(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 107070881 B
(45)授权公告日 2020.11.27

(21)申请号 201710091734.9

(22)申请日 2017.02.20

(65)同一申请的已公布的文献号
申请公布号 CN 107070881 A

(43)申请公布日 2017.08.18

(73)专利权人 北京古盘创世科技发展有限公司
地址 100000 北京市海淀区上地十街1号院5号楼9层901室

(72)发明人 张海鹰 周海燕 蔺旭东

(74)专利代理机构 北京超凡志成知识产权代理事务所(普通合伙) 11371
代理人 朱文杰

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 102236766 A,2011.11.09
CN 102365839 A,2012.02.29
CN 101174942 A,2008.05.07
CN 102647273 A,2012.08.22
CN 106301774 A,2017.01.04
CN 102487503 A,2012.06.06
US 2006126832 A1,2006.06.15
US 2008263363 A1,2008.10.23
王于丁."云计算访问控制技术研究综述".《软件学报》.2015,

审查员 高凯

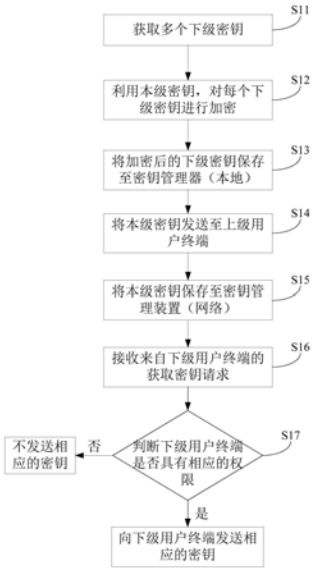
权利要求书2页 说明书9页 附图7页

(54)发明名称

密钥管理方法、系统及用户终端

(57)摘要

本发明提供了一种密钥管理方法、系统及用户终端,涉及信息安全技术领域,包括获取多个下级密钥;利用本级密钥,对每个下级密钥进行加密;将加密后的下级密钥保存至密钥管理器。另外,还可以将本级密钥也保存至密钥管理器。本发明通过利用本级密钥对下级密钥加密并存储的方法,解决了现有密钥保管方式存在安全性低的问题。



CN 107070881 B

1.一种密钥管理方法,其特征在于,所述方法适用于多级用户终端,每个用户终端包括用于存放下级密钥的密钥管理器,多级用户终端至少包括本级终端和下级终端,所述本级终端为本级行政级别用户的终端,所述下级终端为从属于本级行政级别的下级行政级别用户的终端,所述方法应用于本级终端,包括:

当所述本级终端以及从属于本级终端的所有下级终端均处于登录状态时,获取所有从属于本级终端的所述下级终端的下级密钥;

利用本级终端的本级密钥,对每个所述从属于所述本级终端的下级终端的下级密钥进行加密;

将加密后的下级密钥保存至本级终端的密钥管理器,其中所述密钥管理器为本地存储器。

2.根据权利要求1所述的方法,其特征在于,还包括:

将本级密钥保存至所述本级终端的密钥管理器。

3.根据权利要求1或2所述的方法,其特征在于,所述密钥管理器设置有禁止网络读取权限。

4.根据权利要求1所述的方法,其特征在于,还包括:

将本级密钥发送至上级终端。

5.根据权利要求1所述的方法,其特征在于,还包括:

将本级密钥保存至密钥管理装置。

6.根据权利要求5所述的方法,其特征在于,所述将本级密钥保存至密钥管理装置,具体为:

按一定拆分规则,将所述本级密钥拆分为至少两个密钥碎片;

将所述至少两个密钥碎片,分别保存在至少两个密钥管理装置中。

7.根据权利要求1所述的方法,其特征在于,还包括:

接收来自下级终端的获取密钥请求;

判断所述下级终端是否具有相应的权限;

如果所述下级终端具有相应的权限,则向所述下级终端发送相应的密钥;

如果所述下级终端不具有相应的权限,则不发送相应的密钥。

8.一种用户终端,其特征在于,所述用户终端包括用于存放下级密钥的密钥管理器,所述用户终端至少包括本级终端和下级终端,所述本级终端为本级行政级别用户的终端,所述下级终端为从属于本级行政级别的下级行政级别用户的终端,所述用户终端为本级终端,包括:

获取模块,用于当所述本级终端以及从属于本级终端的所有下级终端均处于登录状态时,获取所有从属于本级终端的所述下级终端的下级密钥;

加密模块,用于利用本级终端的本级密钥,对每个所述下级终端的下级密钥进行加密;

通讯模块,用于将加密后的下级终端的下级密钥保存至本级终端的密钥管理器,其中所述密钥管理器为本地存储器。

9.根据权利要求8所述的用户终端,其特征在于,所述通讯模块还用于将本级密钥保存至所述本级终端的密钥管理器。

10.根据权利要求8或9所述的用户终端,其特征在于,所述密钥管理器设置有禁止网络

读取权限。

11.根据权利要求8所述的用户终端，其特征在于，还包括：

拆分模块，用于按一定拆分规则，将所述本级密钥拆分为至少两个密钥碎片；

所述通讯模块还用于，将所述至少两个密钥碎片，分别保存在至少两个密钥管理装置中。

12.根据权利要求8所述的用户终端，其特征在于，还包括：

收发模块，用于接收来自下级终端的获取密钥请求；

判断模块，用于判断所述下级终端是否具有相应的权限；

如果所述下级终端具有相应的权限，则由所述收发模块向所述下级终端发送相应的密钥；

如果所述下级终端不具有相应的权限，则不发送相应的密钥。

13.一种密钥管理系统，其特征在于，包括多个如权利要求8至12任一项所述的用户终端。

14.根据权利要求13所述的密钥管理系统，其特征在于，还包括多个密钥管理装置，每个所述密钥管理装置与一个或多个所述用户终端通讯连接。

密钥管理方法、系统及用户终端

技术领域

[0001] 本发明涉及信息安全技术领域，尤其是涉及一种密钥管理方法、系统及用户终端。

背景技术

[0002] 密钥，即密匙，一般范指生产、生活所应用到的各种加密技术，能够对各人资料、企业机密进行有效的监管，密钥管理就是指对密钥进行管理的行为，如加密、解密、破解等等。其主要表现于管理体制、管理协议和密钥的产生、分配、更换和注入等。

[0003] 公司各个层级的员工都自己拥有系统或者云端应用权限，相对应的每个员工都有自己的密钥，目前，每一级别的员工将密钥存储在自己的密钥保管系统。这种情况很容易受到攻击者的攻击，让攻击者轻易的从员工自己的密钥保管系统中获取员工的密钥，给公司造成不可挽回的损失。因此，现有密钥保管方式存在安全性低的问题。

发明内容

[0004] 有鉴于此，本发明的目的在于提供一种密钥管理方法、系统及用户终端，以解决了现有密钥保管方式存在安全性低的问题。

[0005] 第一方面，本发明实施例提供了一种密钥管理方法，该方法包括：

[0006] 获取多个下级密钥；

[0007] 利用本级密钥，对每个所述下级密钥进行加密；

[0008] 将加密后的下级密钥保存至密钥管理器。

[0009] 结合第一方面，本发明实施例提供了第一方面的第一种可能的实施方式，其中，所述密钥管理器设置有禁止网络读取权限。

[0010] 结合第一方面，本发明实施例提供了第一方面的第二种可能的实施方式，其中，该方法还包括：

[0011] 将本级密钥保存至所述密钥管理器。

[0012] 结合第一方面，本发明实施例提供了第一方面的第三种可能的实施方式，其中，该方法还包括：

[0013] 将本级密钥发送至上级用户终端。

[0014] 结合第一方面，本发明实施例提供了第一方面的第四种可能的实施方式，其中，该方法还包括：

[0015] 将本级密钥保存至密钥管理装置。

[0016] 结合第一方面的第四种可能的实施方式，本发明实施例提供了第一方面的第五种可能的实施方式，其中，所述将本级密钥保存至密钥管理装置，具体为：

[0017] 按一定拆分规则，将所述本级密钥拆分为至少两个密钥碎片；

[0018] 将所述至少两个密钥碎片，分别保存在至少两个密钥管理装置中。

[0019] 结合第一方面，本发明实施例提供了第一方面的第六种可能的实施方式，其中，该方法还包括：

[0020] 接收来自下级用户终端的获取密钥请求；

[0021] 判断所述下级用户终端是否具有相应的权限；

[0022] 如果所述下级用户终端具有相应的权限，则向所述下级用户终端发送相应的密钥；

[0023] 如果所述下级用户终端不具有相应的权限，则不发送相应的密钥。

[0024] 第二方面，本发明实施例还提供一种用户终端，包括：

[0025] 获取模块，用于获取多个下级密钥；

[0026] 加密模块，用于利用本级密钥，对每个所述下级密钥进行加密；

[0027] 通讯模块，用于将加密后的下级密钥保存至密钥管理器。

[0028] 结合第二方面，本发明实施例提供了第二方面的第一种可能的实施方式，其中，所述通讯模块还用于将本级密钥保存至所述密钥管理器。

[0029] 结合第二方面，本发明实施例提供了第二方面的第二种可能的实施方式，其中，所述密钥管理器设置有禁止网络读取权限。

[0030] 结合第二方面，本发明实施例提供了第二方面的第三种可能的实施方式，其中，该用户终端还包括：

[0031] 拆分模块，用于按一定拆分规则，将所述本级密钥拆分为至少两个密钥碎片；

[0032] 所述通讯模块还用于，将所述至少两个密钥碎片，分别保存在至少两个密钥管理装置中。

[0033] 结合第二方面，本发明实施例提供了第二方面的第四种可能的实施方式，其中，该用户终端还包括：

[0034] 收发模块，用于接收来自下级用户终端的获取密钥请求；

[0035] 判断模块，用于判断所述下级用户终端是否具有相应的权限；

[0036] 如果所述下级用户终端具有相应的权限，则由所述收发模块向所述下级用户终端发送相应的密钥；

[0037] 如果所述下级用户终端不具有相应的权限，则不发送相应的密钥。

[0038] 第三方面，本发明实施例还提供了一种密钥管理系统，该系统包括多个如第二方面所述的用户终端。

[0039] 结合第三方面，本发明实施例提供了第三方面的第一种可能的实施方式，其中，该系统还包括多个密钥管理装置，每个所述密钥管理装置与一个或多个所述用户终端通讯连接。

[0040] 本发明实施例带来了以下有益效果：本发明提供的一种密钥管理方法、系统及用户终端，包括获取多个下级密钥；利用本级密钥，对每个下级密钥进行加密；将加密后的下级密钥保存至密钥管理器。本发明通过利用本级密钥对下级密钥加密并对加密后的下级密钥进行存储的方法，使得攻击者只有攻击了本级密钥后，才可以取得下级密钥，解决了现有密钥保管方式存在安全性低的问题。

[0041] 本发明的其他特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

[0042] 为使本发明的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合

所附附图，作详细说明如下。

附图说明

[0043] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案，下面将对具体实施方式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，下面描述中的附图是本发明的一些实施方式，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0044] 图1为本发明实施例提供的密钥管理方法的流程示意图；

[0045] 图2为本发明实施例提供的二级用户终端情况的结示意图；

[0046] 图3为本发明实施例提供的三级用户终端情况的示意图；

[0047] 图4为本发明实施例提供的密钥云端存储的示意图；

[0048] 图5为本发明实施例中将本级密钥保存至密钥管理装置的第一种方式的流程示意图；

[0049] 图6为本发明实施例提供的密钥多云端存储的示意图；

[0050] 图7为本发明实施例提供的密钥拆分存储的示意图；

[0051] 图8为本发明实施例中将本级密钥保存至密钥管理装置的第二种方式的流程示意图；

[0052] 图9为本发明实施例提供的用户终端的结构示意图；

[0053] 图10为本发明实施例提供的密钥管理系统的结构示意图。

具体实施方式

[0054] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合附图对本发明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。

[0055] 目前，公司每一级别的员工将密钥存储在自己的密钥保管系统，这种密钥保管方式存在安全性低的问题。基于此，本发明实施例提供的一种密钥管理方法、系统及用户终端，可以通过利用本级密钥对下级密钥加密并存储的方法，解决了现有密钥保管方式存在安全性低的问题。

[0056] 为便于对本实施例进行理解，首先对本发明实施例所公开的一种密钥管理方法进行详细介绍。

[0057] 实施例一：

[0058] 图1示出了本发明实施例提供的密钥管理方法的流程示意图。如图1所示，该方法包括：

[0059] 步骤S11，获取多个下级密钥；

[0060] 步骤S12，利用本级密钥，对每个下级密钥进行加密；

[0061] 步骤S13，将加密后的下级密钥保存至密钥管理器。

[0062] 具体的，本发明实施例提供的方法适用于多级用户终端，按照行政级别，该多级用户终端可以为员工用户终端、部门经理用户终端以及总经理用户终端，以下简称员工端，部

门经理端以及总经理端。以图2和图3为例，图2示出了本发明实施例提供的二级用户终端情况的示意图，图3示出了本发明实施例提供的三级用户终端情况的示意图。

[0063] 如图2所示，部门经理1端作为本级终端，获取两个下级密钥即员工1端与员工2端的密钥，并利用部门经理1端的本级密钥，对员工1端与员工2端的密钥进行加密，并将加密后的两个下级密钥即员工1端与员工2的密钥保存至部门经理1端的密钥管理器，其中该密钥管理器为本地存储器。另外，部门经理1端还可以将本级密钥也保存至密钥管理器，从而本级密钥的进行保护。

[0064] 作为一个优选方案，该密钥管理器设置有禁止网络读取权限。也就是说，单纯通过网络访问密钥管理器的情况下，不能读取其中存储的密钥。而必须通过特定的本地操作，比如插入U盾、指纹解锁等操作，才能读取其中存储的密钥，并且也仅能以本地方式读取密钥。通过设置禁止网络读取权限，能够在用户终端受到网络攻击时，防止密钥管理器中的密钥被窃取，从而提高了密钥管理的安全性。

[0065] 如图3所示，部门经理2端作为本级终端的密钥存储方法与图2中部门经理1端作为本级终端的密钥存储方法相同，获取其对应的下级员工3端的密钥，应用本级密钥保存并存储在本级密钥管理器。当总经理端作为本级终端时，获取两个下级密钥即部门经理1端和部门经理2端的密钥，并利用本级终端即总经理端的的本级密钥，对部门经理1端和部门经理2端的密钥进行加密，将加密后的部门经理1端和部门经理2端的密钥保存至总经理端的密钥管理器。

[0066] 进一步的，依次类推得到四级或者更多级用户终端情况的密钥管理方法。

[0067] 综上所述，本发明提供了一种密钥管理方法，包括获取多个下级密钥；利用本级密钥，对每个下级密钥进行加密；将加密后的下级密钥保存至本地的密钥管理器。本发明通过利用本级密钥对下级密钥加密并存储的方法，解决了现有密钥保管方式存在安全性低的问题。

[0068] 进一步的，在一种实现方式中，为了增强保密效果，如图1所示，上述方法还包括以下步骤：

[0069] 步骤S14，将本级密钥发送至上级用户终端。

[0070] 具体的，以图2或者图3为例，员工1端和员工2端将本级密钥发送至部门经理1端，员工3端将其本级密钥发送至部门经理2端，部门经理1端利用本级密钥对员工1端和员工2端的密钥进行加密后，将其本级密钥发送至总经理端。部门经理2端利用本级密钥对员工3端的密钥进行加密后，将其本级密钥发送至总经理端。优选的，员工端的密钥可以在员工的上级即部门经理登录自己的系统或者云端时，通过该对应的部门经理端的密钥加密后，自动上传到该部门经理端对应的密钥管理器。当总经理登录云盘或者系统的时候，总经理的下级即多个部门经理的密钥，通过总经理的密钥加密后，自动上传到总经理端的密钥管理器。因此，只有当下级全部登录，下级的密钥才能逐级提交到上级。

[0071] 进一步的，考虑到本地存储容易受到攻击者的攻击，如图1所示，上述方法还包括以下步骤：

[0072] 步骤S15，将本级密钥保存至密钥管理装置。

[0073] 具体的，在一种实现方式中，如图4所示，总经理获得所有的密钥后将本级密钥保存至网络侧的密钥管理装置，部门经理得该部门员工所有的密钥后，也可以将本级密钥保

存至密钥管理装置，该密钥管理装置为云端存储器。

[0074] 进一步的，上述密钥管理装置可以为多个。上述将本级密钥保存至密钥管理装置，可以通过以下两种方式。

[0075] 如图5所示，第一种方式具体为：

[0076] 步骤S151，按一定拆分规则，将本级密钥拆分为至少两个密钥碎片。

[0077] 用户终端首先向云管理系统获取至少两个不同密钥管理装置的名称地址，或者用户终端(员工用户终端、部门经理用户终端或总经理用户终端)直接访问至少两个密钥管理装置，然后用户终端可以按照一定的拆分规则将一个完整的密钥进行切割拆分，分成至少两个部分，也就是切割成至少两个密钥碎片。

[0078] 步骤S152，将至少两个密钥碎片，分别保存在至少两个密钥管理装置中。

[0079] 本实施例中，按照密钥管理装置的名称地址将密钥碎片分别保存到至少两个不同的密钥管理装置中，在不同的密钥管理装置中存储，例如，将部分密钥存放到第一服务商的密钥管理装置，将另外一部分密钥存放到第二服务商的密钥管理装置。本步骤是要把密钥通过以上机制分存到不同的地方进行保存。

[0080] 密钥管理装置是一种专门用于管理密钥的网络系统，比普通的云存储器安全性更高。

[0081] S153：连接每个密钥管理装置，并通过每个密钥管理装置的身份认证。

[0082] 在使用密钥的时候，用户终端连接每个密钥管理装置，输入每个密钥管理装置的认证信息，通过每个密钥管理装置的身份认证。

[0083] S154：分别从每个密钥管理装置中获取每个密钥碎片。

[0084] 用户终端分别从相应密钥管理装置中获取到相应的密钥碎片，因此便能从多个密钥管理装置中获取全部的多个密钥碎片。

[0085] S155：根据拆分规则，将所获取的密钥碎片组合成密钥。

[0086] 在用户终端从每个密钥管理装置中获取到所有的密钥碎片后，根据步骤S151中的拆分规则，可将获取到的密钥碎片重新组合成完整的密钥。只有拿到全部的密钥碎片，才能获得完整的密钥，并利用密钥把秘钥管理装置中的数据解开。

[0087] 例如，当密钥为“10084567”时，可以将该密钥拆分为“1008”和“4567”，并分别存储于密钥管理装置1和密钥管理装置2中。这样，只有通过密钥管理装置1和密钥管理装置2的身份认证并获取到所有的碎片后，才可以获得整个密钥，增强了密钥存储的安全性。如图6所示，总经理获得所有的密钥后将本级密钥保存至密钥管理装置1和密钥管理装置2。

[0088] 如图7所示，公司各个行政级别用户终端的密钥均被拆分为多个碎片后，可以将一部分碎片可以存放在多个密钥管理装置中，而其它碎片如上述逐级上传的方式存储，即总经理需要下级全部登录获得一部分碎片后，然后再去访问多个密钥管理装置获取剩余其它碎片，最终得到所有的密钥，这样进一步增强了密钥存储的安全性。

[0089] 如图8所示，将本级密钥保存至密钥管理装置的第二种方式具体为：

[0090] 步骤S161，按一定拆分规则，将本级密钥拆分为至少两个密钥碎片。

[0091] 用户终端首先向云管理系统获取至少两个不同密钥管理装置的名称地址，或者用户终端(员工用户终端、部门经理用户终端或总经理用户终端)直接访问至少两个密钥管理装置，然后用户终端可以按照一定的拆分规则将一个完整的密钥进行切割拆分，分成至少

两个部分，也就是切割成至少两个密钥碎片。

[0092] 步骤S162，将至少两个密钥碎片，分别保存在至少两个密钥管理装置中。

[0093] 本实施例中，按照密钥管理装置的名称地址将密钥碎片分别保存到至少两个不同的密钥管理装置中，在不同的密钥管理装置中存储，例如，将部分密钥存放到第一服务商的密钥管理装置，将另外一部分密钥存放到第二服务商的密钥管理装置。本步骤是要把密钥通过以上机制分存到不同的地方进行保存。

[0094] 云存储器具体可以为专门用于管理密钥的网络系统，比普通的云存储器安全性更高。

[0095] S163：根据拆分规则，以及至少两个密钥管理装置的地址，生成拆分和分存记录信息。

[0096] 在用户终端按照既定的规则去拆分和分存的时候，自动记录该拆分和分存记录，然后根据该记录生成一个拆分和分存记录。

[0097] S164：将拆分和分存记录信息保存至云管理系统。

[0098] 具体的，用户终端记录步骤S161中的拆分规则，以及每个密钥碎片保存到的密钥管理装置的地址，生成拆分和分存记录，并将该拆分和分存记录保存至云管理系统中。

[0099] S165：连接云管理系统，并通过云管理系统的身份认证。

[0100] 在需要使用密钥的时候，首先取回拆分和分存记录，因此用户终端需要通过云管理系统的认证。

[0101] S166：从云管理系统获取拆分和分存记录信息。

[0102] 云管理系统向用户终端发送该拆分和分存记录，其中包括密钥碎片的拆分规则和每个密钥碎片的存放地址。

[0103] S167：根据拆分和分存记录信息，分别从每个密钥管理装置中获取每个密钥碎片，并将所获取的密钥碎片组合成密钥。

[0104] 因为拆分和分存记录信息中包含有密钥碎片的拆分规则，所以获取到全部密钥碎片之后，可根据该拆分规则将密钥碎片自动组合成完整的密钥，而用户无需再进行组合操作。

[0105] 需要说明的是，可以按行政级别认证所有密钥使用者(包括各个员工、部门经理、总经理)，所有密钥使用者登录后，将主动生成的密钥拆分后，主动存储在至少两个密钥管理装置，并由两个独立的管理员管理，两个独立密钥管理装置都具有独立的认证方式，该两个独立密钥管理装置可以是内部与内部的组合、内部与外部的组合以及外部与外部的组合。每个独立密钥管理装置具有认证功能，可以根据密钥使用者的身份以及被授权权限，按需分发拆分密钥，使用者得到密钥后，再进行组合然后使用。

[0106] 其中，密钥管理装置1和密钥管理装置2可以按照用户既定的组织架构，自动依照组织架构生成一半密钥分发给相应的密钥使用者，该相应的密钥使用者可以将通过密钥管理装置1和密钥管理装置2生成的密钥，再加密自己的数据信息。

[0107] 在上述两种方式中，通过对多个密钥管理装置进行访问后获取凑成一个完整的密钥，使密钥的保存以及获取都能更加安全。

[0108] 作为另一种实施方式，各个级别的密钥在逐级上传的同时，也可以向公司之外的一个密钥管理端(比如私有的公共平台)进行密钥上传，作为备份，以防止密钥在上传过程

中丢失造成的不便。例如，图7中的密钥管理装置1是公司内部的密钥管理端，密钥管理装置2是公司之外的密钥管理端。

[0109] 或者，各个行政级别的员工也可以同时把自己的密钥统一存到公司的两个管理员的终端，这样，公司内部同时有两个人来管理密钥，防止一人失误造成密钥的丢失或者被轻易攻击，从而给公司造成不必要的损失。

[0110] 进一步的，为了密钥安全的发送而不被泄露，如图1所示，上述方法还包括以下步骤：

[0111] 步骤S16，接收来自下级用户终端的获取密钥请求。

[0112] 步骤S17，判断下级用户终端是否具有相应的权限。

[0113] 如果下级用户终端具有相应的权限，则向下级用户终端发送相应的密钥；如果下级用户终端不具有相应的权限，则不发送相应的密钥。

[0114] 以图3为例，当员工1想访问员工2的用户终端，员工1需要员工2的密钥，则员工1需要向部门经理1提出申请，部门经理端接收到申请后，根据员工的行政级别，查询到员工1端具有相应的权限，则向该员工1端发送员工2端的密钥。如果员工1想访问员工3的用户终端，则需要先向部门经理1提出申请，部门经理端接收到申请后，根据员工的行政级别，查询到员工1端具有相应的权限，则将上述申请发送到总经理端，总经理端接收该申请后，向部门经理2端索要员工3端的密钥并发送至总经理端，总经理端将员工3端的密钥发送至部门经理1端，最终由部门经理1端将员工3的密钥发送至员工1端。

[0115] 通过上述逐级申请，逐级发送的方式实现各个行政级别用户终端的相互访问，并对各个用户终端所享有的权限进行验证，保证了各个用户终端相互访问的安全性。

[0116] 实施例二：

[0117] 图9示出了本发明实施例提供的用户终端的结构示意图，如图9所示，该用户终端包括：

[0118] 获取模块51，用于获取多个下级密钥。

[0119] 加密模块52，用于利用本级密钥，对每个下级密钥进行加密。

[0120] 通讯模块53，用于将加密后的下级密钥保存至密钥管理器。

[0121] 同样，以图2为例，部门经理1的用户终端作为本级终端，获取两个下级密钥即员工1用户终端与员工2用户终端的密钥，并利用部门经理1用户终端的本级密钥，对员工1用户终端与员工2用户终端的密钥进行加密，并将加密后的两个下级密钥即员工1端与员工2的密钥保存至部门经理1用户终端的密钥管理器，其中该密钥管理器为本地存储器。另外，通讯模块53还用于将本级密钥保存至密钥管理器，从而本级密钥的进行保护。

[0122] 作为一个优选方案，该密钥管理器设置有禁止网络读取权限。也就是说，单纯通过网络访问密钥管理器的情况下，不能读取其中存储的密钥。而必须通过特定的本地操作，比如插入U盾、指纹解锁等操作，才能读取其中存储的密钥，并且也仅能以本地方式读取密钥。通过设置禁止网络读取权限，能够在用户终端受到网络攻击时，防止密钥管理器中的密钥被窃取，从而提高了密钥管理的安全性。

[0123] 进一步的，为了增强保密效果，如图7所示，上述用户终端还包括：发送模块54，用于将本级密钥发送至上级用户终端。只有当下级全部登录，下级的密钥才能逐级提交到上级。

[0124] 进一步的，考虑到本地存储容易受到攻击者的攻击，如图9所示，上述用户终端还包括：云端存储模块55，用于将本级密钥保存至网络侧的密钥管理装置。其中，该密钥管理装置为云端存储器。

[0125] 进一步的，上述密钥管理装置可以为多个。上述用户终端还包括：拆分模块56，用于按一定拆分规则，将本级密钥拆分为至少两个密钥碎片；通讯模块53还用于将至少两个密钥碎片，分别保存在至少两个密钥管理装置中。

[0126] 例如，当密钥为“100845678”时，可以将该密钥拆分为“100”、“845”及“678”，并分别存储于密钥管理装置1、密钥管理装置2和密钥管理装置3中。这样，只有获取到三个密钥管理装置中存储的所有的碎片后，才可以获得整个密钥，增强了密钥存储的安全性。

[0127] 用户终端还包括第一认证模块以及第一组合模块。第一认证模块用于连接每个密钥管理装置，并通过每个密钥管理装置的身份认证，在使用密钥的时候，第一认证模块能够连接每个密钥管理装置，通过用户输入的每个密钥管理装置的认证信息进行身份认证。

[0128] 通讯模块53还用于分别从每个密钥管理装置中获取每个密钥碎片，通讯模块53能够分别从相应的密钥管理装置中获取到相应的密钥碎片，因此便能从多个密钥管理装置中获取全部的多个密钥碎片。

[0129] 第一组合模块用于根据拆分规则，将所获取的密钥碎片组合成密钥。在通讯模块53从每个密钥管理装置中获取到所有的密钥碎片后，第一组合模块能够根据拆分模块56的拆分规则，将获取到的密钥碎片重新组合成完整的密钥，只有拿到全部的密钥碎片，才能获得完整的密钥，并利用密钥把密钥管理装置中的数据解开。

[0130] 本发明实施例中的用户终端还包括：信息生成模块、第二认证模块以及第二组合模块。信息生成模块用于根据拆分规则，以及至少两个密钥管理装置的地址，生成拆分和分存记录信息。在拆分模块按照既定的规则去拆分和分存的时候，信息生成模块能够自动记录该拆分和分存记录，根据该记录生成一个拆分和分存记录。

[0131] 通讯模块53还用于将拆分和分存记录信息保存至云管理系统。

[0132] 第二认证模块用于连接云管理系统，并通过云管理系统的身份认证。在使用密钥的时候，第二认证模块能够通过用户输入的认证信息进行身份认证，取回拆分和分存记录。

[0133] 通讯模块53还用于从云管理系统获取拆分和分存记录信息，以及根据拆分和分存记录信息，分别从每个密钥管理装置中获取每个密钥碎片；

[0134] 第二组合模块用于将所获取的密钥碎片组合成密钥，在获取到全部密钥碎片之后，第二组合模块可以根据拆分规则将密钥碎片自动组合成完整的密钥。

[0135] 进一步的，为了保证各个用户终端相互访问的安全性，密钥可以安全的发送而不被泄露，上述用户终端还包括：收发模块57，用于接收来自下级用户终端的获取密钥请求；判断模块58，用于判断下级用户终端是否具有相应的权限；如果所下级用户终端具有相应的权限，则由收发模块向所述下级用户终端发送相应的密钥；如果下级用户终端不具有相应的权限，则不发送相应的密钥。

[0136] 本发明实施例通过上述逐级申请，逐级发送的方式实现各个行政级别用户终端的相互访问，并对各个用户终端所享有的权限进行验证，保证了各个用户终端相互访问的安全性。

[0137] 本发明实施例提供的用户终端，与上述实施例提供的密钥管理方法具有相同的技

术特征，所以也能解决相同的技术问题，达到相同的技术效果。

[0138] 实施例三：

[0139] 本发明实施例提供了一种密钥管理系统，该系统包括上述实施例二中的用户终端。

[0140] 进一步的，该系统还包括多个密钥管理装置，其中，每个密钥管理装置与一个或多个用户终端通讯连接。

[0141] 具体的，如图10所示(以三级用户终端为例)，多个员工用户终端与多个部门经理用户终端、多个密钥管理装置通讯连接，多个部门经理用户终端与多个密钥管理装置、总经理用户终端通讯连接。

[0142] 进一步的，密钥管理系统还包括冗余备份存储器，用于对任一密钥管理装置中保存的密钥碎片进行备份，以及用于对拆分和分存记录信息进行备份。

[0143] 在另一种实施方式中，当密钥分存在密钥管理装置中之后，单个密钥管理装置会自动向另一个密钥管理装置空间进行冗余备份，其中，备份的是一个密钥碎片，从而实现当一个密钥管理装置存在问题时，不会出现密钥丢失的情况，保证多个密钥管理装置可以互为备份。

[0144] 本发明提供了一种密钥管理系统，包括多个用户终端和多个密钥管理装置，根据公司的行政级别，每个行政级别对应的用户终端获取多个下级密钥，利用本级密钥对每个下级密钥进行加密，并将加密后的下级密钥保存至本地的密钥管理器。本发明的系统通过利用本级密钥对下级密钥加密并存储的方法，解决了现有密钥保管方式存在安全性低的问题。

[0145] 本发明实施例所提供的密钥管理方法、系统及用户终端的计算机程序产品，包括存储了程序代码的计算机可读存储介质，所述程序代码包括的指令可用于执行前面方法实施例中所述的方法，具体实现可参见方法实施例，在此不再赘述。

[0146] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统和装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0147] 所述功能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，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0148] 最后应说明的是：以上所述实施例，仅为本发明的具体实施方式，用以说明本发明的技术方案，而非对其限制，本发明的保护范围并不局限于此，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：任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化，或者对其中部分技术特征进行等同替换；而这些修改、变化或者替换，并不使相应技术方案的本质脱离本发明实施例技术方案的精神和范围，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所述以权利要求的保护范围为准。

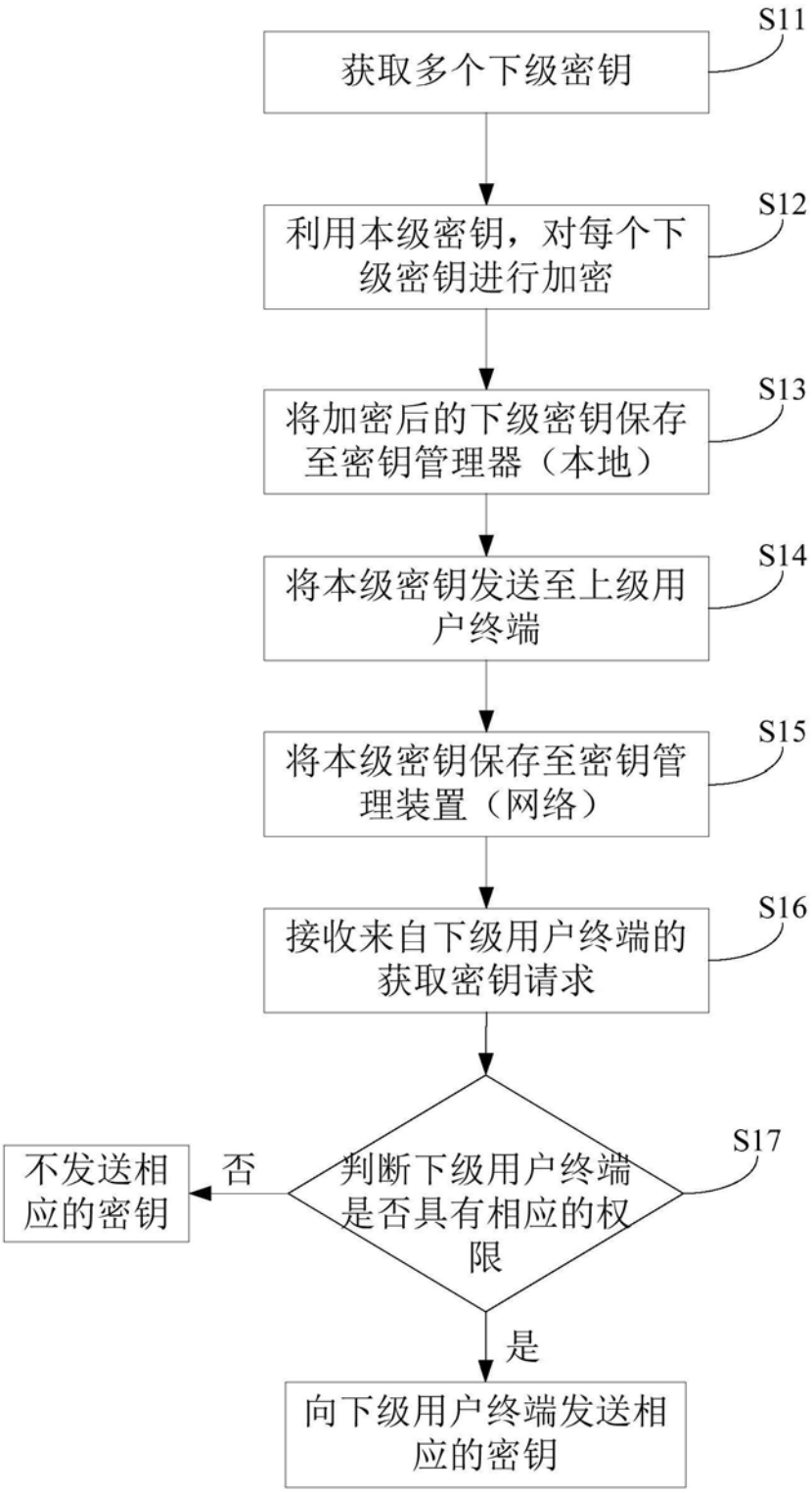

S11
获取多个下级密钥
S12
利用本级密钥，对每个下级密钥进行加密
S13
将加密后的下级密钥保存至密钥管理器（本地）
S14
将本级密钥发送至上级用户终端
S15
将本级密钥保存至密钥管理装置（网络）
S16
接收来自下级用户终端的获取密钥请求
S17
判断下级用户终端是否具有相应的权限
否
不发送相应的密钥
是
向下级用户终端发送相应的密钥

图1

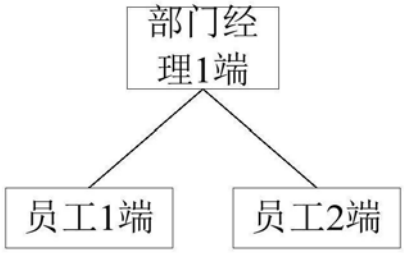

部门经理1端
员工1端
员工2端

图2

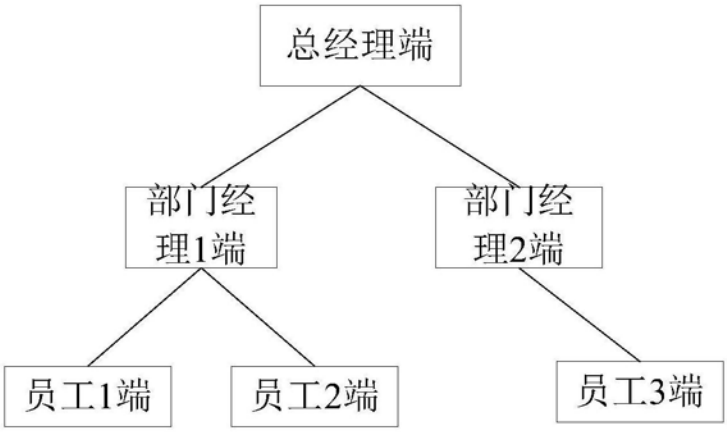

总经理端
部门经理1端
部门经理2端
员工1端
员工2端
员工3端

图3

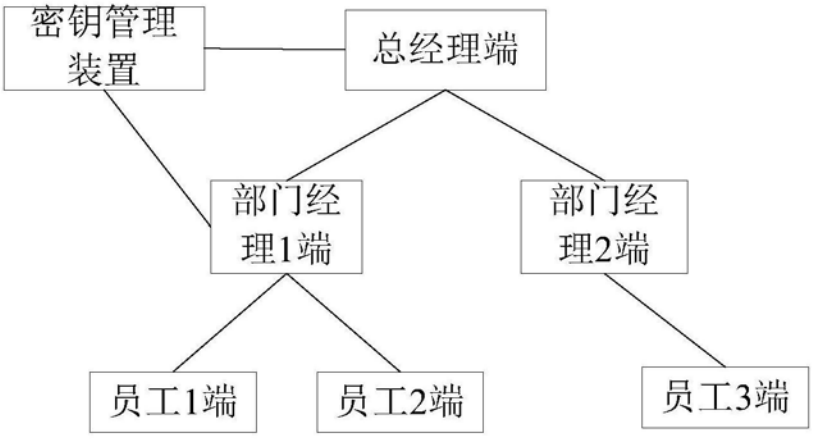

密钥管理装置
总经理端
部门经理1端
部门经理2端
员工1端
员工2端
员工3端

图4

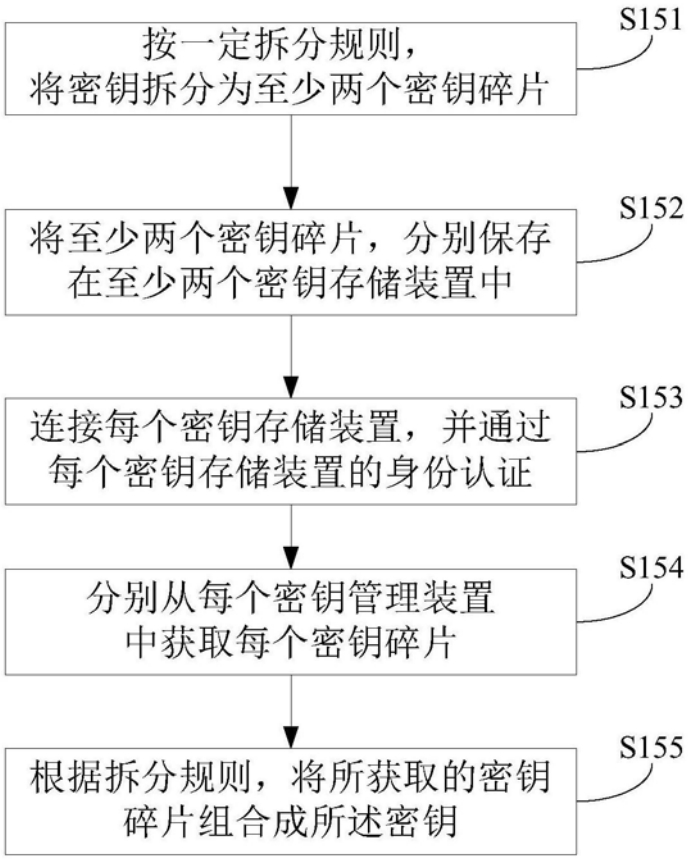

按一定拆分规则，
将密钥拆分为至少两个密钥碎片
S151
将至少两个密钥碎片，分别保存
在至少两个密钥存储装置中
S152
连接每个密钥存储装置，并通过
每个密钥存储装置的身份认证
S153
分别从每个密钥管理装置
中获取每个密钥碎片
S154
根据拆分规则，将所获取的密钥
碎片组合成所述密钥
S155

图5

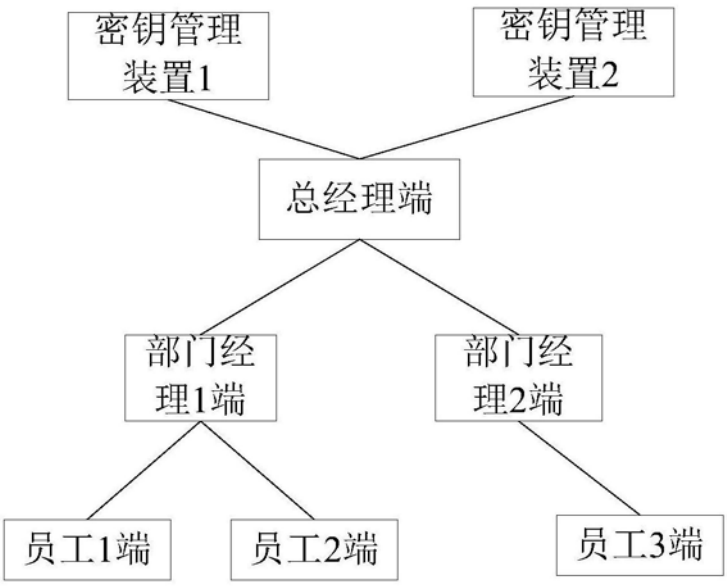

密钥管理
装置1
密钥管理
装置2
总经理端
部门经
理1端
部门经
理2端
员工1端
员工2端
员工3端

图6

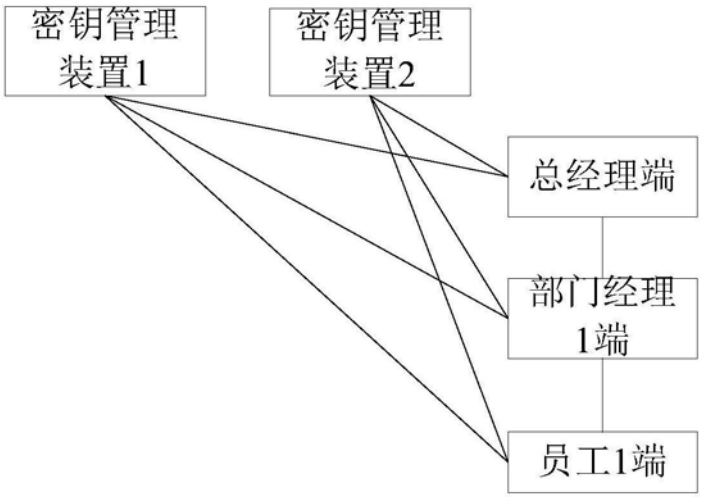


图7

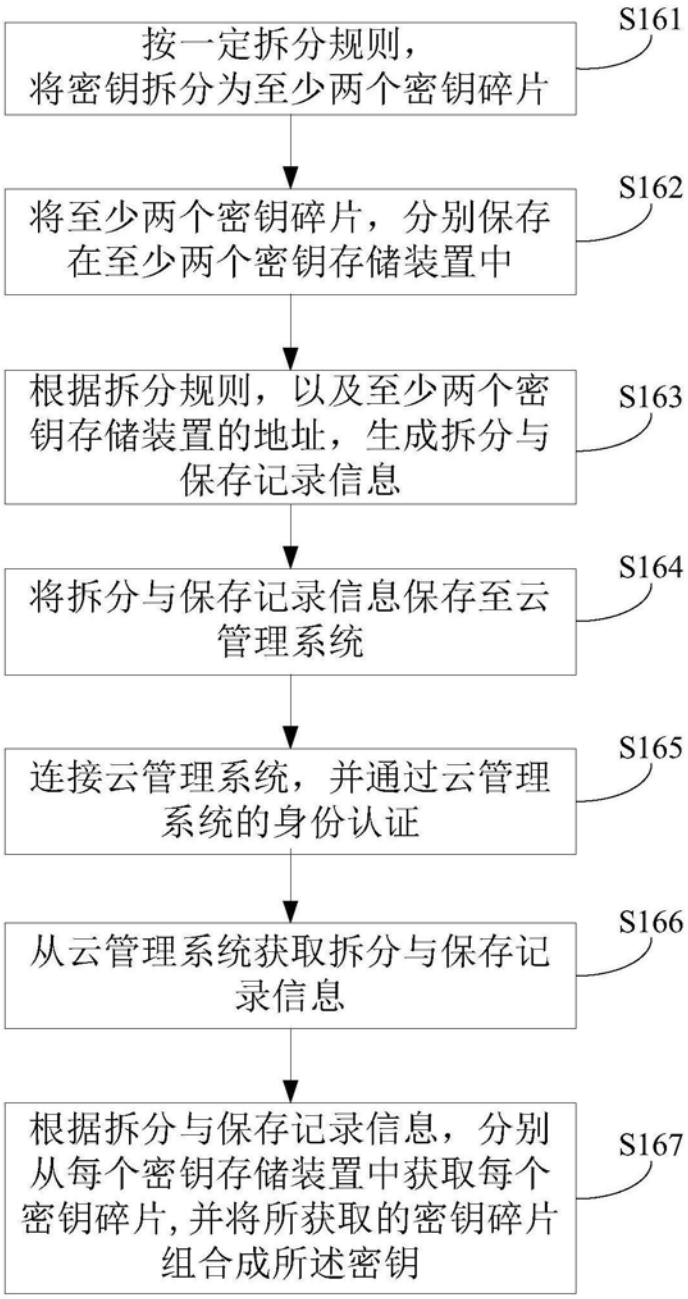

S161
按一定拆分规则，
将密钥拆分为至少两个密钥碎片
S162
将至少两个密钥碎片，分别保存
在至少两个密钥存储装置中
S163
根据拆分规则，以及至少两个密
钥存储装置的地址，生成拆分与
保存记录信息
S164
将拆分与保存记录信息保存至云
管理系统
S165
连接云管理系统，并通过云管理
系统的身份认证
S166
从云管理系统获取拆分与保存记
录信息
S167
根据拆分与保存记录信息，分别
从每个密钥存储装置中获取每个
密钥碎片，并将所获取的密钥碎片
组合成所述密钥

图8

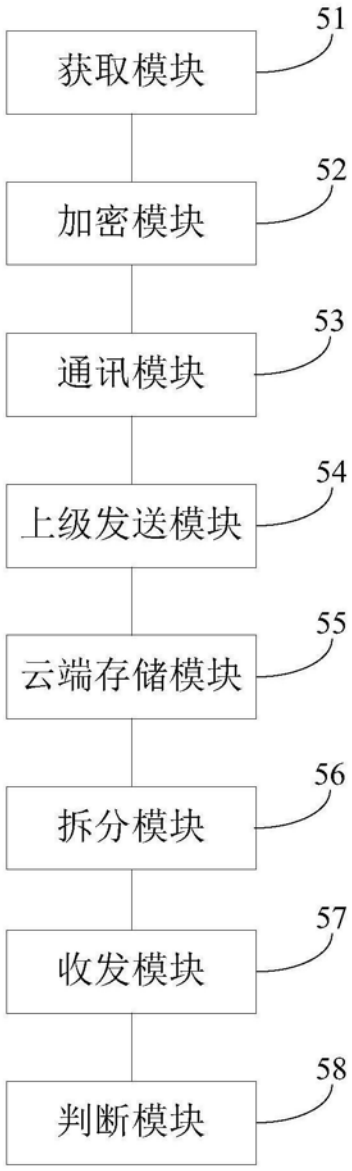

51
获取模块
52
加密模块
53
通讯模块
54
上级发送模块
55
云端存储模块
56
拆分模块
57
收发模块
58
判断模块

图9

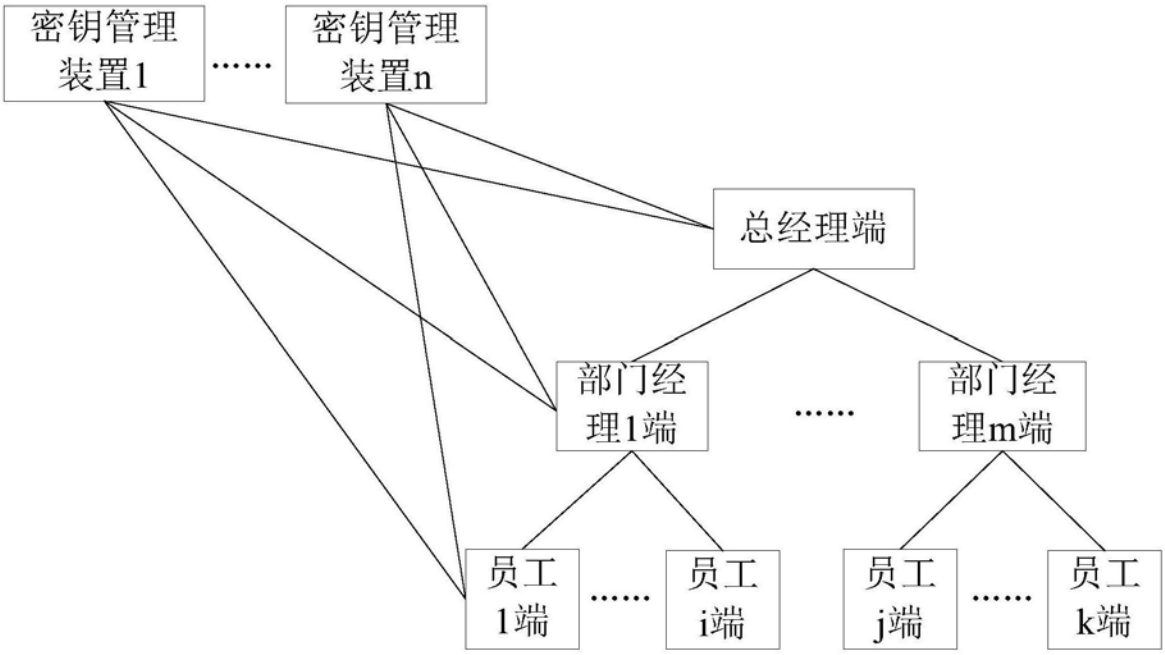


图10