(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 106130968 B
(45)授权公告日 2019.05.03

(21)申请号 201610450080.X

(22)申请日 2016.06.21

(65)同一申请的已公布的文献号
申请公布号 CN 106130968 A

(43)申请公布日 2016.11.16

(73)专利权人 佛山科学技术学院
地址 528231 广东省佛山市禅城区江湾一路18号

(72)发明人 钟勇 马莉 霍颖瑜

(74)专利代理机构 广州市红荔专利代理有限公司 44214
代理人 张文

(51)Int.Cl.
H04L 29/06(2006.01)
G10L 17/02(2013.01)

(56)对比文件
CN 102957688 A,2013.03.06,
CN 103281359 A,2013.09.04,
CN 104715183 A,2015.06.17,
CN 102298929 A,2011.12.28,
US 2006277043 A1,2006.12.07,

审查员 王黎明

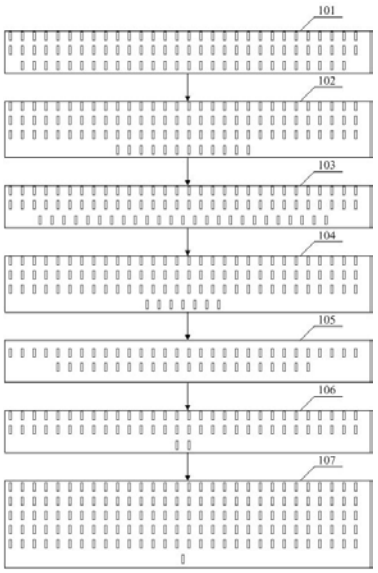
权利要求书3页 说明书8页 附图2页

(54)发明名称

一种身份认证方法、及系统

(57)摘要

本发明实施例公开了一种身份认证方法、及系统，其中方法应用于包含云服务器以及终端设备的云计算网络包括：所述终端设备显示一段随机生成的文字信息并提示所述终端设备的当前的用户读所述文字信息；对音频数据进行特征提取得到语音特征；在所述终端设备中显示提示信息，提示所述用户输入所述用户设置的密码的密码类型；确定所述用户为所述用户身份信息所对应的用户身份；向所述云服务器发送服务请求，携带所述用户身份的信息且指定了云计算服务的具体内容；确定所述虚拟机在运行过程中服务参数是否有被修改，若有并且不是所述终端设备发送的新的服务请求导致的修改，则确定所述虚拟机存在安全风险。具有极高的安全性并且方便使用。



CN 106130968 B

1.一种身份认证方法,应用于包含云服务器以及终端设备的云计算网络,其特征在于,包括:

所述终端设备显示一段随机生成的文字信息并提示所述终端设备的当前的用户读所述文字信息;通过音频采集设备采集所述用户读所述文字信息的音频数据,对所述音频数据进行特征提取得到语音特征;

所述终端设备从数据库中查找与所述语音特征匹配的用户身份信息,并确定所述用户身份信息在所述数据库中保存的密码所包含的密码类型;所述密码类型的组合包含:数字、字母大写、字母小写、数学符号、标点符号中的至少一项;

所述终端设备在所述终端设备中显示提示信息,提示所述用户输入所述用户设置的密码的密码类型,并显示至少三个且种类大于所述数据库中保存的密码所包含的密码类型两倍的密码类型供选择;

所述终端设备接收所述用户从显示的密码类型中选择的密码类型,若所述用户从显示的密码类型中选择的密码类型与所述数据库中保存的密码所包含的密码类型相同,则确定所述用户为所述用户身份信息所对应的用户身份;

所述终端设备向所述云服务器发送服务请求,所述服务请求内携带所述用户身份的信息且指定了云计算服务的具体内容;

所述云服务器在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机;为所述虚拟机配置针对所述云计算服务的具体内容的服务参数;

所述云服务器内包含安全运行环境,在所述安全运行环境下的程序在运行过程不接受外部程序的请求导致的中断以及数据修改;在所述安全运行环境下运行监测程序对所述服务参数进行监测,确定所述虚拟机在运行过程中所述服务参数是否有被修改,若有并且不是所述终端设备发送的新的服务请求导致的修改,则确定所述虚拟机存在安全风险。

2.根据权利要求1所述方法,其特征在于,所述方法还包括:

所述云服务器在创建所述虚拟机的过程中,从所述云服务器的存储块中以随机方式选择在存储空间不连续的存储块组成所述虚拟机的存储空间,将选择的存储块与所述虚拟机的对应关系保存在可信的存储空间内,所述可信的存储空间具有允许所述虚拟机获取所述对应关系以及允许所述云服务器删除和修改所述对应关系,并且拒绝所述云服务器、所述终端设备以及其他任意设备的其他操作的功能;记录选择的存储块为已分配的存储块,在新创建其他虚拟机时不再次分配记录为已分配的存储块;为所述虚拟机分配共享存储空间,在所述共享存储空间中存储有所述虚拟机启动和运行所必要的驱动程序以及操作系统;为所述虚拟机配置针对所述云计算服务的具体内容的服务参数;

所述云服务器在确定所述虚拟机存在安全风险后,删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系。

3.根据权利要求1所述方法,其特征在于,所述终端设备显示一段随机生成的文字信息之前,方法还包括:

所述终端设备显示请用户输入密码,且密码需要具有两种或者两种以上的密码类型的提示信息;接收所述用户输入的密码,若所述用户输入的密码少于两种,则提示所述用户输入的密码类型少于两种,在接收到确认指令后将接收到的密码存入数据库。

4.根据权利要求1至3任意一项所述方法,其特征在于,所述为所述虚拟机配置针对所

述云计算服务的具体内容的服务参数包括：

针对所述云计算服务的具体内容为所述虚拟机配置的向外部发送数据的权限和所述终端设备对所述虚拟机的操作权限。

5.根据权利要求4所述方法，其特征在于，所述云服务器在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机包括：

所述云服务器在确定所述云计算服务的具体内容与所述用户身份相适应后，创建与用户身份相适应的权限以及数据内容的虚拟机。

6.根据权利要求2所述方法，其特征在于，所述删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系之后，所述方法还包括：

将所述选择的存储块记录为未分配的存储块，且不删除所述选择的存储块内存储的数据内容；在有需求创建新的虚拟机时，从未分配的存储块内以随机方式选择在存储空间不连续的存储块组成待创建的新的虚拟机的存储空间。

7.根据权利要求2任意一项所述方法，其特征在于，

在所述共享存储空间中存储的所述虚拟机启动和运行所必要的驱动程序以及操作系统安装于沙箱内，所述沙箱具有输入接口以及输出接口；所述输入接口具有过滤对所述共享存储空间中存储的任意数据进行修改的指令的过滤功能。

8.一种网络系统，包括：终端设备和云服务器，其特征在于，

所述终端设备，用于显示一段随机生成的文字信息并提示所述终端设备的当前的用户读所述文字信息；通过音频采集设备采集所述用户读所述文字信息的音频数据，对所述音频数据进行特征提取得到语音特征；从数据库中查找与所述语音特征匹配的用户身份信息，并确定所述用户身份信息在所述数据库中保存的密码所包含的密码类型；所述密码类型的组合包含：数字、字母大写、字母小写、数学符号、标点符号中的至少一项；在所述终端设备中显示提示信息，提示所述用户输入所述用户设置的密码的密码类型，并显示至少三个且种类大于所述数据库中保存的密码所包含的密码类型两倍的密码类型供选择；接收所述用户从显示的密码类型中选择的密码类型，若所述用户从显示的密码类型中选择的密码类型与所述数据库中保存的密码所包含的密码类型相同，则确定所述用户为所述用户身份信息所对应的用户身份；向所述云服务器发送服务请求，所述服务请求内携带所述用户身份的信息且指定了云计算服务的具体内容；

所述云服务器，用于在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机；为所述虚拟机配置针对所述云计算服务的具体内容的服务参数；所述云服务器内包含安全运行环境，在所述安全运行环境下的程序在运行过程不接受外部程序的请求导致的中断以及数据修改；在所述安全运行环境下运行监测程序对所述服务参数进行监测，确定所述虚拟机在运行过程中所述服务参数是否有被修改，若有并且不是所述终端设备发送的新的服务请求导致的修改，则确定所述虚拟机存在安全风险。

9.根据权利要求8所述网络系统，其特征在于，

所述云服务器，还用于在创建所述虚拟机的过程中，从所述云服务器的存储块中以随机方式选择在存储空间不连续的存储块组成所述虚拟机的存储空间，将选择的存储块与所述虚拟机的对应关系保存在可信的存储空间内，所述可信的存储空间具有允许所述虚拟机获取所述对应关系以及允许所述云服务器删除和修改所述对应关系，并且拒绝所述云服务

器、所述终端设备以及其他任意设备的其他操作的功能；记录选择的存储块为已分配的存储块，在新创建其他虚拟机时不再次分配记录为已分配的存储块；为所述虚拟机分配共享存储空间，在所述共享存储空间中存储有所述虚拟机启动和运行所必要的驱动程序以及操作系统；为所述虚拟机配置针对所述云计算服务的具体内容的服务参数；在确定所述虚拟机存在安全风险后，删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系。

10.根据权利要求9所述网络系统，其特征在于，

所述终端设备，还用于显示一段随机生成的文字信息之前，显示请用户输入密码，且密码需要具有两种或者两种以上的密码类型的提示信息；接收所述用户输入的密码，若所述用户输入的密码少于两种，则提示所述用户输入的密码类型少于两种，在接收到确认指令后将接收到的密码存入数据库；

所述云服务器，用于为所述虚拟机配置针对所述云计算服务的具体内容的服务参数包括：具体用于针对所述云计算服务的具体内容为所述虚拟机配置的向外部发送数据的权限和所述终端设备对所述虚拟机的操作权限；

所述云服务器，用于在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机包括：具体用于在确定所述云计算服务的具体内容与所述用户身份相适应后，创建与用户身份相适应的权限以及数据内容的虚拟机；

所述云服务器，还用于所述删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系之后，将所述选择的存储块记录为未分配的存储块，且不删除所述选择的存储块内存储的数据内容；在有需求创建新的虚拟机时，从未分配的存储块内以随机方式选择在存储空间不连续的存储块组成待创建的新的虚拟机的存储空间；

在所述共享存储空间中存储的所述虚拟机启动和运行所必要的驱动程序以及操作系统安装于沙箱内，所述沙箱具有输入接口以及输出接口；所述输入接口具有过滤对所述共享存储空间中存储的任意数据进行修改的指令的过滤功能。

一种身份认证方法、及系统

技术领域

[0001] 本发明涉及计算机技术领域，特别涉及一种身份认证方法、及系统。

背景技术

[0002] 身份认证也称为“身份验证”或“身份鉴别”，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

[0003] 目前较为广泛使用的身份认证有：指纹认证，但是指纹认证需要设备具有指纹采集设备；另外一种方案是：密码认证，具体如下：用户输入密码预先设置的密码，由设备对用户输入的密码与预先设置的密码进行比对。

[0004] 密码认证的方案需要用户记住密码，通常用户会有各种设置密码的需求，例如：银行卡密码、即时通讯工具的密码，或者其他；一旦用户忘记密码或者记混密码，那么将会导致用户难以实现身份认证，因此密码认证方式对于用户而言较为复杂。

发明内容

[0005] 本发明实施例提供了一种身份认证方法、及系统，用于提身份认证的效率，降低身份认证的复杂度。

[0006] 一方面本发明实施例提供了一种身份认证方法，应用于包含云服务器以及终端设备的云计算网络，包括：

[0007] 所述终端设备显示一段随机生成的文字信息并提示所述终端设备的当前的用户读所述文字信息；通过音频采集设备采集所述用户读所述文字信息的音频数据，对所述音频数据进行特征提取得到语音特征；

[0008] 所述终端设备从数据库中查找与所述语音特征匹配的用户身份信息，并确定所述用户身份信息在所述数据库中保存的密码所包含的密码类型；所述密码类型的组合包含：数字、字母大写、字母小写、数学符号、标点符号中的至少一项；

[0009] 所述终端设备在所述终端设备中显示提示信息，提示所述用户输入所述用户设置的密码的密码类型，并显示至少三个且种类大于所述数据库中保存的密码所包含的密码类型两倍的密码类型供选择；

[0010] 所述终端设备接收所述用户从显示的密码类型中选择的密码类型，若所述用户从显示的密码类型中选择的密码类型与所述数据库中保存的密码所包含的密码类型相同，则确定所述用户为所述用户身份信息所对应的用户身份；

[0011] 所述终端设备向所述云服务器发送服务请求，所述服务请求内携带所述用户身份的信息且指定了云计算服务的具体内容；

[0012] 所述云服务器在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机；为所述虚拟机配置针对所述云计算服务的具体内容的服务参数；

[0013] 所述云服务器内包含安全运行环境，在所述安全运行环境下的程序在运行过程不接受外部程序的请求导致的中断以及数据修改；在所述安全运行环境下运行监测程序对所述服务参数进行监测，确定所述虚拟机在运行过程中所述服务参数是否有被修改，若有并且不是所述终端设备发送的新的服务请求导致的修改，则确定所述虚拟机存在安全风险 。

[0014] 在一个可能的实现方式中，所述方法还包括：

[0015] 所述云服务器在创建所述虚拟机的过程中，从所述云服务器的存储块中以随机方式选择在存储空间不连续的存储块组成所述虚拟机的存储空间，将选择的存储块与所述虚拟机的对应关系保存在可信的存储空间内，所述可信的存储空间具有允许所述虚拟机获取所述对应关系以及允许所述云服务器删除和修改所述对应关系，并且拒绝所述云服务器、所述终端设备以及其他任意设备的其他操作的功能；记录选择的存储块为已分配的存储块，在新创建其他虚拟机时不再次分配记录为已分配的存储块；为所述虚拟机分配共享存储空间，在所述共享存储空间中存储有所述虚拟机启动和运行所必要的驱动程序以及操作系统；为所述虚拟机配置针对所述云计算服务的具体内容的服务参数；

[0016] 所述云服务器在确定所述虚拟机存在安全风险后，删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系。

[0017] 在一个可能的实现方式中，所述终端设备显示一段随机生成的文字信息之前，方法还包括：

[0018] 所述终端设备显示请用户输入密码，且密码需要具有两种或者两种以上的密码类型的提示信息；接收所述用户输入的密码，若所述用户输入的密码少于两种，则提示所述用户输入的密码类型少于两种，在接收到确认指令后将接收到的密码存入数据库。

[0019] 在一个可能的实现方式中，所述为所述虚拟机配置针对所述云计算服务的具体内容的服务参数包括：

[0020] 针对所述云计算服务的具体内容为所述虚拟机配置的向外部发送数据的权限和所述终端设备对所述虚拟机的操作权限。

[0021] 在一个可能的实现方式中，所述云服务器在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机包括：

[0022] 所述云服务器在确定所述云计算服务的具体内容与所述用户身份相适应后，创建与用户身份相适应的权限以及数据内容的虚拟机。

[0023] 在一个可能的实现方式中，所述删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系之后，所述方法还包括：

[0024] 将所述选择的存储块记录为未分配的存储块，且不删除所述选择的存储块内存储的数据内容；在有需求创建新的虚拟机时，从未分配的存储块内以随机方式选择在存储空间不连续的存储块组成待创建的新的虚拟机的存储空间。

[0025] 在一个可能的实现方式中，在所述共享存储空间中存储的所述虚拟机启动和运行所必要的驱动程序以及操作系统安装于沙箱内，所述沙箱具有输入接口以及输出接口；所述输入接口具有过滤对所述共享存储空间中存储的任意数据进行修改的指令的过滤功能。

[0026] 二方面本发明实施例还提供了一种网络系统，包括：终端设备和云服务器；所述终端设备，用于显示一段随机生成的文字信息并提示所述终端设备的当前的用户读所述文字信息；通过音频采集设备采集所述用户读所述文字信息的音频数据，对所述音频数据进行

特征提取得到语音特征;从数据库中查找与所述语音特征匹配的用户身份信息,并确定所述用户身份信息在所述数据库中保存的密码所包含的密码类型;所述密码类型的组合包含:数字、字母大写、字母小写、数学符号、标点符号中的至少一项;在所述终端设备中显示提示信息,提示所述用户输入所述用户设置的密码的密码类型,并显示至少三个且种类大于所述数据库中保存的密码所包含的密码类型两倍的密码类型供选择;接收所述用户从显示的密码类型中选择的密码类型,若所述用户从显示的密码类型中选择的密码类型与所述数据库中保存的密码所包含的密码类型相同,则确定所述用户为所述用户身份信息所对应的用户身份;向所述云服务器发送服务请求,所述服务请求内携带所述用户身份的信息且指定了云计算服务的具体内容;

[0027] 所述云服务器,用于在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机;为所述虚拟机配置针对所述云计算服务的具体内容的服务参数;所述云服务器内包含安全运行环境,在所述安全运行环境下的程序在运行过程不接受外部程序的请求导致的中断以及数据修改;在所述安全运行环境下运行监测程序对所述服务参数进行监测,确定所述虚拟机在运行过程中所述服务参数是否有被修改,若有并且不是所述终端设备发送的新的服务请求导致的修改,则确定所述虚拟机存在安全风险。

[0028] 在一个可能的实现方式中,所述云服务器,还用于在创建所述虚拟机的过程中,从所述云服务器的存储块中以随机方式选择在存储空间不连续的存储块组成所述虚拟机的存储空间,将选择的存储块与所述虚拟机的对应关系保存在可信的存储空间内,所述可信的存储空间具有允许所述虚拟机获取所述对应关系以及允许所述云服务器删除和修改所述对应关系,并且拒绝所述云服务器、所述终端设备以及其他任意设备的其他操作的功能;记录选择的存储块为已分配的存储块,在新创建其他虚拟机时不再次分配记录为已分配的存储块;为所述虚拟机分配共享存储空间,在所述共享存储空间中存储有所述虚拟机启动和运行所必要的驱动程序以及操作系统;为所述虚拟机配置针对所述云计算服务的具体内容的服务参数;在确定所述虚拟机存在安全风险后,删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系。

[0029] 在一个可能的实现方式中,所述终端设备,还用于显示一段随机生成的文字信息之前,显示请用户输入密码,且密码需要具有两种或者两种以上的密码类型的提示信息;接收所述用户输入的密码,若所述用户输入的密码少于两种,则提示所述用户输入的密码类型少于两种,在接收到确认指令后将接收到的密码存入数据库;

[0030] 所述云服务器,用于为所述虚拟机配置针对所述云计算服务的具体内容的服务参数包括:具体用于针对所述云计算服务的具体内容为所述虚拟机配置的向外部发送数据的权限和所述终端设备对所述虚拟机的操作权限;

[0031] 所述云服务器,用于在所述云服务器内创建针对所述云计算服务的具体内容的虚拟机包括:具体用于在确定所述云计算服务的具体内容与所述用户身份相适应后,创建与用户身份相适应的权限以及数据内容的虚拟机;

[0032] 所述云服务器,还用于所述删除所述可信的存储空间内保存的所述选择的存储块与所述虚拟机的对应关系之后,将所述选择的存储块记录为未分配的存储块,且不删除所述选择的存储块内存储的数据内容;在有需求创建新的虚拟机时,从未分配的存储块内以随机方式选择在存储空间不连续的存储块组成待创建的新的虚拟机的存储空间;

[0033] 在所述共享存储空间中存储的所述虚拟机启动和运行所必要的驱动程序以及操作系统安装于沙箱内，所述沙箱具有输入接口以及输出接口；所述输入接口具有过滤对所述共享存储空间中存储的任意数据进行修改的指令的过滤功能。

[0034] 沙箱是一种按照安全策略限制程序行为的执行环境。早期主要用于测试可疑软件等，比如黑客们为了试用某种病毒或者不安全产品，往往可以将它们在沙箱环境中运行，因此沙箱本身是封闭的环境可以控制病毒的传播，本实施例中提供了一个输入接口以及输出接口，规定了输入输出接口所接收指令的类型，保证其安全性。

[0035] 从以上技术方案可以看出，本发明实施例具有以下优点：不用用户记住自己设置的密码，仅需要记得密码有哪些密码类型就可以了，例如：zhongguo123，包含两种密码类型：字母小写和数字。用随机生成的文字信息，用户读一遍就可以了，终端设备分析语音数据得到语音特征；由于文字信息是随机生成的，这可以避免用户语音被录下来导致的安全风险；另外，这步虽然可以实现用户身份的确定，但是有可能存在错误；这种错误有可能是语音特征较少导致的，或者其他原因导致的，例如：用户的声音被模仿；那么通过密码的第二次认证可以消除这种情况的发生，进一步提高安全性。另外，安全运行环境可以是以硬件形式写入嵌入式软件的方式提供的安全运行环境，该安全运行环境独立于虚拟机之外，不受虚拟机的影响，还可以进一步属于云服务器的独立运行环境，不受云服务器内运行的其他软件的影响，因此该监测程序被攻击导致不能准确监测的可能性被消除，从而保证监测结果的准确性；该方案不需要对云计算网络内的所有文件进行病毒扫描，因此数据处理量将会极少，可以提高系统性能。

附图说明

[0036] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，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，对于本领域的普通技术人员来讲，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。

[0037] 图1为本发明实施例方法流程示意图；

[0038] 图2为本发明实施例系统架构示意图。

具体实施方式

[0039] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部份实施例，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它实施例，都属于本发明保护的范围。

[0040] 本发明实施例提供了一种身份认证方法，应用于包含云服务器以及终端设备的云计算网络，如图1所示，包括：

[0041] 101：上述终端设备显示一段随机生成的文字信息并提示上述终端设备的当前的用户读上述文字信息；通过音频采集设备采集上述用户读上述文字信息的音频数据，对上述音频数据进行特征提取得到语音特征；

[0042] 语音特征可以是包含用于区分人声音的各种特征信息，例如：音色特征、响度特

征，还可以结合方言导致将会读错文字的特征，等等。

[0043] 102：上述终端设备从数据库中查找与上述语音特征匹配的用户身份信息，并确定上述用户身份信息在上述数据库中保存的密码所包含的密码类型；上述密码类型的组合包含：数字、字母大写、字母小写、数学符号、标点符号中的至少一项；

[0044] 103：上述终端设备在上述终端设备中显示提示信息，提示上述用户输入上述用户设置的密码的密码类型，并显示至少三个且种类大于上述数据库中保存的密码所包含的密码类型两倍的密码类型供选择；

[0045] 104：上述终端设备接收上述用户从显示的密码类型中选择的密码类型，若上述用户从显示的密码类型中选择的密码类型与上述数据库中保存的密码所包含的密码类型相同，则确定上述用户为上述用户身份信息所对应的用户身份；

[0046] 其中，确定上述用户为所述用户身份信息所对应的用户身份，应该理解为：确定上述用户的身份为上述用户身份信息所对应的用户身份。

[0047] 105：上述终端设备向上述云服务器发送服务请求，上述服务请求内携带上述用户身份的信息且指定了云计算服务的具体内容；

[0048] 106：上述云服务器在上述云服务器内创建针对上述云计算服务的具体内容的虚拟机；为上述虚拟机配置针对上述云计算服务的具体内容的服务参数；

[0049] 107：上述云服务器内包含安全运行环境，在上述安全运行环境下的程序在运行过程不接受外部程序的请求导致的中断以及数据修改；在上述安全运行环境下运行监测程序对上述服务参数进行监测，确定上述虚拟机在运行过程中上述服务参数是否有被修改，若有并且不是上述终端设备发送的新的服务请求导致的修改，则确定上述虚拟机存在安全风险 。

[0050] 本实施例，不用用户记住自己设置的密码，仅需要记得密码有哪些密码类型就可以了，例如：zhongguo123，包含两种密码类型：字母小写和数字。用随机生成的文字信息，用户读一遍就可以了，终端设备分析语音数据得到语音特征；由于文字信息是随机生成的，这可以避免用户语音被录下来导致的安全风险；另外，这步虽然可以实现用户身份的确定，但是有可能存在错误；这种错误有可能是语音特征较少导致的，或者其他原因导致的，例如：用户的声音被模仿；那么通过密码的第二次认证可以消除这种情况的发生，进一步提高安全性。

[0051] 在本实施例中，云计算服务的具体内容，可以是云计算服务所需要的具体服务内容，比如：报表合并的服务，或者，数据挖掘的大数据计算服务，等等；云计算服务的具体内容依需求不同可能会有所不同，本发明实施例对此不作唯一性限定。

[0052] 在本实施例中，安全运行环境可以是以硬件形式写入嵌入式软件的方式提供的安全运行环境，该安全运行环境独立于虚拟机之外，不受虚拟机的影响，还可以进一步属于云服务器的独立运行环境，不受云服务器内运行的其他软件的影响，因此该监测程序被攻击导致不能准确监测的可能性被消除，从而保证监测结果的准确性；该方案不需要对云计算网络内的所有文件进行病毒扫描，因此数据处理量将会极少，可以提高整个云计算系统的性能。

[0053] 进一步地，上述方法还包括：

[0054] 上述云服务器在创建上述虚拟机的过程中，从上述云服务器的存储块中以随机方

式选择在存储空间不连续的存储块组成上述虚拟机的存储空间，将选择的存储块与上述虚拟机的对应关系保存在可信的存储空间内，上述可信的存储空间具有允许上述虚拟机获取上述对应关系以及允许上述云服务器删除和修改上述对应关系，并且拒绝上述云服务器、上述终端设备以及其他任意设备的其他操作的功能；记录选择的存储块为已分配的存储块，在新创建其他虚拟机时不再次分配记录为已分配的存储块；为上述虚拟机分配共享存储空间，在上述共享存储空间中存储有上述虚拟机启动和运行所必要的驱动程序以及操作系统；为上述虚拟机配置针对上述云计算服务的具体内容的服务参数；

[0055] 上述云服务器在确定上述虚拟机存在安全风险后，删除上述可信的存储空间内保存的上述选择的存储块与上述虚拟机的对应关系。

[0056] 虚拟机(Virtual Machine)指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。因此虚拟机会像硬件设备一样具有存储空间：磁盘；本发明实施例中的存储块，是由供云服务器管理的磁盘分块得到的，这些存储块最初在存储空间(即：存储地址)上是连续的，以随机分配存储块的方式可以使最终以存储块组成虚拟机的磁盘后各存储块在存储空间上不连续，那么虚拟机内的磁盘被分配给另一虚拟机使用，并因此导致数据被恢复的可能性就会极低；另外，存储块与虚拟机的对应关系保存在可信的存储空间内，那么被窃取的可能性就会极低，进一步加强虚拟机本身数据的安全性。在共享存储空间中存储上述虚拟机启动和运行所必要的驱动程序以及操作系统，则可以一方面节省重复功能的虚拟机对存储空间的占用，另外，也方便云服务器批量地对具有同一云计算服务的具体内容的虚拟机进行统一管理。

[0057] 在本实施例中，结合虚拟机创建的过程中，存储空间的组成方式，以及在发现虚拟机存在安全风险后的对应关系删除，那么可以极大降低虚拟机内的数据被恢复的可能性，一方面可以防止数据内容被泄露，另一方面可以大大降低病毒软件本身被恢复的可能性。

[0058] 进一步地，上述终端设备显示一段随机生成的文字信息之前，方法还包括：

[0059] 上述终端设备显示请用户输入密码，且密码需要具有两种或者两种以上的密码类型的提示信息；接收上述用户输入的密码，若上述用户输入的密码少于两种，则提示上述用户输入的密码类型少于两种，在接收到确认指令后将接收到的密码存入数据库。

[0060] 本实施例中，提示用户输入两种以上密码类型的密码，可以诱导用户输入两种以上密码类型的密码，另一方面也降低用户设置一种密码类型的密码导致被猜测正确的可能性，即：变相增加猜测正确的难度。

[0061] 可选地，上述为上述虚拟机配置针对上述云计算服务的具体内容的服务参数包括：

[0062] 针对上述云计算服务的具体内容为上述虚拟机配置的向外部发送数据的权限和上述终端设备对上述虚拟机的操作权限。

[0063] 以上两个权限是针对安全服务所特别设计的权限，可以相应减少需要监测的服务参数的量，从而减少数据处理量，相应提高发现服务参数被修改的速度。

[0064] 可选地，上述云服务器在上述云服务器内创建针对上述云计算服务的具体内容的虚拟机包括：

[0065] 上述云服务器在确定上述云计算服务的具体内容与上述用户身份相适应后，创建与用户身份相适应的权限以及数据内容的虚拟机。

[0066] 本实施例提供了一个具体的应用场景，即：用户在云端创建自己私有的虚拟机。结合前述实施例，那么可以应用在大型公司，为员工创建专属的虚拟机，从而实现异地办公更方便，并且员工的专属虚拟机相互独立且不会相互感染病毒。

[0067] 进一步地，上述删除上述可信的存储空间内保存的上述选择的存储块与上述虚拟机的对应关系之后，上述方法还包括：

[0068] 将上述选择的存储块记录为未分配的存储块，且不删除上述选择的存储块内存储的数据内容；在有需求创建新的虚拟机时，从未分配的存储块内以随机方式选择在存储空间不连续的存储块组成待创建的新的虚拟机的存储空间。

[0069] 在本实施例中，由于存储块是随机分配的，虚拟机内的数据被拆分过，因此被恢复的可能性极低，那么在删除虚拟机的时候，可以不必删除这些数据提高磁盘的寿命。

[0070] 可选地，在上述共享存储空间中存储的上述虚拟机启动和运行所必要的驱动程序以及操作系统安装于沙箱内，上述沙箱具有输入接口以及输出接口；上述输入接口具有过滤对上述共享存储空间中存储的任意数据进行修改的指令的过滤功能。

[0071] 基于共享存储空间内存储的数据内容的特性，首先需要保证其安全性，另外数据内容有一定的数据输入输出需求，因此提供了进行过安全设定的接口来穿透沙箱；一方面可以利用沙箱所具有的安全控制功能，另一方面又可以实现必要的数据通讯功能，第三方面还可以共享这部分数据内容节省存储空间。

[0072] 本发明实施例还提供了一种云计算网络系统，如图2所示，包括：终端设备和云服务器；

[0073] 其中，上述终端设备，用于显示一段随机生成的文字信息并提示上述终端设备的当前的用户读上述文字信息；通过音频采集设备采集上述用户读上述文字信息的音频数据，对上述音频数据进行特征提取得到语音特征；从数据库中查找与上述语音特征匹配的用户身份信息，并确定上述用户身份信息在上述数据库中保存的密码所包含的密码类型；上述密码类型的组合包含：数字、字母大写、字母小写、数学符号、标点符号中的至少一项；在上述终端设备中显示提示信息，提示上述用户输入上述用户设置的密码的密码类型，并显示至少三个且种类大于上述数据库中保存的密码所包含的密码类型两倍的密码类型供选择；接收上述用户从显示的密码类型中选择的密码类型，若上述用户从显示的密码类型中选择的密码类型与上述数据库中保存的密码所包含的密码类型相同，则确定上述用户为上述用户身份信息所对应的用户身份；向上述云服务器发送服务请求，上述服务请求内携带上述用户身份的信息且指定了云计算服务的具体内容；

[0074] 上述云服务器，用于在上述云服务器内创建针对上述云计算服务的具体内容的虚拟机；为上述虚拟机配置针对上述云计算服务的具体内容的服务参数；上述云服务器内包含安全运行环境，在上述安全运行环境下的程序在运行过程不接受外部程序的请求导致的中断以及数据修改；在上述安全运行环境下运行监测程序对上述服务参数进行监测，确定上述虚拟机在运行过程中上述服务参数是否有被修改，若有并且不是上述终端设备发送的新的服务请求导致的修改，则确定上述虚拟机存在安全风险。

[0075] 进一步地，上述云服务器，还用于在创建上述虚拟机的过程中，从上述云服务器的存储块中以随机方式选择在存储空间不连续的存储块组成上述虚拟机的存储空间，将选择的存储块与上述虚拟机的对应关系保存在可信的存储空间内，上述可信的存储空间具有允

许上述虚拟机获取上述对应关系以及允许上述云服务器删除和修改上述对应关系，并且拒绝上述云服务器、上述终端设备以及其他任意设备的其他操作的功能；记录选择的存储块为已分配的存储块，在新创建其他虚拟机时不再次分配记录为已分配的存储块；为上述虚拟机分配共享存储空间，在上述共享存储空间中存储有上述虚拟机启动和运行所必要的驱动程序以及操作系统；为上述虚拟机配置针对上述云计算服务的具体内容的服务参数；在确定上述虚拟机存在安全风险后，删除上述可信的存储空间内保存的上述选择的存储块与上述虚拟机的对应关系。

[0076] 进一步地，上述终端设备，还用于显示一段随机生成的文字信息之前，显示请用户输入密码，且密码需要具有两种或者两种以上的密码类型的提示信息；接收上述用户输入的密码，若上述用户输入的密码少于两种，则提示上述用户输入的密码类型少于两种，在接收到确认指令后将接收到的密码存入数据库；

[0077] 上述云服务器，用于为上述虚拟机配置针对上述云计算服务的具体内容的服务参数包括：具体用于针对上述云计算服务的具体内容为上述虚拟机配置的向外部发送数据的权限和上述终端设备对上述虚拟机的操作权限；

[0078] 上述云服务器，用于在上述云服务器内创建针对上述云计算服务的具体内容的虚拟机包括：具体用于在确定上述云计算服务的具体内容与上述用户身份相适应后，创建与用户身份相适应的权限以及数据内容的虚拟机；

[0079] 上述云服务器，还用于上述删除上述可信的存储空间内保存的上述选择的存储块与上述虚拟机的对应关系之后，将上述选择的存储块记录为未分配的存储块，且不删除上述选择的存储块内存储的数据内容；在有需求创建新的虚拟机时，从未分配的存储块内以随机方式选择在存储空间不连续的存储块组成待创建的新的虚拟机的存储空间；

[0080] 在上述共享存储空间中存储的上述虚拟机启动和运行所必要的驱动程序以及操作系统安装于沙箱内，上述沙箱具有输入接口以及输出接口；上述输入接口具有过滤对上述共享存储空间中存储的任意数据进行修改的指令的过滤功能。

[0081] 本领域普通技术人员可以理解实现上述各方法实施例中的全部或部分步骤是可以通过程序来指令相关的硬件完成，相应的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0082] 以上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实施例揭露的技术范围内，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该以权利要求的保护范围为准。

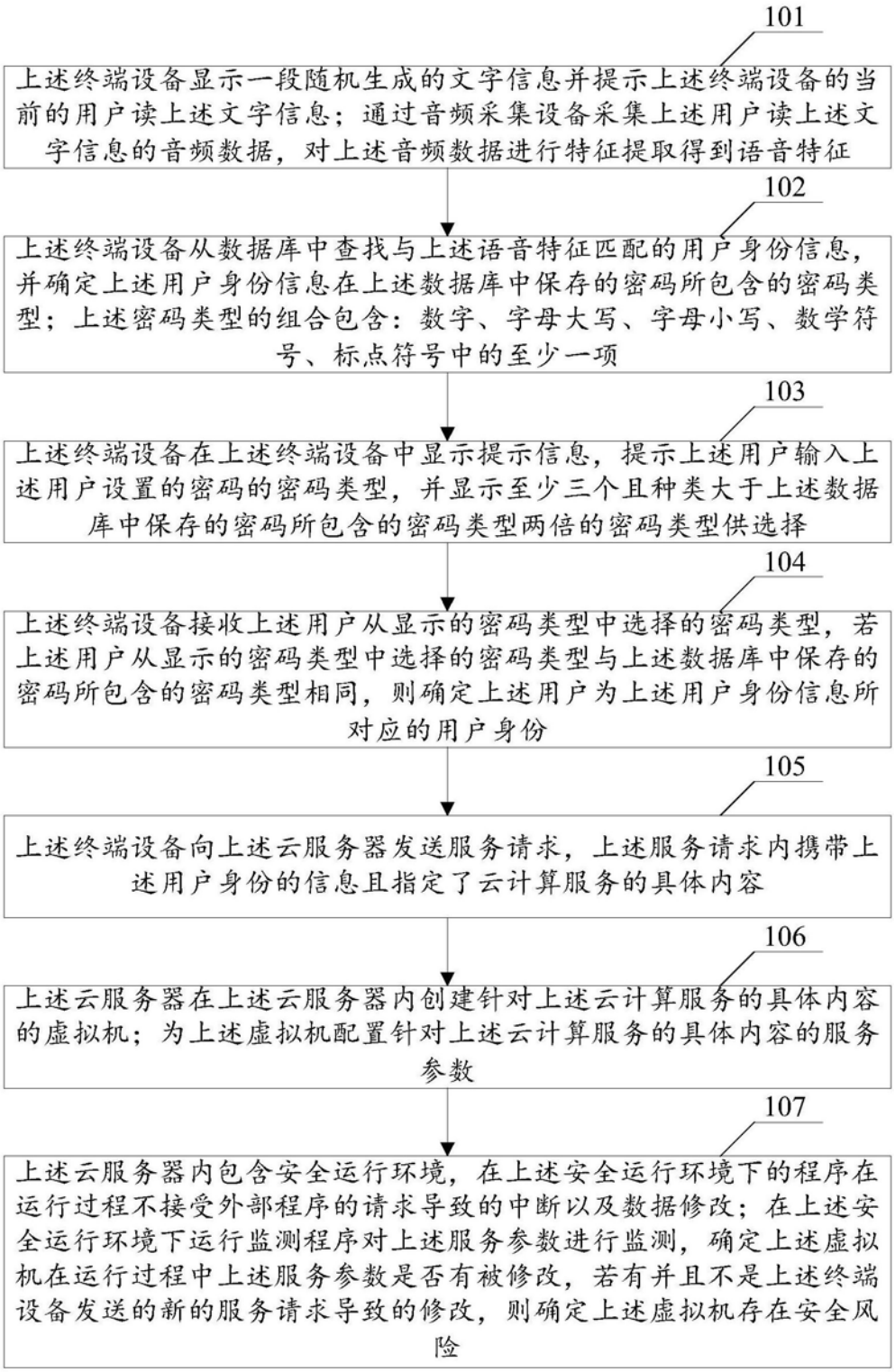

101
上述终端设备显示一段随机生成的文字信息并提示上述终端设备的当前的用户读上述文字信息；通过音频采集设备采集上述用户读上述文字信息的音频数据，对上述音频数据进行特征提取得到语音特征
102
上述终端设备从数据库中查找与上述语音特征匹配的用户身份信息，并确定上述用户身份信息在上述数据库中保存的密码所包含的密码类型；上述密码类型的组合包含：数字、字母大写、字母小写、数学符号、标点符号中的至少一项
103
上述终端设备在上述终端设备中显示提示信息，提示上述用户输入上述用户设置的密码的密码类型，并显示至少三个且种类大于上述数据库中保存的密码所包含的密码类型两倍的密码类型供选择
104
上述终端设备接收上述用户从显示的密码类型中选择的密码类型，若上述用户从显示的密码类型中选择的密码类型与上述数据库中保存的密码所包含的密码类型相同，则确定上述用户为上述用户身份信息所对应的用户身份
105
上述终端设备向上述云服务器发送服务请求，上述服务请求内携带上述用户身份的信息且指定了云计算服务的具体内容
106
上述云服务器在上述云服务器内创建针对上述云计算服务的具体内容的虚拟机；为上述虚拟机配置针对上述云计算服务的具体内容的服务参数
107
上述云服务器内包含安全运行环境，在上述安全运行环境下的程序在运行过程不接受外部程序的请求导致的中断以及数据修改；在上述安全运行环境下运行监测程序对上述服务参数进行监测，确定上述虚拟机在运行过程中上述服务参数是否有被修改，若有并且不是上述终端设备发送的新的服务请求导致的修改，则确定上述虚拟机存在安全风险

图1

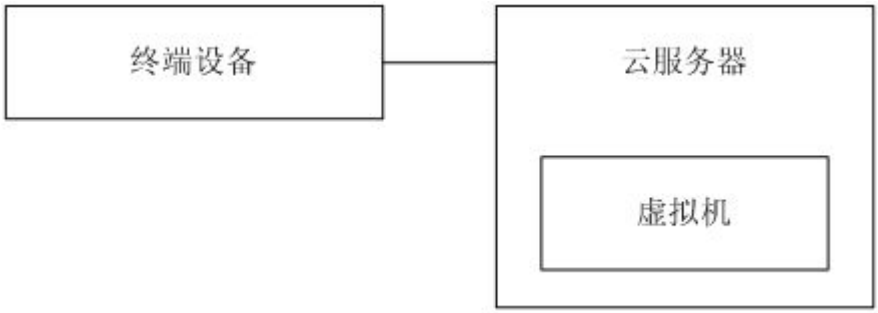


图2