(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 103873245 B
(45)授权公告日 2017.12.22

(21)申请号 201210544060.0

(22)申请日 2012.12.14

(65)同一申请的已公布的文献号
申请公布号 CN 103873245 A

(43)申请公布日 2014.06.18

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 刘新保

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 张莲莲

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 9/455(2006.01)

(56)对比文件
郑兴艳.《安全虚拟桌面系统的设计与实现》.《中国优秀硕士学位论文全文数据库(电子期刊)》.2012,139－269.

审查员 胡锐先

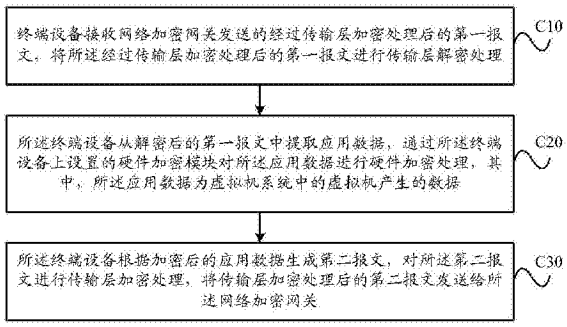
权利要求书5页 说明书12页 附图6页

(54)发明名称

虚拟机系统数据加密方法及设备

(57)摘要

本发明实施例提供一种虚拟机系统数据加密方法及设备，虚拟机系统数据加密方法包括：终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将经过传输层加密处理后的第一报文进行传输层解密处理；终端设备从解密后的第一报文中提取应用数据，通过终端设备上设置的硬件加密模块对应用数据进行硬件加密处理，其中，应用数据为虚拟机系统中的虚拟机产生的数据；终端设备根据加密后的应用数据生成第二报文，对第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给网络加密网关。本发明实施例提供的虚拟机系统数据加密方法及设备，实现了对物理服务器上的多个虚拟机的应用数据的加密支持。



CN 103873245 B

1.一种虚拟机系统数据加密方法，其特征在于，包括：

终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理；所述第一报文为虚拟系统中的虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成后发送给所述网络加密网关的，所述第一报文用于指示所述终端设备对所述虚拟机中的应用程序发送的应用数据进行硬件加密；

所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；

所述终端设备根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关，以使所述网络加密网关将所述第二报文进行传输层解密处理后发送给所述虚拟机；

所述终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，具体为：

所述终端设备通过所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立的经由所述网络加密网关的虚拟通道，接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文；

所述终端设备将传输层加密处理后的第二报文发送给所述网络加密网关，具体为：

所述终端设备将所述传输层加密处理后的第二报文通过所述虚拟通道发送给所述网络加密网关。

2.根据权利要求1所述的虚拟机系统数据加密方法，其特征在于：所述第一报文中包括用以标识密钥的密钥标识；

所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，具体为：

所述终端设备从所述解密后的第一报文中提取所述应用数据和所述密钥标识，将所述应用数据和所述密钥标识发送给所述硬件加密模块，所述硬件加密模块根据所述密钥标识确定密钥，通过所述密钥对所述应用数据进行加密，将加密后的应用数据返回给所述终端设备。

3.根据权利要求1所述的虚拟机系统数据加密方法，其特征在于，所述终端设备通过所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立的经由所述网络加密网关的虚拟通道，接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文之前，所述方法还包括：

所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立所述虚拟通道。

4.根据权利要求1所述的虚拟机系统数据加密方法，其特征在于，所述方法还包括：

所述终端设备接收所述网络加密网关发送的经过传输层加密处理后的第三报文，将所述经过传输层加密处理后的第三报文进行传输层解密处理；

所述终端设备从解密后的第一报文中提取已加密的应用数据，通过所述终端设备上设置的硬件加密模块对所述已加密的应用数据进行硬件解密处理，其中，所述已加密的应用数据为虚拟机系统中的虚拟机产生的、经过所述终端设备的硬件加密模块硬件加密处理过

的数据；

所述终端设备根据解密后的应用数据生成第四报文，对所述第四报文进行传输层加密处理，将传输层加密处理后的第四报文发送给所述网络加密网关。

5.一种虚拟机系统数据加密方法，其特征在于，包括：

虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，通过网络加密网关将所述第一报文进行传输层加密后发送给终端设备；所述第一报文用于指示所述终端设备对所述虚拟机中的应用程序发送的应用数据进行硬件加密；

所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述第二报文为所述终端设备发送给所述网络加密网关的，所述加密后的应用数据为所述终端设备对所述应用数据进行硬件加密处理得到的；

所述虚拟机将所述第一报文发送给网络加密网关，具体为：

所述虚拟机通过所述虚拟机的虚拟桌面代理模块与所述终端设备的虚拟桌面代理客户端模块建立的经由所述网络加密网关的虚拟通道，将所述第一报文发送给所述网络加密网关；

所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，具体为：

所述虚拟机通过所述虚拟通道接收所述网络加密网关发送的经过传输层解密处理后的第二报文。

6.根据权利要求5所述的虚拟机系统数据加密方法，其特征在于，所述虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，具体为：

所述虚拟机根据接收到的所述应用程序发送的应用数据和密钥标识生成所述第一报文，其中，所述密钥标识用以标识密钥。

7.根据权利要求5所述的虚拟机系统数据加密方法，其特征在于，所述虚拟机将所述第一报文发送给网络加密网关之前，所述方法还包括：

所述虚拟机的虚拟桌面代理模块与所述终端设备的虚拟桌面代理客户端模块建立所述虚拟通道。

8.根据权利要求5所述的虚拟机系统数据加密方法，其特征在于，所述方法还包括：

所述虚拟机根据接收到的所述虚拟机中的应用程序发送的已加密的应用数据生成第三报文，将所述第三报文发送给网络加密网关；

所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第四报文，提取所述经过传输层解密处理后的第四报文中的解密后的应用数据，将所述解密后的应用数据发送给所述应用程序，其中，所述解密后的应用数据为终端设备对所述已加密的应用数据进行硬件解密处理得到的。

9.一种终端设备，其特征在于，包括：

传输层解密模块，用于接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理；所述第一报文为虚拟系统中的虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成后发送给所述网络加密网关的，所述第一报文用于指示所述终端设备对所述虚拟机中的应用程序发送的应

用数据进行硬件加密；

加密服务模块，与所述传输层解密模块连接，用于从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；

传输层加密模块，与所述加密服务模块连接，用于根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关，以使所述网络加密网关将所述第二报文进行传输层解密处理后发送给所述虚拟机；

还包括：

虚拟桌面代理客户端模块，用于与所述虚拟机的虚拟桌面代理模块建立经由所述网络加密网关的虚拟通道；

所述传输层解密模块具体用于通过所述虚拟通道接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文；

所述传输层加密模块具体用于将所述传输层加密处理后的第二报文通过所述虚拟通道发送给所述网络加密网关。

10.根据权利要求9所述的终端设备，其特征在于：所述第一报文中包括用以标识密钥的密钥标识；

所述加密服务模块具体用于从所述解密后的第一报文中提取所述应用数据和所述密钥标识，将所述应用数据和所述密钥标识发送给所述硬件加密模块，所述硬件加密模块根据所述密钥标识确定密钥，通过所述密钥对所述应用数据进行加密，将加密后的应用数据返回给所述终端设备。

11.根据权利要求9所述的终端设备，其特征在于：

所述传输层解密模块还用于接收所述网络加密网关发送的经过传输层加密处理后的第三报文，将所述经过传输层加密处理后的第三报文进行传输层解密处理；

所述加密服务模块还从解密后的第一报文中提取已加密的应用数据，通过所述终端设备上设置的硬件加密模块对所述已加密的应用数据进行硬件解密处理，其中，所述已加密的应用数据为虚拟机系统中的虚拟机产生的、经过所述终端设备的硬件加密模块硬件加密处理过的数据；

所述传输层加密模块还用于根据解密后的应用数据生成第四报文，对所述第四报文进行传输层加密处理，将传输层加密处理后的第四报文发送给所述网络加密网关。

12.一种虚拟机，其特征在于，包括：

发送处理模块，用于根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，通过网络加密网关将所述第一报文进行传输层加密后发送给终端设备；所述第一报文用于指示所述终端设备对所述虚拟机中的应用程序发送的应用数据进行硬件加密；

接收处理模块，用于接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述第二报文为所述终端设备发送给所述网络加密网关的，所述加密后的应用数据为所述终端设备对所述应用数据进行硬件加密处理得到的；

还包括：

虚拟桌面代理模块，用于与所述终端设备的虚拟桌面代理客户端模块建立经由所述网络加密网关的虚拟通道；

所述发送处理模块具体用于通过所述虚拟通道将所述第一报文发送给所述网络加密网关；

所述接收处理模块具体用于通过所述虚拟通道接收所述网络加密网关发送的经过传输层解密处理后的第二报文。

13.根据权利要求12所述的虚拟机，其特征在于：所述发送处理模块具体用于根据接收到的所述应用程序发送的应用数据和密钥标识生成所述第一报文，其中，所述密钥标识用以标识密钥。

14.根据权利要求12所述的虚拟机，其特征在于：

所述发送处理模块还用于根据接收到的所述虚拟机中的应用程序发送的已加密的应用数据生成第三报文，将所述第三报文发送给网络加密网关；

所述接收处理模块还用于接收所述网络加密网关发送的经过传输层解密处理后的第四报文，提取所述经过传输层解密处理后的第四报文中的解密后的应用数据，将所述解密后的应用数据发送给所述应用程序，其中，所述解密后的应用数据为终端设备对所述已加密的应用数据进行硬件解密处理得到的。

15.一种终端设备，其特征在于，包括：处理器，通信接口，存储器和总线：

其中所述处理器、所述通信接口和所述存储器通过所述总线完成相互间的通信；

所述通信接口，用于接收网络加密网关发送的经过传输层加密处理后的第一报文，以及将传输层加密处理后的第二报文发送给所述网络加密网关，以使所述网络加密网关将所述第二报文进行传输层解密处理后发送给虚拟机；所述第一报文为虚拟系统中的虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成后发送给所述网络加密网关的，所述第一报文用于指示所述终端设备对所述虚拟机中的应用程序发送的应用数据进行硬件加密；

所述存储器，用于存储指令；

所述处理器被配置为执行存储在所述存储器中的指令，其中，所述处理器被配置为用于将所述经过传输层加密处理后的第一报文进行传输层解密处理，从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理；

所述通信接口，具体用于通过所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立的经由所述网络加密网关的虚拟通道，接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文；以及将所述传输层加密处理后的第二报文通过所述虚拟通道发送给所述网络加密网关。

16.一种用于虚拟机的计算机节点，其特征在于，包括：处理器，通信接口，存储器和总线：

其中所述处理器、所述通信接口和所述存储器通过所述总线完成相互间的通信；

所述通信接口，用于通过网络加密网关将第一报文进行传输层加密后发送给终端设

备，以及接收所述网络加密网关发送的经过传输层解密处理后的第二报文；所述第一报文用于指示所述终端设备对所述虚拟机中的应用程序发送的应用数据进行硬件加密，所述第二报文为所述终端设备发送给所述网络加密网关的；

所述存储器，用于存储指令；

所述处理器被配置为执行存储在所述存储器中的指令，其中，所述处理器被配置为用于根据接收到的所述虚拟机中的应用程序发送的应用数据生成所述第一报文；提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为所述终端设备对所述应用数据进行硬件加密处理得到的；

所述通信接口，具体用于通过所述虚拟机的虚拟桌面代理模块与所述终端设备的虚拟桌面代理客户端模块建立的经由所述网络加密网关的虚拟通道，将所述第一报文发送给所述网络加密网关；以及，通过所述虚拟通道接收所述网络加密网关发送的经过传输层解密处理后的第二报文。

虚拟机系统数据加密方法及设备

技术领域

[0001] 本发明实施例涉及通信技术，尤其涉及一种虚拟机系统数据加密方法及设备。

背景技术

[0002] 随着计算机技术的发展，虚拟化技术得到大面积的推广和应用。桌面虚拟化是在实现数据中心的物理服务器上安装虚拟机系统，由虚拟机系统模拟出操作系统运行所需要的硬件资源。操作系统运行在这些虚拟的硬件资源之上，可以达到多个操作系统共享物理服务器的硬件资源，从而提高资源利用率。

[0003] 加密是保证数据的安全性的一种重要的手段，加密卡是为PC(PersonalComputer，个人计算机)提供加密服务的专用插卡式密码设备。在PC上插设加密卡，加密卡可以对PC上的数据或者从该PC流出的数据进行加密，以保证数据的安全性。通过加密卡进行数据加密，由于目密钥并不存放在内存中，因此更加安全。但是，对于安装有虚拟机系统的物理服务器，在物理服务器上插设加密卡时，由于现有技术中并没有加密卡的虚拟化技术，会导致在同一时刻，物理服务器上只有一台虚拟机独占加密卡进行加密业务，亟需提出一种解决方案。

发明内容

[0004] 本发明实施例提供一种虚拟机系统数据加密方法及设备，以实现对物理服务器上的多个虚拟机的应用数据的加密支持。

[0005] 第一方面，本发明实施例提供一种虚拟机系统数据加密方法，包括：

[0006] 终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理；

[0007] 所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；

[0008] 所述终端设备根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关。

[0009] 在第一种可能的实现方式中，所述第一报文中包括用以标识密钥的密钥标识；

[0010] 所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，具体为：

[0011] 所述终端设备从所述解密后的第一报文中提取所述应用数据和所述密钥标识，将所述应用数据和所述密钥标识发送给所述硬件加密模块，所述硬件加密模块根据所述密钥标识确定密钥，通过所述密钥对所述应用数据进行加密，将加密后的应用数据返回给所述终端设备。

[0012] 结合第一方面或第一方面的第一种可能的实现方式，在第二种可能的实现方式中，所述终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，具体为：

[0013] 所述终端设备通过所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立的经由所述网络加密网关的虚拟通道，接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文；

[0014] 所述终端设备将传输层加密处理后的第二报文发送给所述网络加密网关，具体为：

[0015] 所述终端设备将所述传输层加密处理后的第二报文通过所述虚拟通道发送给所述网络加密网关。

[0016] 结合第一方面的第二种可能的实现方式，在第三种可能的实现方式中，所述终端设备通过所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立的经由所述网络加密网关的虚拟通道，接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文之前，所述方法还包括：

[0017] 所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立所述虚拟通道。

[0018] 在第四种可能的实现方式中，所述方法还包括：

[0019] 所述终端设备接收所述网络加密网关发送的经过传输层加密处理后的第三报文，将所述经过传输层加密处理后的第三报文进行传输层解密处理；

[0020] 所述终端设备从解密后的第一报文中提取已加密的应用数据，通过所述终端设备上设置的硬件加密模块对所述已加密的应用数据进行硬件解密处理，其中，所述已加密的应用数据为虚拟机系统中的虚拟机产生的、经过所述终端设备的硬件加密模块硬件加密处理过的数据；

[0021] 所述终端设备根据解密后的应用数据生成第四报文，对所述第四报文进行传输层加密处理，将传输层加密处理后的第四报文发送给所述网络加密网关。

[0022] 第二方面，本发明实施例一种虚拟机系统数据加密方法，包括：

[0023] 虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，将所述第一报文发送给网络加密网关；

[0024] 所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的。

[0025] 在第一种可能的实现方式中，所述虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，具体为：

[0026] 所述虚拟机根据接收到的所述应用程序发送的应用数据和密钥标识生成所述第一报文，其中，所述密钥标识用以标识密钥。

[0027] 结合第二方面或第二方面的第一种可能的实现方式，在第二种可能的实现方式中，所述虚拟机将所述第一报文发送给网络加密网关，具体为：

[0028] 所述虚拟机通过所述虚拟机的虚拟桌面代理模块与所述终端设备的虚拟桌面代理客户端模块建立的经由所述网络加密网关的虚拟通道，将所述第一报文发送给所述网络加密网关；

[0029] 所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，具

体为：

[0030] 所述虚拟机通过所述虚拟通道接收所述网络加密网关发送的经过传输层解密处理后的第二报文。

[0031] 结合第二方面的第二种可能的实现方式，在第三种可能的实现方式中，所述虚拟机将所述第一报文发送给网络加密网关之前，所述方法还包括：

[0032] 所述虚拟机的虚拟桌面代理模块与所述终端设备的虚拟桌面代理客户端模块建立所述虚拟通道。

[0033] 在第四种可能的实现方式中，所述方法，还包括：

[0034] 所述虚拟机根据接收到的所述虚拟机中的应用程序发送的已加密的应用数据生成第三报文，将所述第三报文发送给网络加密网关；

[0035] 所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第四报文，提取所述经过传输层解密处理后的第四报文中的解密后的应用数据，将所述解密后的应用数据发送给所述应用程序，其中，所述解密后的应用数据为终端设备对所述已加密的应用处理进行硬件解密处理得到的。

[0036] 第三方面，本发明实施例提供一种终端设备，包括：

[0037] 传输层解密模块，用于接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理；

[0038] 加密服务模块，与所述传输层解密模块连接，用于从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；

[0039] 传输层加密模块，与所述加密服务模块连接，用于根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关。

[0040] 在第一种可能的实现方式中，所述第一报文中包括用以标识密钥的密钥标识；

[0041] 所述加密服务模块具体用于从所述解密后的第一报文中提取所述应用数据和所述密钥标识，将所述应用数据和所述密钥标识发送给所述硬件加密模块，所述硬件加密模块根据所述密钥标识确定密钥，通过所述密钥对所述应用数据进行加密，将加密后的应用数据返回给所述终端设备。

[0042] 结合第三方面或第三方面的第一种可能的实现方式，在第二种可能的实现方式中，所述终端设备还包括：

[0043] 虚拟桌面代理客户端模块，用于与所述虚拟机的虚拟桌面代理模块建立经由所述网络加密网关的虚拟通道；

[0044] 所述传输层解密模块具体用于通过所述虚拟通道接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文；

[0045] 所述传输层加密模块具体用于将所述传输层加密处理后的第二报文通过所述虚拟通道发送给所述网络加密网关。

[0046] 在第三种可能的实现方式中，所述传输层解密模块还用于接收所述网络加密网关发送的经过传输层加密处理后的第三报文，将所述经过传输层加密处理后的第三报文进行传输层解密处理；

[0047] 所述加密服务模块还从解密后的第一报文中提取已加密的应用数据，通过所述终端设备上设置的硬件加密模块对所述已加密的应用数据进行硬件解密处理，其中，所述已加密的应用数据为虚拟机系统中的虚拟机产生的、经过所述终端设备的硬件加密模块硬件加密处理过的数据；

[0048] 所述传输层加密模块还用于根据解密后的应用数据生成第四报文，对所述第四报文进行传输层加密处理，将传输层加密处理后的第四报文发送给所述网络加密网关。

[0049] 第四方面，本发明实施例提供一种虚拟机，包括：

[0050] 发送处理模块，用于根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，将所述第一报文发送给网络加密网关；

[0051] 接收处理模块，用于接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的。

[0052] 在第一种可能的实现方式中，所述发送处理模块具体用于根据接收到的所述应用程序发送的应用数据和密钥标识生成所述第一报文，其中，所述密钥标识用以标识密钥。

[0053] 结合第四方面或第四方面的第一种可能的实现方式，在第二种可能的实现方式中，所述虚拟机还包括：

[0054] 虚拟桌面代理模块，用于与所述终端设备的虚拟桌面代理客户端模块建立经由所述网络加密网关的虚拟通道；

[0055] 所述发送处理模块具体用于通过所述虚拟通道将所述第一报文发送给所述网络加密网关；

[0056] 所述接收处理模块具体用于通过所述虚拟通道接收所述网络加密网关发送的经过传输层解密处理后的第二报文。

[0057] 在第三种可能的实现方式中，所述发送处理模块还用于根据接收到的所述虚拟机中的应用程序发送的已加密的应用数据生成第三报文，将所述第三报文发送给网络加密网关；

[0058] 所述接收处理模块还用于接收所述网络加密网关发送的经过传输层解密处理后的第四报文，提取所述经过传输层解密处理后的第四报文中的解密后的应用数据，将所述解密后的应用数据发送给所述应用程序，其中，所述解密后的应用数据为终端设备对所述已加密的应用处理进行硬件解密处理得到的。

[0059] 第五方面，本发明实施例提供一种终端设备，包括：处理器，通信接口，存储器和总线：

[0060] 其中所述处理器、所述通信接口和所述存储器通过所述总线完成相互间的通信；

[0061] 所述通信接口，用于接收网络加密网关发送的经过传输层加密处理后的第一报文，以及将传输层加密处理后的第二报文发送给所述网络加密网关；

[0062] 所述存储器，用于存储指令；

[0063] 所述处理器被配置为执行存储在所述存储器中的指令，其中，所述处理器被配置为用于将所述经过传输层加密处理后的第一报文进行传输层解密处理，从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加

密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理。

[0064] 第六方面，本发明实施例提供一种用于虚拟机的计算机节点，包括：处理器，通信接口，存储器和总线：

[0065] 其中所述处理器、所述通信接口和所述存储器通过所述总线完成相互间的通信；

[0066] 所述通信接口，用于将第一报文发送给网络加密网关，以及接收所述网络加密网关发送的经过传输层解密处理后的第二报文；

[0067] 所述存储器，用于存储指令；

[0068] 所述处理器被配置为执行存储在所述存储器中的指令，其中，所述处理器被配置为用于根据接收到的所述虚拟机中的应用程序发送的应用数据生成所述第一报文；提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的。

[0069] 由上述技术方案可知，本发明实施例提供的一种虚拟机系统数据加密方法及设备，终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将经过传输层加密处理后的第一报文进行传输层解密处理，从解密后的第一报文中提取应用数据，通过终端设备上设置的硬件加密模块对应用数据进行硬件加密处理，其中，应用数据为虚拟机系统中的虚拟机产生的数据，根据加密后的应用数据生成第二报文，对第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给网络加密网关。通过设置有硬件加密模块的终端设备对虚拟机产生的应用数据进行加密，无需在物理服务器上插设加密卡，实现了对物理服务器上的多个虚拟机的应用数据的加密支持。而且，该加密过程充分利用了终端设备的处理能力，减轻了虚拟机的负载。

附图说明

[0070] 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一简单地介绍，显而易见地，下面描述中的附图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。

[0071] 图1为本发明实施例提供的第一种虚拟机系统数据加密方法流程图；

[0072] 图2为发明实施例提供的第二种虚拟机系统数据加密方法流程图；

[0073] 图3为本发明实施例提供的第三种虚拟机系统数据加密方法流程图；

[0074] 图4为本发明实施例提供的第四种虚拟机系统数据加密方法流程图；

[0075] 图5为本发明实施例提供的第一种终端设备结构示意图；

[0076] 图6为本发明实施例提供的第二种终端设备结构示意图；

[0077] 图7为本发明实施例提供的第一种虚拟机结构示意图；

[0078] 图8为本发明实施例提供的第二种虚拟机结构示意图；

[0079] 图9为本发明实施例提供的第三种终端设备结构示意图；

[0080] 图10为本发明实施例提供的用于虚拟机的计算机节点结构示意图。

具体实施方式

[0081] 为使本发明实施例的目的、技术方案和优点更加清楚，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作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。

[0082] 图1为本发明实施例提供的第一种虚拟机系统数据加密方法流程图。如图1所示，本实施例提供的虚拟机系统数据加密方法具体可以应用于虚拟机系统中的数据加密处理过程，该虚拟机系统中可以包括至少一个物理服务器，每个物理服务器上设置有至少两个虚拟机，以下以其中一个虚拟机为例，对虚拟机系统数据加密方法进行说明。本实施例提供的虚拟机系统数据加密方法，具体包括：

[0083] 步骤C10、终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理；

[0084] 步骤C20、所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；

[0085] 步骤C30、所述终端设备根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关。

[0086] 具体地，该终端设备可以是该虚拟机系统提供业务服务的对象，例如，该虚拟机系统可以用于但并不限于为用户提供虚拟桌面业务，用户可以使用终端设备通过桌面传输协议访问虚拟机系统中的虚拟机，终端设备将用户鼠标、键盘等操作信息发给虚拟机，虚拟机则将虚拟桌面信息发至终端设备。虚拟机系统还可以为用户提供邮件业务和存储业务等其他业务服务。该终端设备具体可以为智能手机、平板电脑和笔记本电脑等电子设备。

[0087] 网络加密网关具体可以设置在虚拟机系统的出口处，对虚拟机系统中的虚拟机发出的报文进行传输层加密。通常虚拟机上运行有应用程序，以实现相应的业务，应用数据具体为业务过程中应用程序产生的数据，当应用程序需要将应用数据加密时，虚拟机将该应用数据生成第一报文，将该第一报文发送给网络加密网关，网络加密网关对该第一报文进行传输层加密处理，传输层加密也采用硬件加密的方式来实现，以保证传输层加密的可靠性。网络加密网关将经过传输层加密处理后的第一报文发送给终端设备。由于虚拟机发出的报文是明文，通过网络加密网关对第一报文进行传输层加密可以保证应用数据的安全性。

[0088] 终端设备上设置有硬件加密模块，该硬件加密模块具体可以为加密芯片或USB(Universal Serial BUS，通用串行总线)加密设备等，硬件加密模块中存储有密钥和/或数字证书。终端设备接收网络加密网关发送的该经过传输层加密处理后的第一报文，进行传输层解密处理，从解密后的第一报文中提取应用数据，再通过硬件加密模块的驱动接口函数将应用数据发送给硬件加密模块，硬件加密模块将应用数据通过密钥和/或数字证书加密后，将加密后的应用数据返回给终端设备，终端设备将加密后的应用数据生成第二报文，再对该第二报文进行传输层加密。对第二报文进行传输层加密时，也可以通过终端设备的硬件加密模块对第二报文进行硬件加密，移动终端将经过传输层加密后的第二报文发送给

网络加密网关，网络加密网关对接收到的第二报文进行传输层解密后发给虚拟机。虚拟机从第二报文中提取应用数据，该应用数据是经过终端设备硬件加密后的应用数据，对该应用数据进行相应的处理，该处理例如可以为将应用数据转发或将应用数据写入磁盘等操作。

[0089] 当虚拟机系统中的多个虚拟机同时需要对应用数据进行加密时，均可以通过上述方法通过终端设备对应用数据进行加密。每个虚拟机对应的终端设备可以为同一个终端设备，也可以为不同的终端设备。

[0090] 本实施例提供的虚拟机系统数据加密方法，终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将经过传输层加密处理后的第一报文进行传输层解密处理，从解密后的第一报文中提取应用数据，通过终端设备上设置的硬件加密模块对应用数据进行硬件加密处理，其中，应用数据为虚拟机系统中的虚拟机产生的数据，根据加密后的应用数据生成第二报文，对第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给网络加密网关。通过设置有硬件加密模块的终端设备对虚拟机产生的应用数据进行加密，无需在物理服务器上插设加密卡，实现了对物理服务器上的多个虚拟机的应用数据的加密支持。而且，该加密过程充分利用了终端设备的处理能力，减轻了虚拟机的负载。

[0091] 在本实施例中，所述第一报文中包括用以标识密钥的密钥标识；相应地，步骤C20，所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，具体可以为：

[0092] 所述终端设备从所述解密后的第一报文中提取所述应用数据和所述密钥标识，将所述应用数据和所述密钥标识发送给所述硬件加密模块，所述硬件加密模块根据所述密钥标识确定密钥，通过所述密钥对所述应用数据进行加密，将加密后的应用数据返回给所述终端设备。

[0093] 具体地，终端设备的硬件加密模块中存储的密钥数量可以为多个，每个密钥具有唯一密钥标识，则应用程序提供的数据中除了需要加密的应用数据还有密钥标识，虚拟机将应用数据和密钥标识生成第一报文。

[0094] 终端设备将从第一报文中提取到的应用数据和密钥标识发送给硬件加密模块，硬件加密模块根据密钥标识确定相应的密钥，通过该密钥对应用数据进行加密后返回终端设备。

[0095] 在本实施例中，步骤C10，所述终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，具体可以为：

[0096] 所述终端设备通过所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立的经由所述网络加密网关的虚拟通道，接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文；

[0097] 步骤C30，所述终端设备将传输层加密处理后的第二报文发送给所述网络加密网关，具体可以为：

[0098] 所述终端设备将所述传输层加密处理后的第二报文通过所述虚拟通道发送给所述网络加密网关。

[0099] 具体地，该虚拟机系统例如为提供虚拟桌面业务的系统，则虚拟机系统的虚拟机中设置有虚拟桌面代理(Virtual Desktop Agent，简称VDA)模块，相应地，终端设备中设置

有虚拟桌面代理客户端(Virtual Desktop AgentClient)模块。在虚拟桌面业务中，虚拟机的虚拟桌面代理模块会与终端设备的虚拟桌面代理客户端模块建立虚拟通道，该虚拟通道经由网络加密网关。则虚拟机与终端设备的交互可以通过该虚拟通道实现。当桌面云代替传统的桌面办公后，保障了原来的加密业务不丧失，并且不需要改动原来的加密程序。另可复用终端设备上的硬件加密模块，提供终端设备与桌面云数据中心即虚拟机系统的传输层加密能力，节省了在终端设备侧部署网络加密机的成本并使桌面终端的接入地点灵活。

[0100] 在本实施例中，所述终端设备通过所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立的经由所述网络加密网关的虚拟通道，接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文之前，所述方法还包括：

[0101] 所述终端设备的虚拟桌面代理客户端模块与所述虚拟机的虚拟桌面代理模块建立所述虚拟通道。

[0102] 具体地，建立虚拟通道的处理流程可以由终端设备的虚拟桌面代理客户端模块向虚拟机的虚拟桌面代理模块发起请求，也可以由虚拟机的虚拟桌面代理模块向终端设备的虚拟桌面代理客户端模块发起请求。

[0103] 图2为发明实施例提供的第二种虚拟机系统数据加密方法流程图。如图2所示，在本实施例中，所述虚拟机系统数据加密方法还可以包括：

[0104] 步骤C40、所述终端设备接收所述网络加密网关发送的经过传输层加密处理后的第三报文，将所述经过传输层加密处理后的第三报文进行传输层解密处理；

[0105] 步骤C50、所述终端设备从解密后的第一报文中提取已加密的应用数据，通过所述终端设备上设置的硬件加密模块对所述已加密的应用数据进行硬件解密处理，其中，所述已加密的应用数据为虚拟机系统中的虚拟机产生的、经过所述终端设备的硬件加密模块硬件加密处理过的数据；

[0106] 步骤C60、所述终端设备根据解密后的应用数据生成第四报文，对所述第四报文进行传输层加密处理，将传输层加密处理后的第四报文发送给所述网络加密网关。

[0107] 具体地，终端设备还可以通过硬件加密模块对虚拟机发送的已加密的应用数据进行解密。该已加密的应用数据为之前虚拟机的应用程序产生的，由该终端设备的硬件加密模块进行硬件加密处理后的数据。

[0108] 当虚拟机上的应用程序需要将已加密的应用数据解密时，虚拟机将该已加密的应用数据生成第三报文，将该第三报文发送给网络加密网关，网络加密网关对该第三报文进行传输层加密处理后发送给终端设备。终端设备接收网络加密网关发送的该经过传输层加密处理后的第三报文，进行传输层解密处理，该传输层解密过程也可以通过终端设备上设置的硬件加密模块实现。从解密后的第三报文中提取已加密的应用数据，再通过硬件加密模块的驱动接口函数将该已加密的应用数据发送给硬件加密模块，硬件加密模块将该已加密的应用数据通过密钥和/或数字证书解密后，将解密后的应用数据返回给终端设备，终端设备将解密后的应用数据生成第四报文，对该第四报文进行传输层加密后发送给网络加密网关，网络加密网关对接收到的第四报文进行传输层解密后发给虚拟机。虚拟机从第四报文中提取解密后的应用数据，对该应用数据进行相应的处理，该处理例如可以为将应用数据转发或将应用数据写入磁盘等操作。

[0109] 当虚拟机系统中的多个虚拟机同时需要对应用数据进行解密时，均可以通过上述

方法通过终端设备对应用数据进行解密。

[0110] 当然，在解密处理流程中，终端设备与虚拟机的交互也可以通过上述虚拟通道实现，具体实现过程，在此不再赘述。

[0111] 图3为本发明实施例提供的第三种虚拟机系统数据加密方法流程图。如图3所示，本实施例提供的虚拟机系统数据加密方法具体可以与本发明任意实施例提供的应用于终端设备的虚拟机系统数据加密方法配合实现，具体实现过程在此不再赘述。本实施例提供的虚拟机系统数据加密方法，具体包括：

[0112] 步骤S10、虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，将所述第一报文发送给网络加密网关；

[0113] 步骤S20、所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的。

[0114] 本实施例提供的虚拟机系统数据加密方法，虚拟机根据接收到的虚拟机中的应用程序发送的应用数据生成第一报文，将第一报文发送给网络加密网关，接收网络加密网关发送的经过传输层解密处理后的第二报文，提取经过传输层解密处理后的第二报文中的加密后的应用数据，将加密后的应用数据发送给应用程序，其中，加密后的应用数据为终端设备对应用处理进行硬件加密处理得到的。通过设置有硬件加密模块的终端设备对虚拟机产生的应用数据进行加密，无需在物理服务器上插设加密卡，实现了对物理服务器上的多个虚拟机的应用数据的加密支持。而且，该加密过程充分利用了终端设备的处理能力，减轻了虚拟机的负载。

[0115] 在本实施例中，步骤S10，所述虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，具体可以为：

[0116] 所述虚拟机根据接收到的所述应用程序发送的应用数据和密钥标识生成所述第一报文，其中，所述密钥标识用以标识密钥。

[0117] 当终端设备的硬件加密模块中存储有多个密钥时，通过密钥标识的设置，并不将真实的密钥传输，保证了密钥的安全性。

[0118] 在本实施例中，步骤S10，所述虚拟机将所述第一报文发送给网络加密网关，具体为：

[0119] 所述虚拟机通过所述虚拟机的虚拟桌面代理模块与所述终端设备的虚拟桌面代理客户端模块建立的经由所述网络加密网关的虚拟通道，将所述第一报文发送给所述网络加密网关；

[0120] 步骤S20，所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，具体为：

[0121] 所述虚拟机通过所述虚拟通道接收所述网络加密网关发送的经过传输层解密处理后的第二报文。

[0122] 在本实施例中，步骤S10，所述虚拟机将所述第一报文发送给网络加密网关之前，所述方法还可以包括：

[0123] 所述虚拟机的虚拟桌面代理模块与所述终端设备的虚拟桌面代理客户端模块建

立所述虚拟通道。

[0124] 图4为本发明实施例提供的第四种虚拟机系统数据加密方法流程图。如图4所示，所述虚拟机系统数据加密方法，还可以包括：

[0125] 步骤S30、所述虚拟机根据接收到的所述虚拟机中的应用程序发送的已加密的应用数据生成第三报文，将所述第三报文发送给网络加密网关；

[0126] 步骤S40、所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第四报文，提取所述经过传输层解密处理后的第四报文中的解密后的应用数据，将所述解密后的应用数据发送给所述应用程序，其中，所述解密后的应用数据为终端设备对所述已加密的应用处理进行硬件解密处理得到的。

[0127] 图5为本发明实施例提供的第一种终端设备结构示意图。如图5所示，本实施例提供的终端设备81具体可以实现本发明任意实施例提供的应用于终端设备的虚拟机系统数据加密方法的各个步骤，具体实现过程在此不再赘述。本实施例提供的终端设备81具体包括传输层解密模块11、加密服务模块12和传输层加密模块13。所述传输层解密模块11用于接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理；所述加密服务模块12与所述传输层解密模块11连接，用于从解密后的第一报文中提取应用数据，通过所述终端设备81上设置的硬件加密模块14对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；所述传输层加密模块13与所述加密服务模块12连接，用于根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关。

[0128] 本实施例提供的终端设备81，传输层解密模块11接收网络加密网关发送的经过传输层加密处理后的第一报文，将经过传输层加密处理后的第一报文进行传输层解密处理，加密服务模块12从解密后的第一报文中提取应用数据，通过终端设备81上设置的硬件加密模块14对应用数据进行硬件加密处理，其中，应用数据为虚拟机系统中的虚拟机产生的数据，传输层加密模块13根据加密后的应用数据生成第二报文，对第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给网络加密网关。通过设置有硬件加密模块14的终端设备81对虚拟机产生的应用数据进行加密，无需在物理服务器上插设加密卡，实现了对物理服务器上的多个虚拟机的应用数据的加密支持。而且，该加密过程充分利用了终端设备81的处理能力，减轻了虚拟机的负载。

[0129] 在本实施例中，所述第一报文中包括用以标识密钥的密钥标识；所述加密服务模块12具体用于从所述解密后的第一报文中提取所述应用数据和所述密钥标识，将所述应用数据和所述密钥标识发送给所述硬件加密模块14，所述硬件加密模块14根据所述密钥标识确定密钥，通过所述密钥对所述应用数据进行加密，将加密后的应用数据返回给所述终端设备81。

[0130] 图6为本发明实施例提供的第二种终端设备结构示意图。如图6所示，在本实施例中，所述终端设备81还包括虚拟桌面代理客户端模块15，所述虚拟桌面代理客户端模块15用于与所述虚拟机的虚拟桌面代理模块建立经由所述网络加密网关的虚拟通道；相应地，所述传输层解密模块11具体用于通过所述虚拟通道接收所述网络加密网关发送的所述经过传输层加密处理后的第一报文；所述传输层加密模块13具体用于将所述传输层加密处理

后的第二报文通过所述虚拟通道发送给所述网络加密网关。

[0131] 在本实施例中，所述传输层解密模块11还用于接收所述网络加密网关发送的经过传输层加密处理后的第三报文，将所述经过传输层加密处理后的第三报文进行传输层解密处理；所述加密服务模块12还从解密后的第一报文中提取已加密的应用数据，通过所述终端设备81上设置的硬件加密模块14对所述已加密的应用数据进行硬件解密处理，其中，所述已加密的应用数据为虚拟机系统中的虚拟机产生的、经过所述终端设备81的硬件加密模块14硬件加密处理过的数据；所述传输层加密模块13还用于根据解密后的应用数据生成第四报文，对所述第四报文进行传输层加密处理，将传输层加密处理后的第四报文发送给所述网络加密网关。

[0132] 图7为本发明实施例提供的第一种虚拟机结构示意图。如图7所示，本实施例提供的虚拟机82具体可以实现本发明任意实施例提供的应用于虚拟机的虚拟机系统数据加密方法的各个步骤，具体实现过程在此不再赘述。本实施例提供的虚拟机82具体包括发送处理模块21和接收处理模块22。所述发送处理模块21用于根据接收到的所述虚拟机82中的应用程序发送的应用数据生成第一报文，将所述第一报文发送给网络加密网关；所述接收处理模块22用于接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的。

[0133] 具体地，在实际实现过程中，虚拟机82中的应用程序可以通过调用发送处理模块21的API(Application Programming Interface，应用程序编程接口)，将应用数据发送给发送处理模块21。

[0134] 本实施例提供的虚拟机82，发送处理模块21根据接收到的虚拟机82中的应用程序发送的应用数据生成第一报文，将第一报文发送给网络加密网关，接收处理模块22接收网络加密网关发送的经过传输层解密处理后的第二报文，提取经过传输层解密处理后的第二报文中的加密后的应用数据，将加密后的应用数据发送给应用程序，其中，加密后的应用数据为终端设备对应用处理进行硬件加密处理得到的。通过设置有硬件加密模块的终端设备对虚拟机82产生的应用数据进行加密，无需在物理服务器上插设加密卡，实现了对物理服务器上的多个虚拟机82的应用数据的加密支持。而且，该加密过程充分利用了终端设备的处理能力，减轻了虚拟机82的负载。

[0135] 在本实施例中，所述发送处理模块21具体用于根据接收到的所述应用程序发送的应用数据和密钥标识生成所述第一报文，其中，所述密钥标识用以标识密钥。

[0136] 图8为本发明实施例提供的第二种虚拟机结构示意图。如图8所示，在本实施例中，所述虚拟机82还包括虚拟桌面代理模块23，所述虚拟桌面代理模块23，用于与所述终端设备的虚拟桌面代理客户端模块建立经由所述网络加密网关的虚拟通道；相应地，所述发送处理模块21具体用于通过所述虚拟通道将所述第一报文发送给所述网络加密网关；所述接收处理模块22具体用于通过所述虚拟通道接收所述网络加密网关发送的经过传输层解密处理后的第二报文。

[0137] 在本实施例中，所述发送处理模块21还用于根据接收到的所述虚拟机82中的应用程序发送的已加密的应用数据生成第三报文，将所述第三报文发送给网络加密网关；所述

接收处理模块22还用于接收所述网络加密网关发送的经过传输层解密处理后的第四报文，提取所述经过传输层解密处理后的第四报文中的解密后的应用数据，将所述解密后的应用数据发送给所述应用程序，其中，所述解密后的应用数据为终端设备对所述已加密的应用处理进行硬件解密处理得到的。

[0138] 图9为本发明实施例提供的第三种终端设备结构示意图。如图9所示，本实施例提供的终端设备700具体可以实现本发明任意实施例提供的应用于终端设备的虚拟机系统数据加密方法的各个步骤，具体实现过程在此不再赘述。本实施例提供的终端设备700具体包括：处理器710，通信接口720，存储器730和通信总线740：其中所述处理器710、所述通信接口720和所述存储器730通过所述通信总线740完成相互间的通信；所述通信接口720，用于接收网络加密网关发送的经过传输层加密处理后的第一报文，以及将传输层加密处理后的第二报文发送给所述网络加密网关；所述存储器730，用于存储指令；所述处理器710被配置为执行存储在所述存储器730中的指令，其中，所述处理器710被配置为用于将所述经过传输层加密处理后的第一报文进行传输层解密处理，从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据；根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理。

[0139] 图10为本发明实施例提供的用于虚拟机的计算机节点结构示意图。如图10所述，本实施例提供的用于虚拟机的计算机节点800具体可以实现本发明任意实施例提供的应用于虚拟机的虚拟机系统数据加密方法的各个步骤，具体实现过程在此不再赘述。本实施例提供的用于虚拟机的计算机节点800具体包括：处理器810，通信接口820，存储器830和通信总线840：其中所述处理器810、所述通信接口820和所述存储器830通过所述通信总线840完成相互间的通信；所述通信接口820，用于将第一报文发送给网络加密网关，以及接收所述网络加密网关发送的经过传输层解密处理后的第二报文；所述存储器830，用于存储指令；所述处理器810被配置为执行存储在所述存储器830中的指令，其中，所述处理器810被配置为用于根据接收到的所述虚拟机中的应用程序发送的应用数据生成所述第一报文；提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的。

[0140] 本领域普通技术人员可以理解：实现上述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。

[0141] 最后应说明的是：以上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范围。

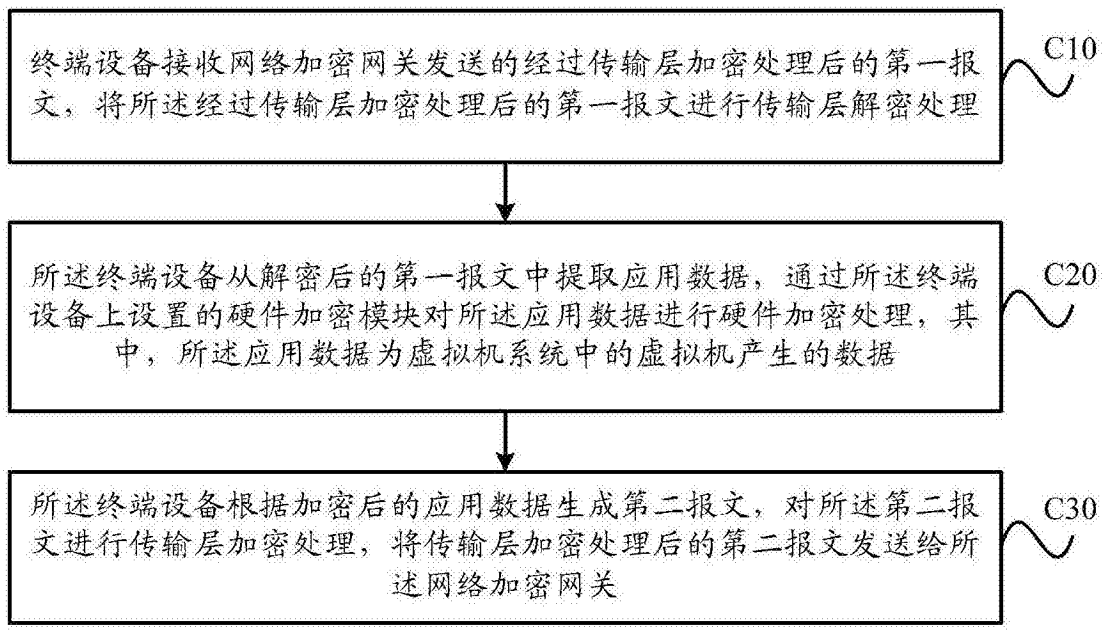

终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理
C10
所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据
C20
所述终端设备根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关
C30

图1

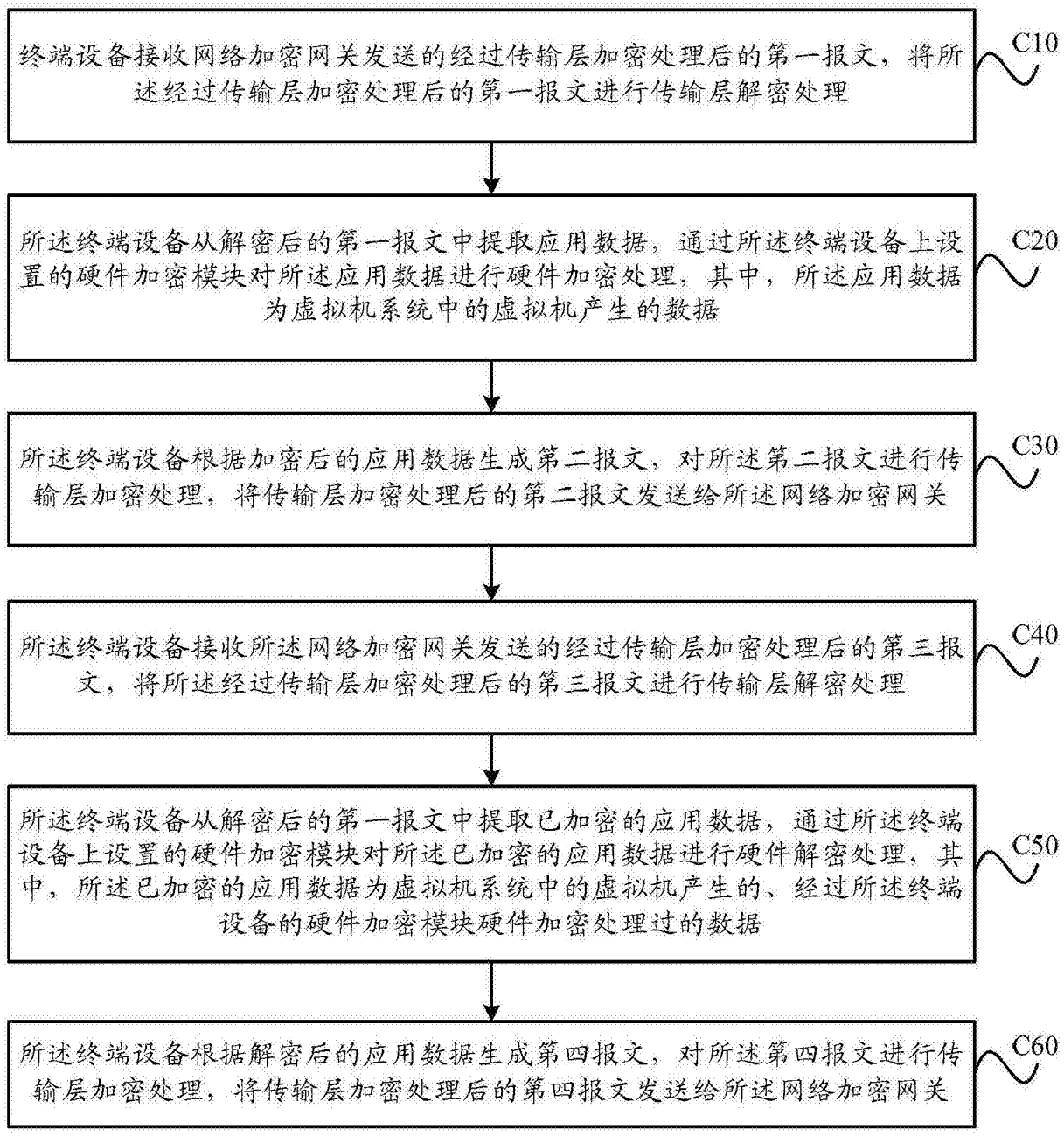

终端设备接收网络加密网关发送的经过传输层加密处理后的第一报文，将所述经过传输层加密处理后的第一报文进行传输层解密处理
C10
所述终端设备从解密后的第一报文中提取应用数据，通过所述终端设备上设置的硬件加密模块对所述应用数据进行硬件加密处理，其中，所述应用数据为虚拟机系统中的虚拟机产生的数据
C20
所述终端设备根据加密后的应用数据生成第二报文，对所述第二报文进行传输层加密处理，将传输层加密处理后的第二报文发送给所述网络加密网关
C30
所述终端设备接收所述网络加密网关发送的经过传输层加密处理后的第三报文，将所述经过传输层加密处理后的第三报文进行传输层解密处理
C40
所述终端设备从解密后的第一报文中提取已加密的应用数据，通过所述终端设备上设置的硬件加密模块对所述已加密的应用数据进行硬件解密处理，其中，所述已加密的应用数据为虚拟机系统中的虚拟机产生的、经过所述终端设备的硬件加密模块硬件加密处理过的数据
C50
所述终端设备根据解密后的应用数据生成第四报文，对所述第四报文进行传输层加密处理，将传输层加密处理后的第四报文发送给所述网络加密网关
C60

图2

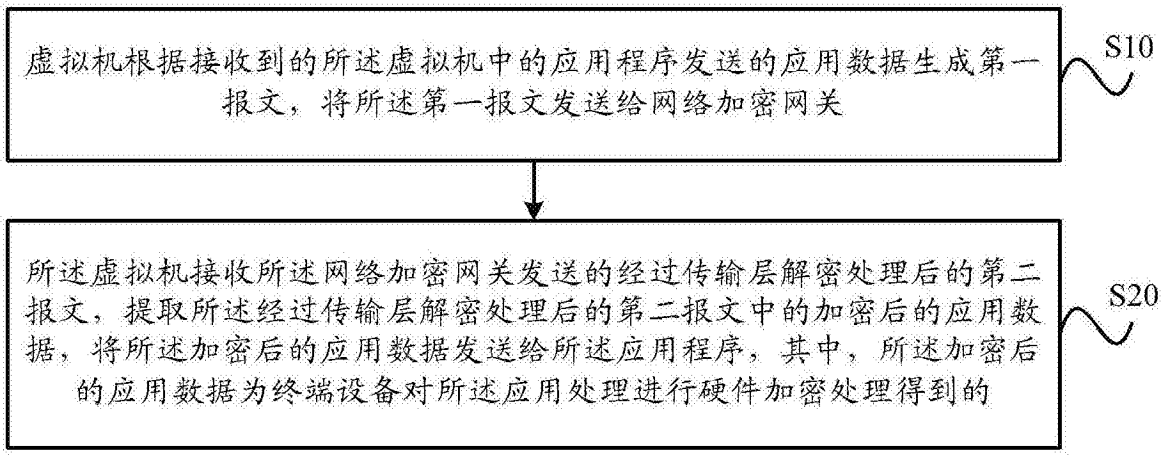

虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，将所述第一报文发送给网络加密网关
S10
所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的
S20

图3

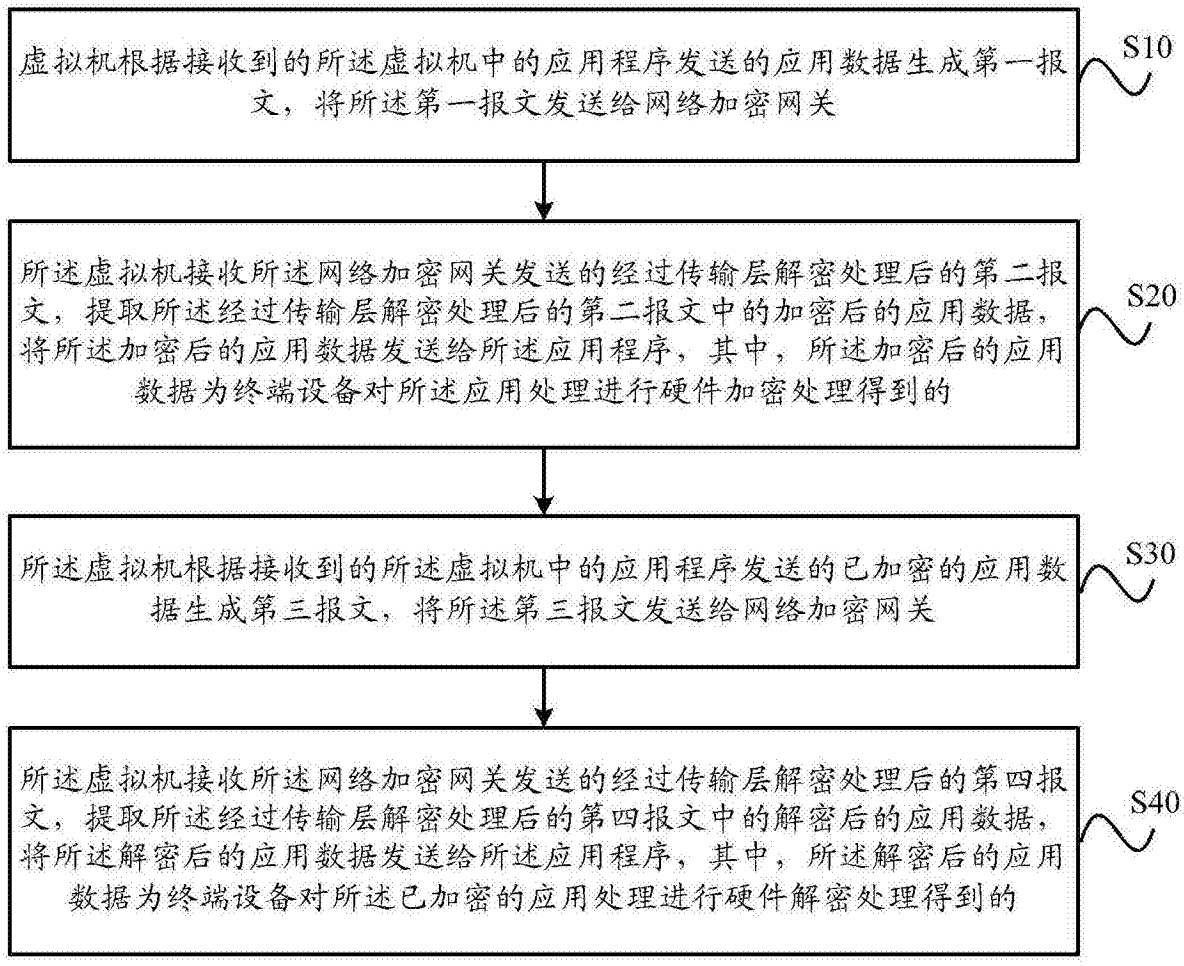

虚拟机根据接收到的所述虚拟机中的应用程序发送的应用数据生成第一报文，将所述第一报文发送给网络加密网关
S10
所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第二报文，提取所述经过传输层解密处理后的第二报文中的加密后的应用数据，将所述加密后的应用数据发送给所述应用程序，其中，所述加密后的应用数据为终端设备对所述应用处理进行硬件加密处理得到的
S20
所述虚拟机根据接收到的所述虚拟机中的应用程序发送的已加密的应用数据生成第三报文，将所述第三报文发送给网络加密网关
S30
所述虚拟机接收所述网络加密网关发送的经过传输层解密处理后的第四报文，提取所述经过传输层解密处理后的第四报文中的解密后的应用数据，将所述解密后的应用数据发送给所述应用程序，其中，所述解密后的应用数据为终端设备对所述已加密的应用处理进行硬件解密处理得到的
S40

图4

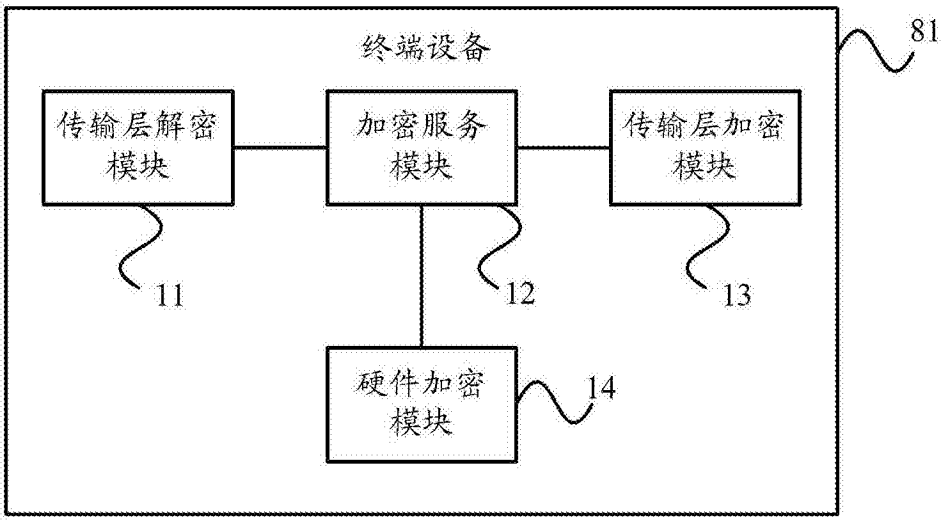

终端设备
81
传输层解密模块
加密服务模块
传输层加密模块
11
12
13
硬件加密模块
14

图5

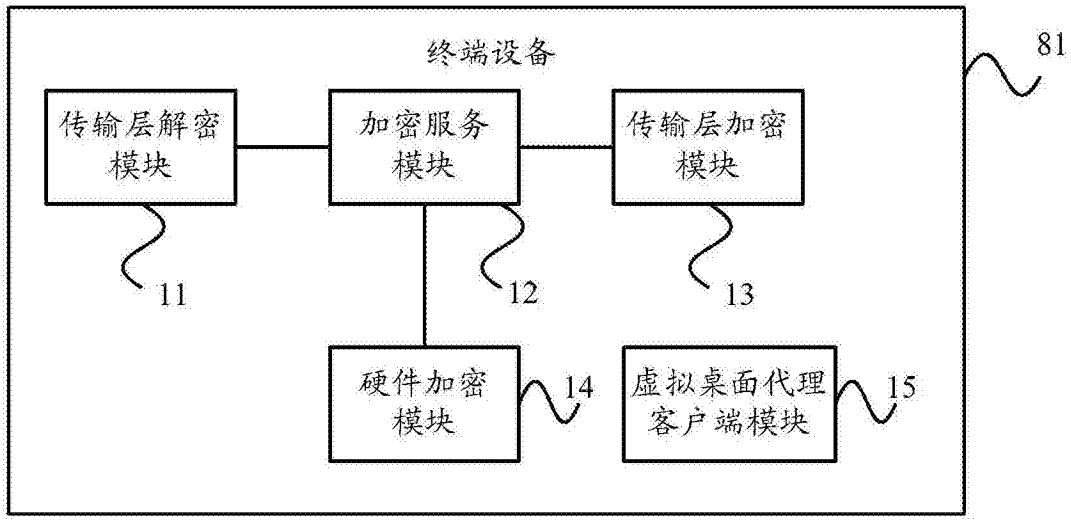

终端设备
81
传输层解密模块
加密服务模块
传输层加密模块
11
12
13
硬件加密模块
14
虚拟桌面代理客户端模块
15

图6

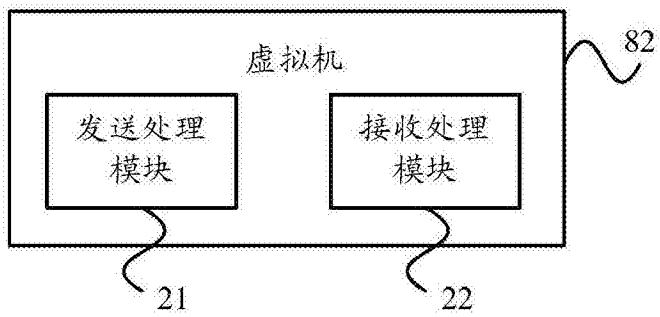

虚拟机
82
发送处理模块
接收处理模块
21
22

图7

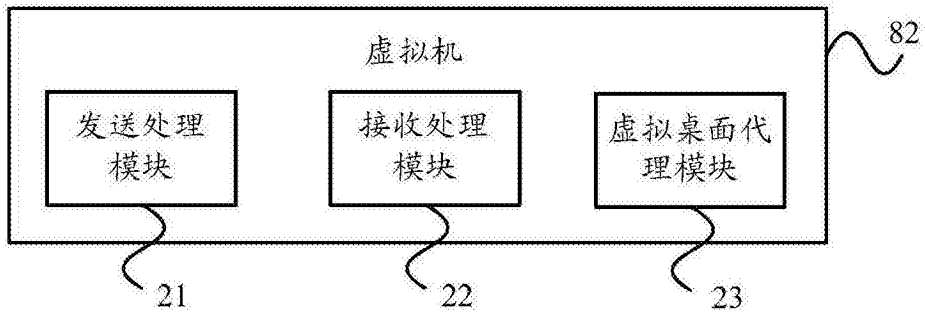

虚拟机
82
发送处理模块
接收处理模块
虚拟桌面代理模块
21
22
23

图8

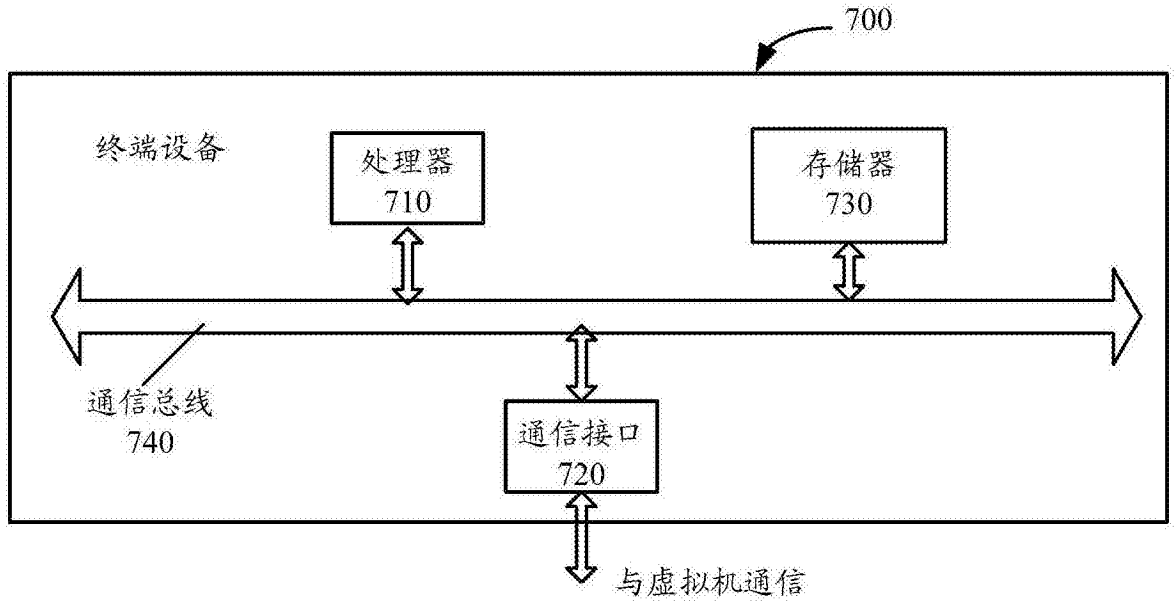

700
终端设备
处理器
710
存储器
730
通信总线
740
通信接口
720
与虚拟机通信

图9

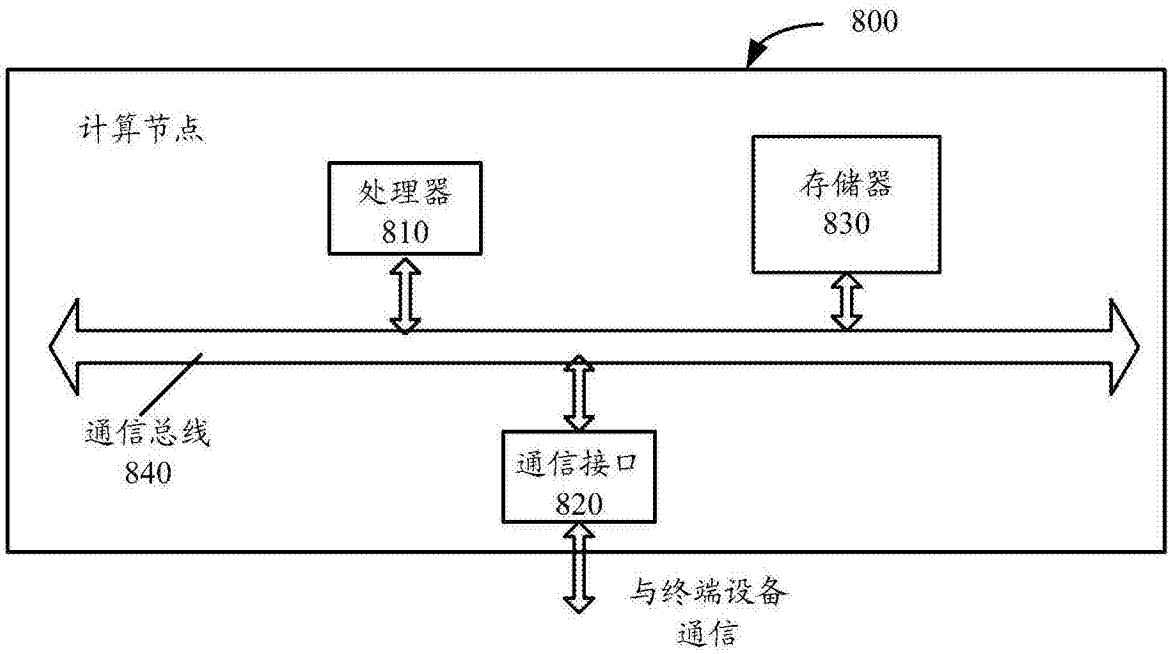


图10