(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114595465 A
(43)申请公布日 2022.06.07

(21)申请号 202011404254.1

(22)申请日 2020.12.04

(71)申请人 成都鼎桥通信技术有限公司
地址 610041 四川省成都市高新区天华二路219号天府软件园C区3栋3-5层

(72)发明人 孙洪波 冯小兵 张闯

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
专利代理师 朱颖 刘芳

(51)Int.Cl.
G06F 21/60(2013.01)

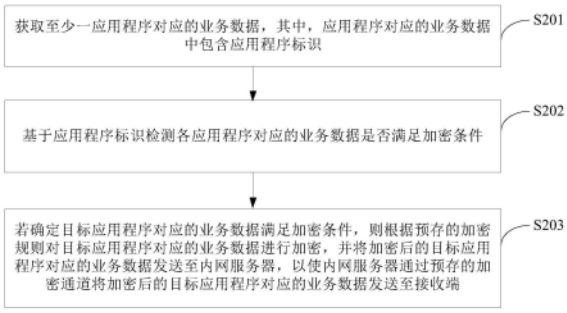
权利要求书2页 说明书9页 附图3页

(54)发明名称

数据加密处理方法、装置及电子设备

(57)摘要

本发明实施例提供了一种数据加密处理方法、装置及电子设备，所述方法应用于终端设备，具体包括：获取至少一应用程序对应的业务数据，其中，应用程序对应的业务数据中包含应用程序标识，基于应用程序标识检测各应用程序对应的业务数据是否满足加密条件，若确定目标应用程序对应的业务数据需加密传输，则根据预存的加密规则对目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至内网服务器，以使内网服务器通过预存的加密通道将加密后的目标应用程序对应的业务数据发送至接收端。该实施例提高了业务数据的安全性，进而保证了各业务的正常实现。



CN 114595465 A

1.一种数据加密处理方法,其特征在于,应用于终端设备,所述方法包括:

获取至少一应用程序对应的业务数据,其中,所述应用程序对应的业务数据中包含应用程序标识;

基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件;

若确定目标应用程序对应的业务数据满足所述加密条件,则根据预存的加密规则对所述目标应用程序对应的业务数据进行加密,并将加密后的目标应用程序对应的业务数据发送至内网服务器,以使内网服务器通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

2.根据权利要求1所述的方法,其特征在于,所述基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件,包括:

获取预存的应用程序标识列表;

判断所述应用程序标识是否在所述应用程序标识列表中;

若存在,则确定所述应用程序对应的业务数据满足加密条件。

3.根据权利要求1所述的方法,其特征在于,所述基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件,包括:

基于加密检测模型确定包含应用程序标识的各应用程序对应的业务数据是否需加密传输,其中,所述加密检测模型为通过包含应用程序标识的各应用程序对应的业务训练数据训练得到的。

4.根据权利要求1所述的方法,其特征在于,所述若确定目标应用程序对应的业务数据需加密传输,则根据预存的加密规则对所述目标应用程序对应的业务数据进行加密,包括:

若确定目标应用程序对应的业务数据需加密传输,则根据分组密码算法SM1、椭圆曲线公钥密码算法SM2、杂凑算法SM3、对称算法SM4、高级加密标准AES、公钥加密算法RSA,以及哈希Hash算法中的任意一种或多种对所述目标应用程序对应的业务数据进行加密。

5.根据权利要求1-4任一项所述的方法,其特征在于,在所述并将加密后的目标应用程序对应的业务数据发送至内网服务器,以使内网服务器通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端之后,还包括:

接收并显示所述内网服务器发送的发送成功提示。

6.一种数据加密处理方法,其特征在于,应用于内网服务器,所述方法包括:

接收终端设备发送的加密后的目标应用程序对应的业务数据,其中,所述加密后的目标应用程序对应的业务数据为根据预存的加密规则对所述目标应用程序对应的业务数据进行加密得到的;

通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

7.根据权利要求6所述的方法,其特征在于,所述通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端,包括:

通过预存的加密规则对应的专用加密通道对所述加密后的目标应用程序对应的业务数据发送至接收端。

8.一种数据加密处理装置,其特征在于,应用于终端设备,所述装置包括:

获取模块,用于获取至少一应用程序对应的业务数据,其中,所述应用程序对应的业务数据中包含应用程序标识;

处理模块，用于基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件；

所述处理模块，还用于若确定目标应用程序对应的业务数据需加密传输，则根据预存的加密规则对所述目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至内网服务器，以使内网服务器通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

9.一种数据加密处理装置，其特征在于，应用于内网服务器，所述装置包括：

接收模块，用于接收终端设备发送的加密后的目标应用程序对应的业务数据，其中，所述加密后的目标应用程序对应的业务数据为根据预存的加密规则对所述目标应用程序对应的业务数据进行加密得到的；

处理模块，用于通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

10.一种电子设备，其特征在于，包括：至少一个处理器和存储器；

所述存储器存储计算机执行指令；

所述至少一个处理器执行所述存储器存储的计算机执行指令，使得所述至少一个处理器执行如权利要求1至7任一项所述的数据加密处理方法。

11.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机执行指令，当处理器执行所述计算机执行指令时，实现如权利要求1至7任一项所述的数据加密处理方法。

12.一种计算机程序产品，包括计算机程序，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任一项所述的数据加密处理方法。

数据加密处理方法、装置及电子设备

技术领域

[0001] 本发明实施例涉及通信领域，尤其涉及一种数据加密处理方法、装置及电子设备。

背景技术

[0002] 随着互联网技术的发展以及各应用领域需求的不断细化，以终端设备为载体的行业应用也越来越普及，在带来便利的同时，对终端设备通信的安全性诉求也越来越迫切。

[0003] 在终端设备中可以安装有不同的应用程序，每个应用程序可以实现多种不同的业务，在实现业务的过程中，又可能涉及到文本、图像、声音、视频等业务数据的处理与传输。对应的，上述业务数据大多是基于通用的移动端框架生成的，业务数据生成之后，可以通过通用的标准网络协议将多媒体数据发送至接收端，接收端获取到业务数据之后，可以进一步对业务数据进行处理，进而实现相关的业务功能。

[0004] 然而，由于终端设备丢失、黑客入侵等因素，导致基于通用的移动端框架生成的业务数据存在被他人截获、篡改数据等风险，降低了业务数据的安全性，进而影响了各业务的正常实现。

发明内容

[0005] 本发明实施例提供一种数据加密处理方法、装置及电子设备，以提高数据的安全性。

[0006] 第一方面，本发明实施例提供一种数据加密处理方法，应用于终端设备，所述方法包括：

[0007] 获取至少一应用程序对应的业务数据，其中，所述应用程序对应的业务数据中包含应用程序标识；

[0008] 基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件；

[0009] 若确定目标应用程序对应的业务数据需加密传输，则根据预存的加密规则对所述目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至内网服务器，以使内网服务器通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

[0010] 可选的，所述基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件，包括：

[0011] 获取预存的应用程序标识列表；

[0012] 判断所述应用程序标识是否在所述应用程序标识列表中；

[0013] 若存在，则确定所述应用程序对应的业务数据满足加密条件。

[0014] 可选的，所述基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件，包括：

[0015] 基于加密检测模型确定包含应用程序标识的各应用程序对应的业务数据是否需加密传输，其中，所述加密检测模型为通过包含应用程序标识的各应用程序对应的业务训

练数据训练得到的。

[0016] 可选的，所述若确定目标应用程序对应的业务数据需加密传输，则根据预存的加密规则对所述目标应用程序对应的业务数据进行加密，包括：

[0017] 若确定目标应用程序对应的业务数据需加密传输，则根据分组密码算法SM1、椭圆曲线公钥密码算法SM2、杂凑算法SM3、对称算法SM4、高级加密标准AES、公钥加密算法RSA，以及哈希Hash算法中的任意一种或多种对所述目标应用程序对应的业务数据进行加密。

[0018] 可选的，在所述并将加密后的目标应用程序对应的业务数据发送至内网服务器，以使内网服务器通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端之后，还包括：

[0019] 接收并显示所述内网服务器发送的发送成功提示。

[0020] 第二方面，本发明实施例提供一种数据加密处理方法，应用于内网服务器，所述方法包括：

[0021] 接收终端设备发送的加密后的目标应用程序对应的业务数据，其中，所述加密后的目标应用程序对应的业务数据为根据预存的加密规则对所述目标应用程序对应的业务数据进行加密得到的；

[0022] 通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

[0023] 可选的，所述通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端，包括：

[0024] 通过预存的加密规则对应的专用加密通道对所述加密后的目标应用程序对应的业务数据发送至接收端。

[0025] 第三方面，本发明实施例提供一种数据加密处理装置，应用于终端设备，所述装置包括：

[0026] 获取模块，用于获取至少一应用程序对应的业务数据，其中，所述应用程序对应的业务数据中包含应用程序标识；

[0027] 处理模块，用于基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件；

[0028] 所述处理模块，还用于若确定目标应用程序对应的业务数据需加密传输，则根据预存的加密规则对所述目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至内网服务器，以使内网服务器通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

[0029] 第四方面，本发明实施例提供一种数据加密处理装置，应用于内网服务器，所述装置包括：

[0030] 接收模块，用于接收终端设备发送的加密后的目标应用程序对应的业务数据，其中，所述加密后的目标应用程序对应的业务数据为根据预存的加密规则对所述目标应用程序对应的业务数据进行加密得到的；

[0031] 处理模块，用于通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

[0032] 第五方面，本发明实施例提供一种电子设备，包括：至少一个处理器和存储器；

[0033] 所述存储器存储计算机执行指令；

[0034] 所述至少一个处理器执行所述存储器存储的计算机执行指令，使得所述至少一个处理器执行如第一方面和第二方面以及各种可能的设计所述的数据加密处理方法。

[0035] 第六方面，本发明实施例提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当处理器执行所述计算机执行指令时，实现如第一方面和第二方面以及各种可能的设计所述的数据加密处理方法。

[0036] 第七方面，本发明实施例提供一种计算机程序产品，包括计算机程序，所述计算机程序被处理器执行时，实现如第一方面和第二方面以及各种可能的设计所述的数据加密处理方法。

[0037] 本发明实施例提供了一种数据加密处理方法、装置及电子设备，采用上述方案后，可以先获取至少一应用程序对应的业务数据，其中，应用程序对应的业务数据中包含应用程序标识，然后基于应用程序标识检测各应用程序对应的业务数据是否满足加密条件，若满足，则可以根据预存的加密规则对目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至接收端，通过先对应用程序对应的业务数据进行检测，并在检测出满足加密条件后，再对应用程序对应的业务数据通过预存的加密规则进行加密处理和加密传输，提高了业务数据的安全性，进而保证了各业务的正常实现。

附图说明

[0038] 为了更清楚地说明本发明实施例或现有技术中的技术方案，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。

[0039] 图1为本发明实施例提供的数据加密处理方法的应用系统的架构示意图；

[0040] 图2为本发明实施例提供的数据加密处理方法的流程示意图；

[0041] 图3为本发明实施例提供的发送成功提示的应用示意图；

[0042] 图4为本发明另一实施例提供的数据加密处理方法的流程示意图；

[0043] 图5为本发明实施例提供的数据加密处理系统的应用示意图；

[0044] 图6为本发明实施例提供的数据加密处理装置的结构示意图；

[0045] 图7为本发明另一实施例提供的数据加密处理装置的结构示意图；

[0046] 图8为本发明实施例提供的电子设备的硬件结构示意图。

具体实施方式

[0047] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0048] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等(如果存在)是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例还能够包括除

了图示或描述的那些实例以外的其他顺序实例。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0049] 现有技术中，在终端设备中可以安装有不同的应用程序，每个应用程序可以实现多种不同的业务，例如，可以安装有视频类应用程序、购物类应用程序、出行类应用程序等，出行类应用程序可以涉及到打车业务、导航业务、充值业务等不同的业务。在实现业务的过程中，又可能涉及到文本、图像、声音、视频等业务数据的处理与传输。对应的，上述业务数据大多是基于通用的移动端框架生成的，业务数据生成之后，可以通过通用的标准网络协议将业务数据发送至接收端，接收端获取到业务数据之后，可以进一步对业务数据进行处理，进而实现相关的业务功能。然而，由于终端设备丢失、黑客入侵等因素，导致基于通用的移动端框架生成的业务数据存在被他人截获、篡改数据等风险，降低了业务数据的安全性，进而影响了各业务的正常实现。

[0050] 基于上述问题，本申请通过先对应用程序对应的业务数据进行检测，并在检测出满足加密条件后，再对应用程序对应的业务数据通过预存的加密规则进行加密处理和加密传输的方式，达到了既提高了业务数据的安全性，又保证了各业务的正常实现的技术效果。

[0051] 图1为本发明实施例提供的数据加密处理方法的应用系统的架构示意图，如图1所示，所述系统可以包括：终端设备101、内网服务器102和接收端103，其中，接收端103可以为智能手机、平板或其他可以实现特定功能的专网终端。终端设备101中安装有若干应用程序，在任一应用程序需要实现相关业务功能时，终端设备101可以获取该应用程序对应的业务数据，然后对其进行检测，并在检测出满足加密条件时，对该应用程序对应的业务数据进行加密处理，然后发送至内网服务器102，内网服务器102再根据预存的加密通道将加密后的应用程序对应的业务数据发送至接收端，以使接收端根据该加密后的应用程序对应的业务数据实现相关的业务功能。

[0052] 下面以具体地实施例对本发明的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0053] 图2为本发明实施例提供的数据加密处理方法的流程示意图，本实施例的方法可以由终端设备101执行。如图2所示，本实施例的方法，可以包括：

[0054] S201：获取至少一应用程序对应的业务数据，其中，应用程序对应的业务数据中包含应用程序标识。

[0055] 在本实施例中，应用程序可以有多个，每个应用程序还可以对应若干业务数据，用来实现相关的业务功能。

[0056] 进一步的，还可以通过应用程序标识来表示应用程序。对应的，应用程序标识可以为大写字母、小写字母以及数字中的任意一种或多种的组合，示例性的，应用程序标识可以为A1、A2、B1、B2等。

[0057] S202：基于应用程序标识检测各应用程序对应的业务数据是否满足加密条件。

[0058] 在本实施例中，有的应用程序本身对应的业务数据的保密等级高，因此，需要对该应用程序对应的业务数据进行加密处理。即在对应用程序对应的业务数据进行处理之前，可以先对应用程序对应的业务数据进行检测，确定其是否满足加密条件，即确定其是否需

要加密处理。

[0059] 在一种可能的实现方式中，基于应用程序标识检测各应用程序对应的业务数据是否满足加密条件，具体可以包括：

[0060] 获取预存的应用程序标识列表。

[0061] 判断所述应用程序标识是否在所述应用程序标识列表中。

[0062] 若存在，则确定所述应用程序对应的业务数据满足加密条件。

[0063] 具体的，可以根据实际应用场景预先设置一应用程序标识列表，该应用程序标识列表中对应的应用程序的业务数据均满足加密条件。若获取到的应用程序标识在该应用程序标识列表中，则确定满足加密条件，若获取到的应用程序标识不在该应用程序标识列表中，则确定不满足加密条件。

[0064] 在另一种可能的实现方式中，基于应用程序标识检测各应用程序对应的业务数据是否满足加密条件，具体可以包括：

[0065] 基于加密检测模型确定包含应用程序标识的各应用程序对应的业务数据是否需加密传输，其中，所述加密检测模型为通过包含应用程序标识的各应用程序对应的业务训练数据训练得到的。

[0066] 具体的，可以预先训练一加密检测模型，然后通过该加密检测模型来对包含应用程序标识的各应用程序对应的业务数据进行识别，确定是否需要加密传输。

[0067] 此外，可以通过包含应用程序标识的各应用程序对应的业务训练数据对神经网络进行训练，得到加密检测模型。

[0068] S203：若确定目标应用程序对应的业务数据满足加密条件，则根据预存的加密规则对目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至内网服务器，以使内网服务器通过预存的加密通道将加密后的目标应用程序对应的业务数据发送至接收端。

[0069] 在本实施例中，在确定出目标应用程序对应的业务数据满足加密条件后，可以根据预存的加密规则对目标应用程序对应的业务数据进行加密，具体实现过程可以包括：

[0070] 若确定目标应用程序对应的业务数据需加密传输，则根据分组密码算法SM1、椭圆曲线公钥密码算法SM2、杂凑算法SM3、对称算法SM4、AES(Advanced Encryption Standard，高级加密标准)、公钥加密算法RSA，以及哈希Hash算法中的任意一种或多种对所述目标应用程序对应的业务数据进行加密。

[0071] 采用上述方案后，可以先获取至少一应用程序对应的业务数据，其中，应用程序对应的业务数据中包含应用程序标识，然后基于应用程序标识检测各应用程序对应的业务数据是否满足加密条件，若满足，则可以根据预存的加密规则对目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至接收端，通过先对应用程序对应的业务数据进行检测，并在检测出满足加密条件后，再对应用程序对应的业务数据通过预存的加密规则进行加密处理和加密传输，提高了业务数据的安全性，进而保证了各业务的正常实现。

[0072] 基于图2的方法，本说明书实施例还提供了该方法的一些具体实施方案，下面进行说明。

[0073] 在另一实施例中，在并将加密后的目标应用程序对应的业务数据发送至内网服务

器，以使内网服务器通过预存的加密通道将加密后的目标应用程序对应的业务数据发送至接收端之后，还包括：

[0074] 接收并显示内网服务器发送的发送成功提示。

[0075] 在本实施例中，在内网服务器将加密后的目标应用程序对应的业务数据成功发送至接收端之后，为了提高用户体验，内网服务器可以向终端设备发送一发送成功提示。

[0076] 示例性的，图3为本发明实施例提供的发送成功提示的应用示意图，如图3所示，在该实施例中，可以通过文字信息“加密后的业务数据已成功发送至接收端”来提醒用户业务数据已成功发送至接收端。

[0077] 图4为本发明另一实施例提供的数据加密处理方法的流程示意图，本实施例的方法可以由内网服务器102执行。如图4所示，本实施例的方法，可以包括：

[0078] S401：接收终端设备发送的加密后的目标应用程序对应的业务数据，其中，加密后的目标应用程序对应的业务数据为根据预存的加密规则对目标应用程序对应的业务数据进行加密得到的。

[0079] S402：通过预存的加密通道将加密后的目标应用程序对应的业务数据发送至接收端。

[0080] 进一步的，通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端，具体可以包括：

[0081] 通过预存的加密规则对应的专用加密通道对所述加密后的目标应用程序对应的业务数据发送至接收端。

[0082] 在本实施例中，在终端设备中安装有安全接入应用，可以使用专用密码作为信源加密，安全接入应用会接管满足加密条件的应用程序对应的所有业务数据，然后可以通过安全接入系统建立的专用加密通道，并将指定业务应用的数据导向内网，达到直接访问内网服务的目的。其中，内网业务服务器是用户在内网的业务服务器集群，例如FTP服务器、ERP系统以及其他业务服务器等。将企业内网业务先进行专用密码加密，完成后通过专用密码加密通道发送到接收端，实现业务端到端加密。数据传输过程中可以采用128位专用密码SSL(Secure Socket Layer，安全套接字层)加密后的加密通道。

[0083] 该实施例的核心从终端设备信源维持专用密码的技术安全性考虑，本地存储采用专用密码进行数据隔离保护，保证信源在基于源有移动端架构上进行专用密码加密保护，对本地存储数据文本、图像、声音、视频进行专用密码隔离保护，业务传输中采用高强度的专用加密通道，保障了数据的加密隔离安全，提高了业务数据的安全性，进而保证了业务的正常实现。

[0084] 图5为本发明实施例提供的数据加密处理系统的应用示意图，如图5所示，所述系统分为三个部分：终端设备、安全接入设备和内网服务器。

[0085] 在终端设备侧，安装有安全接入客户端，使用专用密码作为信源加密，安全接入客户端会接管指定应用的所有网络数据，通过安全接入系统建立的加密通道，将指定应用的数据导向企业内网，达到访问内网服务的目的。安全接入设备可以用于将网关和认证服务器，从专用链路连接管理，为用户搭建加密通道，然后还可以负责管理用户证书，以及完成秘钥和用户身份认证。内网业务是用户在内网的业务服务器集群，例如FTP服务器、ERP系统以及其他业务服务器等。将企业内网业务先进行信源加密，完成后通过加密通道发送到接

收端,实现业务端到端加密。

[0086] 基于同样的思路,本说明书实施例还提供了上述方法对应的装置,图6为本发明实施例提供的数据加密处理装置的结构示意图,如图6所示,应用于终端设备,可以包括:

[0087] 获取模块601,用于获取至少一应用程序对应的业务数据,其中,所述应用程序对应的业务数据中包含应用程序标识。

[0088] 处理模块602,用于基于所述应用程序标识检测各应用程序对应的业务数据是否满足加密条件。

[0089] 在本实施例中,在一种实现方式中,所述处理模块602,还用于:

[0090] 获取预存的应用程序标识列表。

[0091] 判断所述应用程序标识是否在所述应用程序标识列表中。

[0092] 若存在,则确定所述应用程序对应的业务数据满足加密条件。

[0093] 在另一种实现方式中,所述处理模块602,还用于:

[0094] 基于加密检测模型确定包含应用程序标识的各应用程序对应的业务数据是否需加密传输,其中,所述加密检测模型为通过包含应用程序标识的各应用程序对应的业务训练数据训练得到的。

[0095] 所述处理模块602,还用于若确定目标应用程序对应的业务数据需加密传输,则根据预存的加密规则对所述目标应用程序对应的业务数据进行加密,并将加密后的目标应用程序对应的业务数据发送至内网服务器,以使内网服务器通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

[0096] 在本实施例中,所述处理模块602还用于:

[0097] 若确定目标应用程序对应的业务数据需加密传输,则根据分组密码算法SM1、椭圆曲线公钥密码算法SM2、杂凑算法SM3、对称算法SM4、高级加密标准AES、公钥加密算法RSA,以及哈希Hash算法中的任意一种或多种对所述目标应用程序对应的业务数据进行加密。

[0098] 此外,在另一实施例中,所述处理模块,还用于:

[0099] 接收并显示所述内网服务器发送的发送成功提示。

[0100] 图7为本发明另一实施例提供的数据加密处理装置的结构示意图,如图7所示,应用于内网服务器,所述装置包括:

[0101] 接收模块701,用于接收终端设备发送的加密后的目标应用程序对应的业务数据,其中,所述加密后的目标应用程序对应的业务数据为根据预存的加密规则对所述目标应用程序对应的业务数据进行加密得到的。

[0102] 处理模块702,用于通过预存的加密通道将所述加密后的目标应用程序对应的业务数据发送至接收端。

[0103] 在本实施例中,所述处理模块702,还用于:

[0104] 通过预存的加密规则对应的专用加密通道对所述加密后的目标应用程序对应的业务数据发送至接收端。

[0105] 本发明实施例提供的装置,可以实现上述如图2所示的实施例的方法,其实现原理和技术效果类似,此处不再赘述。

[0106] 图8为本发明实施例提供的电子设备的硬件结构示意图,如图8所示,本实施例提供的设备800包括:至少一个处理器801和存储器802。其中,处理器801、存储器802通过总线

803连接。

[0107] 在具体实现过程中,至少一个处理器801执行所述存储器802存储的计算机执行指令,使得至少一个处理器801执行上述方法实施例中的方法。

[0108] 处理器801的具体实现过程可参见上述方法实施例,其实现原理和技术效果类似,本实施例此处不再赘述。

[0109] 在上述的图8所示的实施例中,应理解,处理器可以是中央处理单元(英文:Central Processing Unit,简称:CPU),还可以是其他通用处理器、数字信号处理器(英文:Digital Signal Processor,简称:DSP)、专用集成电路(英文:Application Specific Integrated Circuit,简称:ASIC)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。结合发明所公开的方法的步骤可以直接体现为硬件处理器执行完成,或者用处理器中的硬件及软件模块组合执行完成。

[0110] 存储器可能包含高速RAM存储器,也可能还包括非易失性存储NVM,例如至少一个磁盘存储器。

[0111] 总线可以是工业标准体系结构(Industry Standard Architecture,ISA)总线、外部设备互连(Peripheral Component Interconnect,PCI)总线或扩展工业标准体系结构(Extended Industry Standard Architecture,EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示,本申请附图中的总线并不限定仅有一根总线或一种类型的总线。

[0112] 本发明实施例还提供一种计算机可读存储介质,所述计算机可读存储介质中存储有计算机执行指令,当处理器执行所述计算机执行指令时,实现上述方法实施例的数据加密处理方法。

[0113] 本发明实施例还提供一种计算机程序产品,包括计算机程序,所述计算机程序被处理器执行时,实现如上所述的数据加密处理方法。

[0114] 上述的计算机可读存储介质,上述可读存储介质可以是由任何类型的易失性或非易失性存储设备或者它们的组合实现,如静态随机存取存储器(SRAM),电可擦除可编程只读存储器(EEPROM),可擦除可编程只读存储器(EPROM),可编程只读存储器(PROM),只读存储器(ROM),磁存储器,快闪存储器,磁盘或光盘。可读存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0115] 一种示例性的可读存储介质耦合至处理器,从而使处理器能够从该可读存储介质读取信息,且可向该可读存储介质写入信息。当然,可读存储介质也可以是处理器的组成部分。处理器和可读存储介质可以位于专用集成电路(Application Specific Integrated Circuits,简称:ASIC)中。当然,处理器和可读存储介质也可以作为分立组件存在于设备中。

[0116] 本领域普通技术人员可以理解:实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时,执行包括上述各方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0117] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述各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，或者对其中部分或者全部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范围。

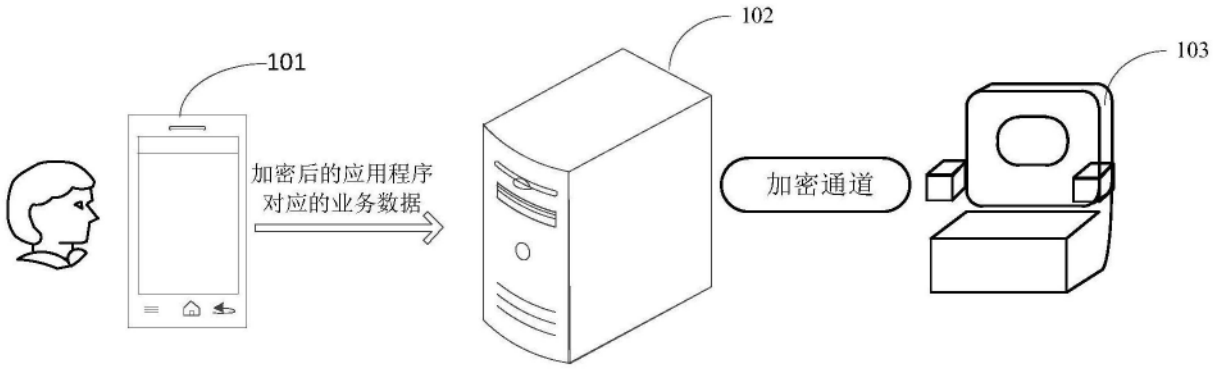

101
102
103
加密后的应用程序
对应的业务数据
加密通道

图1

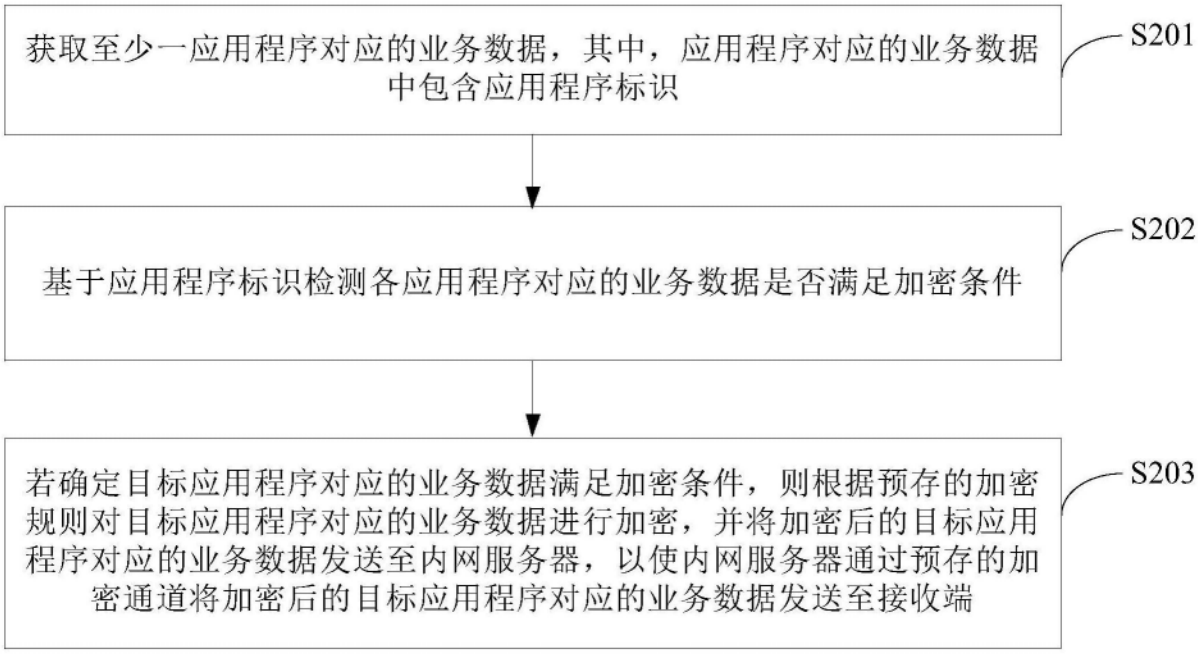

获取至少一应用程序对应的业务数据，其中，应用程序对应的业务数据中包含应用程序标识
S201
基于应用程序标识检测各应用程序对应的业务数据是否满足加密条件
S202
若确定目标应用程序对应的业务数据满足加密条件，则根据预存的加密规则对目标应用程序对应的业务数据进行加密，并将加密后的目标应用程序对应的业务数据发送至内网服务器，以使内网服务器通过预存的加密通道将加密后的目标应用程序对应的业务数据发送至接收端
S203

图2

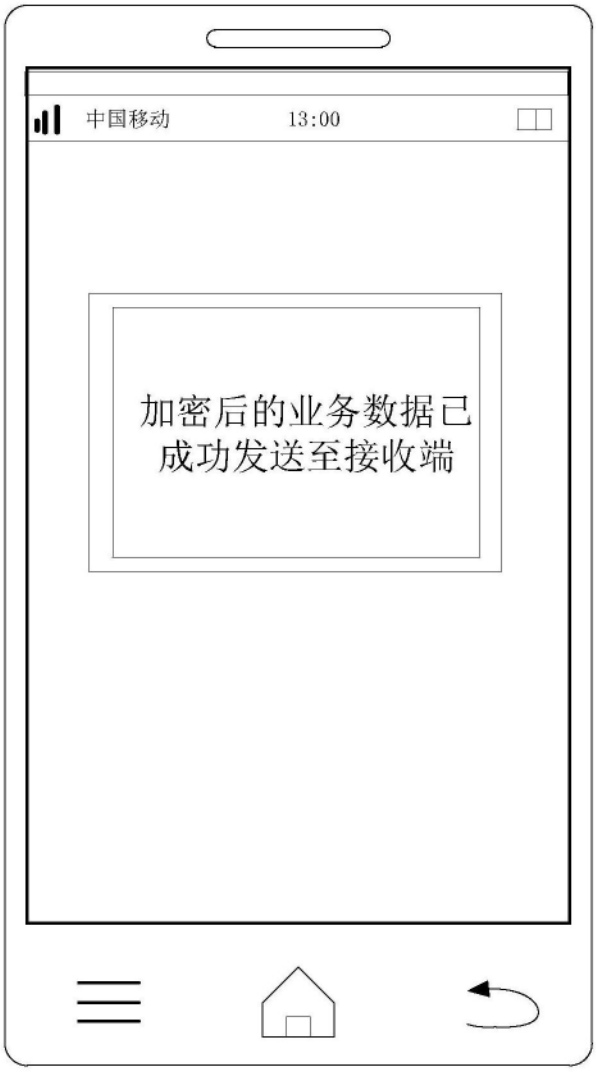

中国移动
13:00
加密后的业务数据已成功发送至接收端

图3

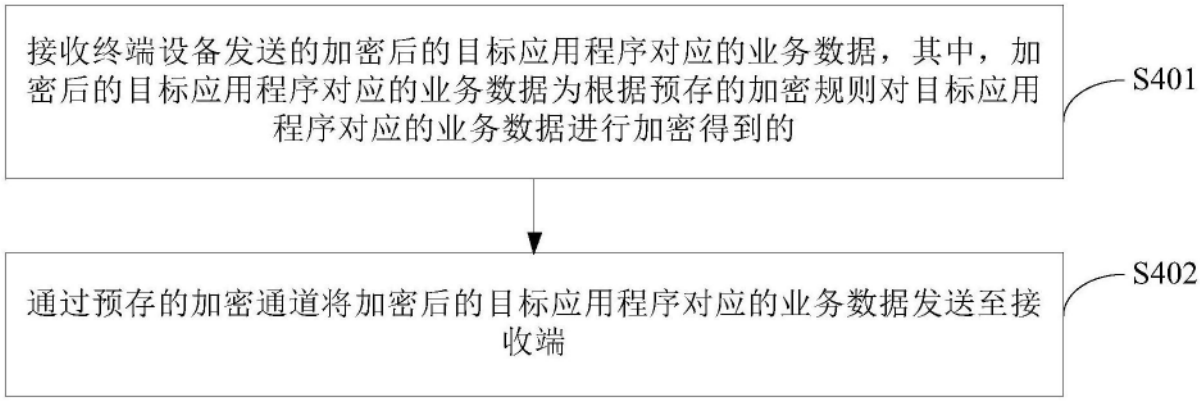

接收终端设备发送的加密后的目标应用程序对应的业务数据，其中，加密后的目标应用程序对应的业务数据为根据预存的加密规则对目标应用程序对应的业务数据进行加密得到的
S401
通过预存的加密通道将加密后的目标应用程序对应的业务数据发送至接收端
S402

图4

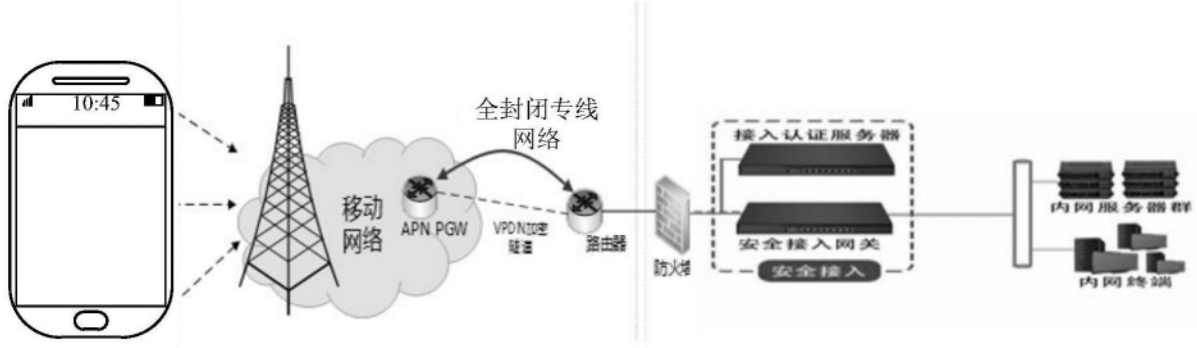

10:45
移动网络
APN PGW
VPDN加密隧道
全封闭专线网络
路由器
防火墙
接入认证服务器
安全接入网关
安全接入
内网服务器群
内网终端

图5

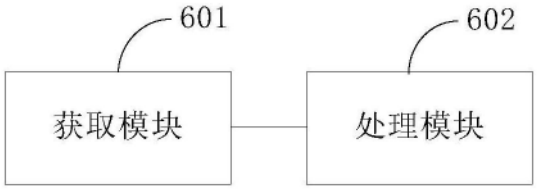

601
602
获取模块
处理模块

图6

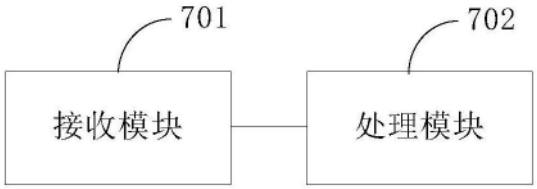

701
702
接收模块
处理模块

图7

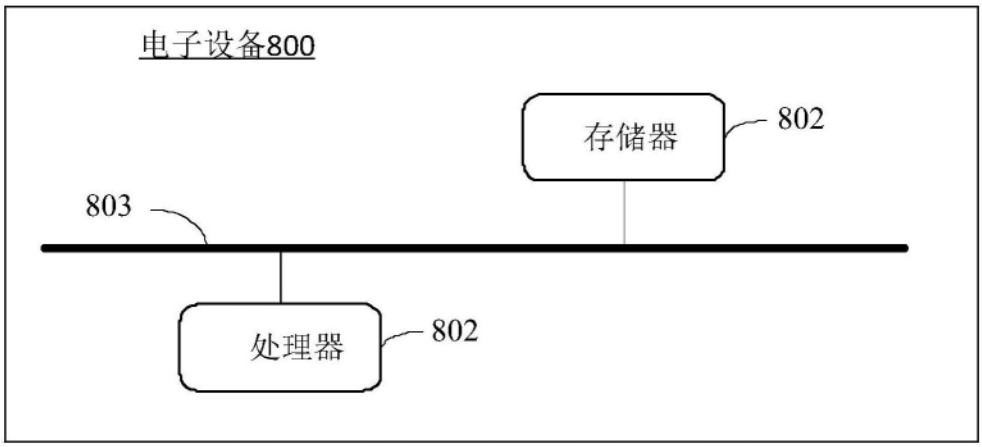

电子设备800
存储器
802
803
处理器
802

图8