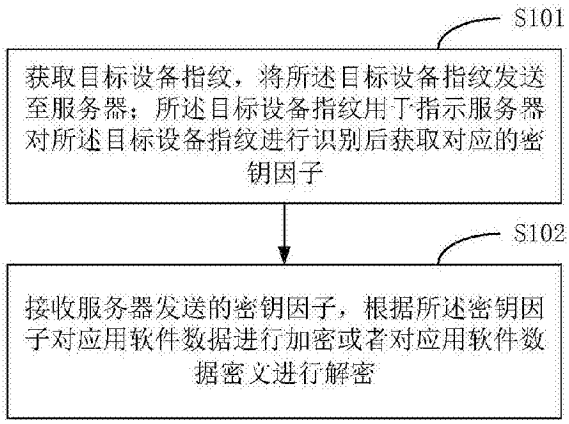
权利要求书1页 说明书8页 附图2页

(54)发明名称

应用软件数据安全使用方法、终端设备及服务器

(57)摘要

本发明涉及计算机技术领域，提供了一种应用软件数据安全使用方法、终端设备及服务器。该方法包括：获取目标设备指纹，将所述目标设备指纹发送至服务器；所述目标设备指纹用于指示服务器对所述目标设备指纹进行识别后获取对应的密钥因子；接收服务器发送的密钥因子，根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。本发明将密钥因子保存于服务器中，相对于密钥因子保存在客户端更安全，不容易被破解；通过设备指纹获取对应的密钥因子，能够免去用户记忆及输入密码的操作，极大简化用户操作，进而提高用户对应用软件数据进行加密的积极性，提升用户体验度。



CN 108718313 A

1.一种应用软件数据安全使用方法，其特征在于，应用于客户端，包括：

获取目标设备指纹，将所述目标设备指纹发送至服务器；所述目标设备指纹用于指示服务器对所述目标设备指纹进行识别后获取对应的密钥因子；

接收服务器发送的密钥因子，根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

2.如权利要求1所述的应用软件数据安全使用方法，其特征在于，所述密钥因子包括：对称密钥、对称密钥生成因子、非对称密钥、非对称密钥生成因子、白盒算法加密表、白盒算法解密表中的一种或多种。

3.如权利要求2所述的应用软件数据安全使用方法，其特征在于，所述密钥因子包括白盒算法解密表，所述应用软件数据安全使用方法还包括：

接收服务器发送的应用软件数据密文并保存于客户端，以便客户端在需要使用应用软件数据时，根据所述白盒算法解密表以及预设白盒算法解密所述应用软件数据密文得到应用软件数据。

4.如权利要求1所述的应用软件数据安全使用方法，其特征在于，所述目标设备指纹由目标设备中的可变信息及不可变信息组成。

5.一种应用软件数据安全使用方法，其特征在于，应用于服务器，包括：

接收客户端发送的目标设备指纹；

对所述目标设备指纹进行识别后获取对应的密钥因子，并将所述密钥因子发送至客户端，以便客户端根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

6.如权利要求5所述的应用软件数据安全使用方法，其特征在于，所述对所述目标设备指纹进行识别后获取对应的密钥因子包括：

根据预设分类算法对所述目标设备指纹进行分类，根据分类结果获取对应的密钥因子。

7.如权利要求5所述的应用软件数据安全使用方法，其特征在于，所述密钥因子包括白盒算法解密表，所述应用软件数据安全使用方法还包括：

生成应用软件数据，并根据所述白盒算法解密表对应的密钥对所述应用软件数据进行加密得到应用软件数据密文，将所述应用软件数据密文发送至客户端。

8.一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至4任一项所述方法的步骤。

9.一种服务器，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求5至7任一项所述方法的步骤。

10.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至7任一项所述方法的步骤。

应用软件数据安全使用方法、终端设备及服务器

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种应用软件数据安全使用方法、终端设备及服务器。

背景技术

[0002] 现有对应用软件数据进行加密的方式主要有两种，通过软件预置密钥进行加密或者用户输入加密密钥进行加密。由于应用软件运行于比较开放的环境，预置密钥很容易被破解，安全性较低。用户输入密钥需要用户记住并输入密钥，操作复杂，且容易与用户记忆的其他密钥相混淆，用户体验不好。

发明内容

[0003] 有鉴于此，本发明实施例提供了应用软件数据安全使用方法、终端设备及服务器，以解决目前应用软件数据的加密方式由于容易破解或操作复杂导致用户体验差的问题。

[0004] 本发明实施例的第一方面提供了应用软件数据安全使用方法，应用于客户端，包括：

[0005] 获取目标设备指纹，将所述目标设备指纹发送至服务器；所述目标设备指纹用于指示服务器对所述目标设备指纹进行识别后获取对应的密钥因子；

[0006] 接收服务器发送的密钥因子，根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0007] 本发明实施例的第二方面提供了应用软件数据安全使用方法，应用于服务器，包括：

[0008] 接收客户端发送的目标设备指纹；

[0009] 对所述目标设备指纹进行识别后获取对应的密钥因子，并将所述密钥因子发送至客户端，以便客户端根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0010] 本发明实施例的第三方面提供了终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现第一方面中的应用软件数据安全使用方法。

[0011] 本发明实施例的第四方面提供了服务器，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现第二方面中的应用软件数据安全使用方法。

[0012] 本发明实施例的第五方面提供了计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现第一方面或第二方面中的应用软件数据安全使用方法。

[0013] 本发明实施例与现有技术相比存在的有益效果是：通过获取目标设备指纹，将目标设备指纹发送至服务器；目标设备指纹用于指示服务器对目标设备指纹进行识别后获取

对应的密钥因子；接收服务器发送的密钥因子，根据密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。本发明实施例将密钥因子保存于服务器中，相对于密钥因子保存在客户端更安全，不容易被破解；通过设备指纹获取对应的密钥因子，能够免去用户记忆及输入密码的操作，极大简化用户操作，进而提高用户对应用软件数据进行加密的积极性，提升用户体验度。

附图说明

[0014] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0015] 图1是本发明实施例一个提供的应用软件数据安全使用方法的实现流程图；

[0016] 图2是本发明另一实施例提供的应用软件数据安全使用方法的实现流程图；

[0017] 图3是本发明一个实施例提供的应用软件数据安全使用装置的示意图；

[0018] 图4是本发明另一实施例提供的应用软件数据安全使用装置的示意图；

[0019] 图5是本发明实施例提供的终端设备的示意图；

[0020] 图6是本发明实施例提供的服务器的示意图。

具体实施方式

[0021] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本发明实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本发明。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本发明的描述。

[0022] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0023] 图1为本发明一个实施例提供的应用软件数据安全使用方法的实现流程图，该方法应用于客户端，详述如下：

[0024] 在S101中，获取目标设备指纹，将所述目标设备指纹发送至服务器；所述目标设备指纹用于指示服务器对所述目标设备指纹进行识别后获取对应的密钥因子。

[0025] 在本实施例中，目标设备指纹为客户端设备的设备指纹。客户端获取设备的目标设备指纹，将目标设备指纹发送至服务器。服务器可以接收客户端发送的目标设备指纹，对目标设备指纹进行识别，获取目标设备指纹对应的密钥因子，并将密钥因子返回至客户端。

[0026] 可选地，所述密钥因子包括：对称密钥、对称密钥生成因子、非对称密钥、非对称密钥生成因子、白盒算法加密表、白盒算法解密表中的一种或多种。

[0027] 可选地，所述目标设备指纹由目标设备中的可变信息及不可变信息组成。

[0028] 其中，不可变信息为目标设备的一些固有的、较难篡改的、唯一的设备标识，比如设备的硬件ID(Identity)，IMEI(International Mobile Equipment Identity，国际移动设备标志)编号，如网卡的MAC(Media Access Control)地址等。可变信息为随着用户使用可能发生变化的目标设备的特征，例如目标设备上安装的应用软件个数、应用软件种类、目标设备的系统设置参数、通讯录、通话记录、通知消息等。

[0029] 服务器可以对目标设备指纹进行识别，识别出该目标设备指纹对应的设备，并在数据库中获取到该设备对应的密钥因子。

[0030] 在S102中，接收服务器发送的密钥因子，根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0031] 在本实施例中，应用软件数据为应用软件的敏感数据。客户端接收服务器发送的密钥因子，可以根据密钥因子对应用软件数据进行加密，得到应用软件数据密文；也可以根据密钥因子对应用软件数据密文进行解密，得到应用软件数据。

[0032] 本发明实施例通过获取目标设备指纹，将目标设备指纹发送至服务器；目标设备指纹用于指示服务器对目标设备指纹进行识别后获取对应的密钥因子；接收服务器发送的密钥因子，根据密钥因子对应用软件数据加密或者对应用软件数据密文进行解密。本发明实施例将密钥因子保存于服务器中，相对于密钥因子保存在客户端更安全，不容易被破解；通过设备指纹获取对应的密钥因子，能够免去用户记忆及输入密码的操作，极大简化用户操作，进而提高用户对应用软件数据进行加密的积极性，提升用户体验度。

[0033] 作为本发明的一个实施例，所述密钥因子包括白盒算法解密表，所述应用软件数据安全使用方法还包括：

[0034] 接收服务器发送的应用软件数据密文并保存于客户端，以便客户端在需要使用应用软件数据时，根据所述白盒算法解密表以及预设白盒算法解密所述应用软件数据密文得到应用软件数据。

[0035] 在本实施例中，服务器可以对应用软件数据进行加密得到应用软件数据密文，并将应用软件数据密文发送至客户端。客户端可以接收并保存服务器发送的应用软件数据密文。客户端在需要使用应用软件数据时，可以根据白盒算法解密表及预设白盒算法对保存的应用软件数据密文进行解密，从而得到应用软件数据。

[0036] 图2为本发明另一实施例提供的应用软件数据安全使用方法的实现流程图，该方法应用于服务器，详述如下：

[0037] 在S201中，接收客户端发送的目标设备指纹。

[0038] 在本实施例中，客户端获取设备的目标设备指纹，可以将目标设备指纹加密发送至服务器。服务器可以接收客户端发送的目标设备指纹。

[0039] 在S202中，对所述目标设备指纹进行识别后获取对应的密钥因子，并将所述密钥因子发送至客户端，以便客户端根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0040] 在本实施例中，服务器对目标设备指纹进行识别，获取目标设备指纹对应的密钥因子，并将密钥因子返回至客户端。客户端接收服务器发送的密钥因子，根据密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0041] 本发明实施例通过获取目标设备指纹，将目标设备指纹发送至服务器；目标设备指纹用于指示服务器对目标设备指纹进行识别后获取对应的密钥因子；接收服务器发送的密钥因子，根据密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。本发明实施例将密钥因子保存于服务器中，相对于密钥因子保存在客户端更安全，不容易被破解；通过设备指纹获取对应的密钥因子，能够免去用户记忆及输入密码的操作，极大简化用户操作，进而提高用户对应用软件数据进行加密的积极性，提升用户体验度。

[0042] 可选地，S202中“对所述目标设备指纹进行识别后获取对应的密钥因子”包括：

[0043] 根据预设分类算法对所述目标设备指纹进行分类，根据分类结果获取对应的密钥因子。在本发明的一个实施例中，若分类结果不属于现有分类，则添加新分类并生成对应的密钥因子。

[0044] 作为本发明的一个实施例，所述密钥因子包括白盒算法解密表，所述应用软件数据安全使用方法还可以包括：

[0045] 生成应用软件数据，并根据所述白盒算法解密表对应的密钥对所述应用软件数据进行加密得到应用软件数据密文，将所述应用软件数据密文发送至客户端。在本发明的一个实施例中，服务器对所述目标设备指纹进行识别后，获取对应的传统加密算法密钥、白盒算法加密表、白盒算法解密表。白盒算法解密表对应的密钥，可以是白盒算法加密表或是传统加密算法密钥，所述根据所述白盒算法解密表对应的密钥对所述应用软件数据进行加密得到应用软件数据密文可以是根据白盒加密表及白盒加密算法对所述应用软件数据进行加密或者是根据传统加密算法密钥及传统加密算法对所述应用软件数据进行加密得到应用软件数据密文。

[0046] 本发明实施例通过获取目标设备指纹，将目标设备指纹发送至服务器；目标设备指纹用于指示服务器对目标设备指纹进行识别后获取对应的密钥因子；接收服务器发送的密钥因子，根据密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。本发明实施例将密钥因子保存于服务器中，相对于密钥因子保存在客户端更安全，不容易被破解；通过设备指纹获取对应的密钥因子，能够免去用户记忆及输入密码的操作，极大简化用户操作，进而提高用户对应用软件数据进行加密的积极性，提升用户体验度。

[0047] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0048] 对应于上文实施例所述的应用软件数据安全使用方法，图3示出了本发明一个实施例提供的应用软件数据安全使用装置的示意图。为了便于说明，仅示出了与本实施例相关的部分。

[0049] 参照图3，该装置应用于客户端，包括获取模块31和生成模块32。

[0050] 获取模块31，用于获取目标设备指纹，将所述目标设备指纹发送至服务器；所述目标设备指纹用于指示服务器对所述目标设备指纹进行识别后获取对应的密钥因子。

[0051] 生成模块32，用于接收服务器发送的密钥因子，根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0052] 可选地，所述密钥因子包括：对称密钥、对称密钥生成因子、非对称密钥、非对称密钥生成因子、白盒算法加密表、白盒算法解密表中的一种或多种。

[0053] 可选地，所述密钥因子包括白盒算法解密表，该装置还包括保存模块，保存模块用于：

[0054] 接收服务器发送的应用软件数据密文并保存于客户端，以便客户端在需要使用应用软件数据时，根据所述白盒算法解密表以及预设白盒算法解密所述应用软件数据密文得到应用软件数据。

[0055] 可选地，所述目标设备指纹由目标设备中的可变信息及不可变信息组成。

[0056] 本发明实施例通过获取目标设备指纹，将目标设备指纹发送至服务器；目标设备指纹用于指示服务器对目标设备指纹进行识别后获取对应的密钥因子；接收服务器发送的密钥因子，根据密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。本发明实施例将密钥因子保存于服务器中，相对于密钥因子保存在客户端更安全，不容易被破解；通过设备指纹获取对应的密钥因子，能够免去用户记忆及输入密码的操作，极大简化用户操作，进而提高用户对应用软件数据进行加密的积极性，提升用户体验度。

[0057] 对应于上文实施例所述的应用软件数据安全使用方法，图4示出了本发明另一实施例提供的应用软件数据安全使用装置的示意图。为了便于说明，仅示出了与本实施例相关的部分。

[0058] 参照图4，该装置应用于服务器，包括接收模块41和发送模块42。

[0059] 接收模块41，用于接收客户端发送的目标设备指纹。

[0060] 发送模块42，用于对所述目标设备指纹进行识别后获取对应的密钥因子，并将所述密钥因子发送至客户端，以便客户端根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0061] 可选地，发送模块42用于：

[0062] 根据预设分类算法对所述目标设备指纹进行分类，根据分类结果获取对应的密钥因子。

[0063] 可选地，所述密钥因子包括白盒算法解密表，该装置还包括加密模块，加密模块用于：

[0064] 生成应用软件数据，并根据所述白盒算法解密表对应的密钥对所述应用软件数据进行加密得到应用软件数据密文，将所述应用软件数据密文发送至客户端。

[0065] 本发明实施例通过获取目标设备指纹，将目标设备指纹发送至服务器；目标设备指纹用于指示服务器对目标设备指纹进行识别后获取对应的密钥因子；接收服务器发送的密钥因子，根据密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。本发明实施例将密钥因子保存于服务器中，相对于密钥因子保存在客户端更安全，不容易被破解；通过设备指纹获取对应的密钥因子，能够免去用户记忆及输入密码的操作，极大简化用户操作，进而提高用户对应用软件数据进行加密的积极性，提升用户体验度。

[0066] 图5是本发明一实施例提供的终端设备的示意图。如图5所示，该实施例的终端设备5包括：处理器50、存储器51以及存储在所述存储器51中并可在所述处理器50上运行的计算机程序52，例如程序。所述处理器50执行所述计算机程序52时实现上述各个方法实施例中的步骤，例如图1所示的步骤101至102。或者，所述处理器50执行所述计算机程序52时实现上述各装置实施例中各模块/单元的功能，例如图3所示模块31至32的功能。

[0067] 示例性的，所述计算机程序52可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器51中，并由所述处理器50执行，以完成本发明。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序52在所述终端设备5中的执行过程。例如，所述计算机程序52可以被分割成获取模块和生成模块，各模块具体功能如下：

[0068] 获取模块，用于获取目标设备指纹，将所述目标设备指纹发送至服务器；所述目标设备指纹用于指示服务器对所述目标设备指纹进行识别后获取对应的密钥因子；

[0069] 生成模块，用于接收服务器发送的密钥因子，根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0070] 所述终端设备5可以是桌上型计算机、笔记本、掌上电脑及手机等计算设备。所述终端设备可包括，但不仅限于，处理器50、存储器51。本领域技术人员可以理解，图5仅仅是终端设备5的示例，并不构成对终端设备5的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备还可以包括输入输出设备、网络接入设备、总线、显示器等。

[0071] 所称处理器50可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0072] 所述存储器51可以是所述终端设备5的内部存储单元，例如终端设备5的硬盘或内存。所述存储器51也可以是所述终端设备5的外部存储设备，例如所述终端设备5上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。进一步地，所述存储器51还可以既包括所述终端设备5的内部存储单元也包括外部存储设备。所述存储器51用于存储所述计算机程序以及所述终端设备所需的其他程序和数据。所述存储器51还可以用于暂时地存储已经输出或者将要输出的数据。

[0073] 图6是本发明一实施例提供的服务器的示意图。如图6所示，该实施例的服务器6包括：处理器60、存储器61以及存储在所述存储器61中并可在所述处理器60上运行的计算机程序62，例如程序。所述处理器60执行所述计算机程序62时实现上述各个方法实施例中的步骤，例如图2所示的步骤201至202。或者，所述处理器60执行所述计算机程序62时实现上述各装置实施例中各模块/单元的功能，例如图4所示模块41至42的功能。

[0074] 示例性的，所述计算机程序62可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器61中，并由所述处理器60执行，以完成本发明。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序62在所述服务器6中的执行过程。例如，所述计算机程序62可以被分割成接收模块和发送模块，各模块具体功能如下：

[0075] 接收模块，用于接收客户端发送的目标设备指纹；

[0076] 发送模块，用于对所述目标设备指纹进行识别后获取对应的密钥因子，并将所述密钥因子发送至客户端，以便客户端根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密。

[0077] 所述服务器可包括，但不仅限于，处理器60、存储器61。本领域技术人员可以理解，图6仅仅是服务器6的示例，并不构成对服务器6的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述服务器还可以包括输入输出设备、网络接入设备、总线、显示器等。

[0078] 所称处理器60可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路

(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0079] 所述存储器61可以是所述服务器6的内部存储单元,例如服务器6的硬盘或内存。所述存储器61也可以是所述服务器6的外部存储设备,例如所述服务器6上配备的插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)等。进一步地,所述存储器61还可以既包括所述服务器6的内部存储单元也包括外部存储设备。所述存储器61用于存储所述计算机程序以及所述服务器所需的其他程序和数据。所述存储器61还可以用于暂时地存储已经输出或者将要输出的数据。

[0080] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,仅以上述各功能单元、模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能单元、模块完成,即将所述装置的内部结构划分成不同的功能单元或模块,以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中,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单元中,上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。另外,各功能单元、模块的具体名称也只是为了便于相互区分,并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0081] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述或记载的部分,可以参见其它实施例的相关描述。

[0082] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0083] 在本发明所提供的实施例中,应该理解到,所揭露的装置/终端设备和方法,可以通过其它的方式实现。例如,以上所描述的装置/终端设备实施例仅仅是示意性的,例如,所述模块或单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口,装置或单元的间接耦合或通讯连接,可以是电性,机械或其它的形式。

[0084] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0085] 另外,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单元中,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单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0086] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或

使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括是电载波信号和电信信号。

[0087] 以上所述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

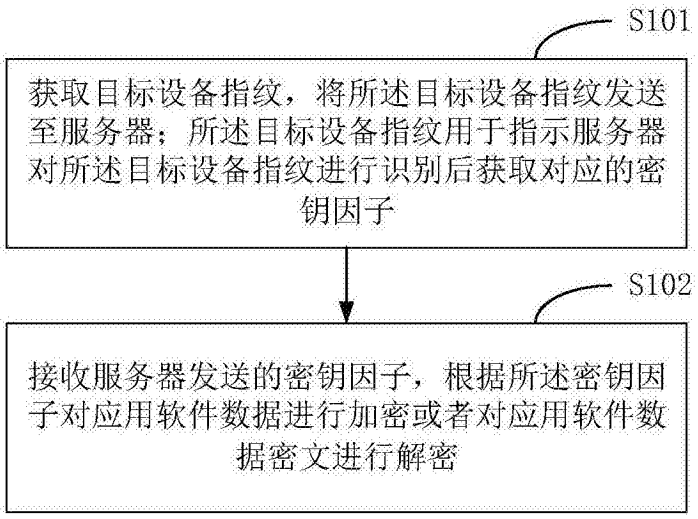

S101
获取目标设备指纹，将所述目标设备指纹发送至服务器；所述目标设备指纹用于指示服务器对所述目标设备指纹进行识别后获取对应的密钥因子
S102
接收服务器发送的密钥因子，根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密

图1

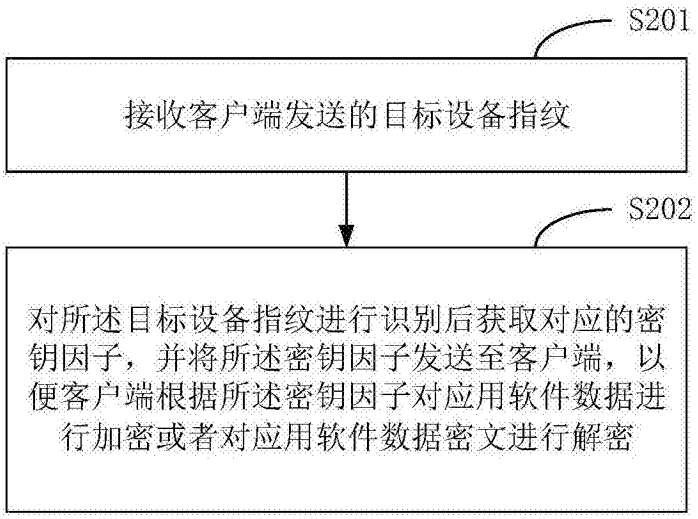

S201
接收客户端发送的目标设备指纹
S202
对所述目标设备指纹进行识别后获取对应的密钥因子，并将所述密钥因子发送至客户端，以便客户端根据所述密钥因子对应用软件数据进行加密或者对应用软件数据密文进行解密

图2

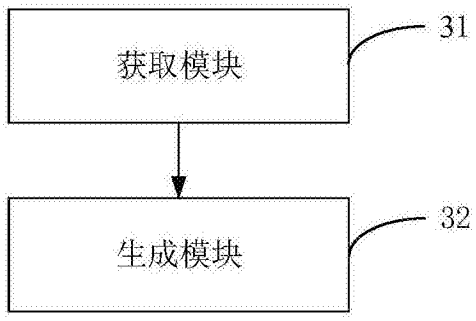

获取模块
31
生成模块
32

图3

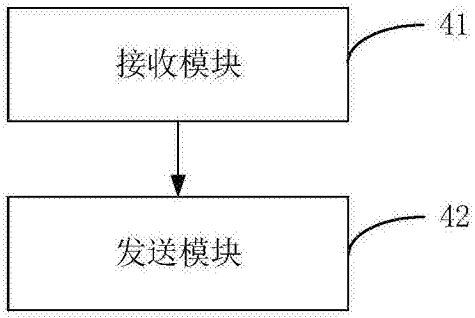

接收模块
41
发送模块
42

图4

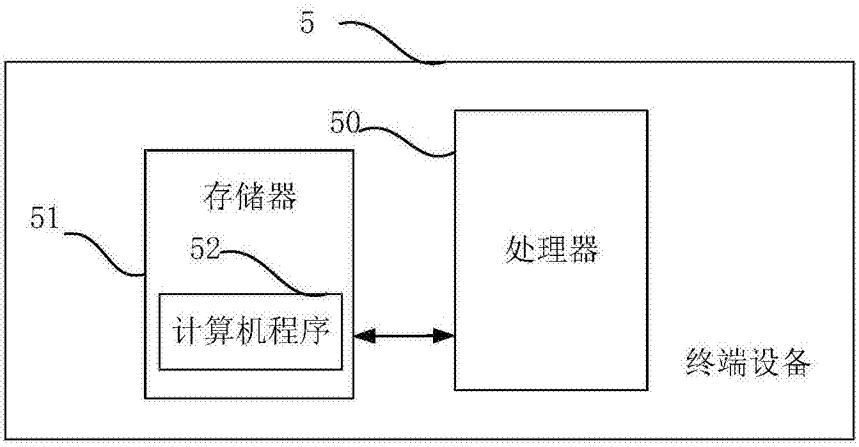

5
50
存储器
51
52
计算机程序
处理器
终端设备

图5

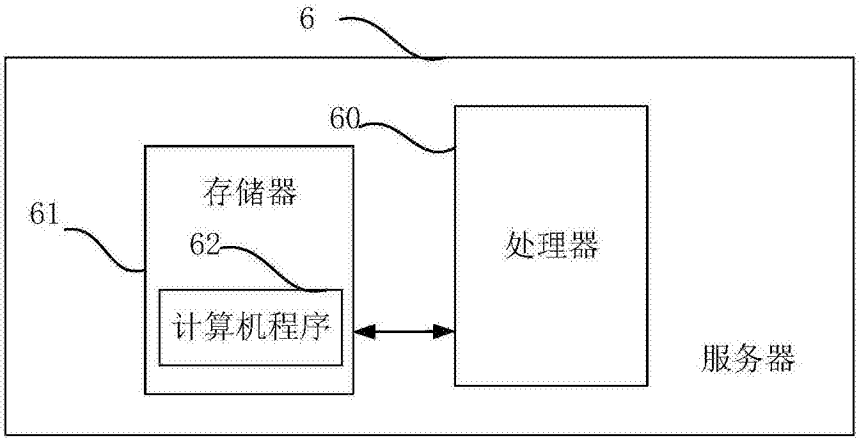

6
60
存储器
61
62
计算机程序
处理器
服务器

图6