



(12) 发明专利

(10) 授权公告号 CN 113608933 B

(45) 授权公告日 2022. 02. 08

(21) 申请号 202111178820.6

(22) 申请日 2021.10.11

(65) 同一申请的已公布的文献号  
申请公布号 CN 113608933 A

(43) 申请公布日 2021.11.05

(73) 专利权人 环球数科集团有限公司  
地址 518063 广东省深圳市南山区粤海街  
道高新南九道10号深圳湾科技生态园  
10栋B座17层01-03号

(72) 发明人 张卫平 丁焯 张浩宇

(74) 专利代理机构 北京清控智云知识产权代理  
事务所(特殊普通合伙)  
11919

代理人 马肃

(51) Int.Cl.

G06F 11/14 (2006.01)

G06F 16/27 (2019.01)

G06F 16/953 (2019.01)

G06F 21/60 (2013.01)

G06Q 30/06 (2012.01)

(56) 对比文件

CN 113132362 A, 2021.07.16

CN 105740717 A, 2016.07.06

US 2020125537 A1, 2020.04.23

CN 104683161 A, 2015.06.03

CN 102833346 A, 2012.12.19

审查员 马丹凤

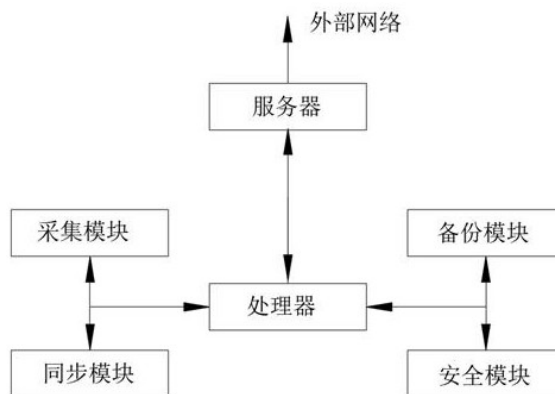
权利要求书3页 说明书9页 附图2页

(54) 发明名称

一种面向公有云租户业务敏感数据的分布式备份同步系统

(57) 摘要

本发明提供了一种面向公有云租户业务敏感数据的分布式备份同步系统,包括采集模块、安全模块、备份模块、同步模块、核验模块和处理器,处理器分别与采集模块、安全模块、备份模块、同步模块和核验模块控制连接,其中,采集模块用于对租户的数据进行采集,以实现租户的业务以及身份ID进行采集;核验模块用于对租户身份和访问的移动终端进行核验;安全模块用于对租户的数据进行防护;备份模块用于对各个租户的数据进行备份;同步模块在接收经过核验模块的核验过的访问请求时,触发对租户数据的同步。本发明通过对所述租户的数据进行备份操作、以及对备份的数据进行标记,使得所有的操作均能被追溯,以确保整个数据的安全。



1. 一种面向公有云租户业务敏感数据的分布式备份同步系统,其特征在于,该系统包括采集模块、安全模块、备份模块、同步模块、核验模块和处理器,

所述处理器分别与所述采集模块、所述安全模块、所述备份模块、同步模块和核验模块控制连接,其中,所述采集模块用于对租户的数据进行采集,以实现与所述租户的业务以及身份ID进行采集;所述核验模块用于对所述租户身份和访问的移动终端进行核验;所述安全模块用于对所述租户的数据进行防护,以配合所述备份模块对租户的数据进行备份;所述备份模块用于对各个租户的数据进行备份,并存储在所述租户的个人数据库中;

所述同步模块在接收经过核验模块的核验过的访问请求时,触发对所述租户数据的同步;

所述采集模块包括联网单元和数据库,所述联网单元用于与所述租户的移动终端进行联网,组建传输网络,其中,所述传输网络在连接前通过所述核验模块对各个租户对应的移动终端的授权许可进行核验;所述数据库用于对所述联网单元采集的各个租户信息进行存储,并反馈存储序列号;

所述采集模块还包括管理单元,所述管理单元利用租户提供的身份信息生成相应的通行码,当使用所述通行码则需要访问的位置进行核验,若通行码符合通行条件,则对所需业务进行访问;

所述管理单元还包括通行码生成器,所述通行码生成器用于自动生成通行码以及备份ID,所述通行码生成器通过下式公式生成通行码 $pass_i$ :

$$Pass_i = \frac{(z_i - d_i)}{w_i} \left( \frac{task_i}{u_i} + k_i \right)$$

其中, $u_i$ 为租户*i*访问总次数; $task_i$ 为租户*i*当天访问的次数; $z_i$ 为当前时间; $d_i$ 为截止时间; $w_i$ 为租户*i*访问时触发的等待时间; $k_i$ 为租户*i*上一次访问的通行码,

$$k_i = \sum_{v=1}^N series, \quad 0 \leq series \leq 9$$

其中,series为租户的身份ID;且当生成新的通行码后,对通行码进行更新;

所述通行码生成器通过下式生成备份ID:

$$Backup_i = ag_i + bk_i$$

其中,Backup<sub>*i*</sub>为备份ID;a和b为系数,其值跟租户发布的项目或者需求有关; $g_i$ 为用户上传的数据总存储量; $k_i$ 为上一次访问的通行码;

所述管理单元在响应所述租户的访问请求前,需要利用所述通行码生成器生成新的通行码和备份ID,且新下发所述通行码和备份ID与原来的通行码和备份ID需不一致才有效,使访问请求的记录可被追溯;

所述核验模块包括核验单元和授权单元,所述核验单元用于对所述租户的身份进行核验,若并未进行注册,则向所述租户反馈所述未进行注册的结果;

所述核验单元包括注册子单元和ID创建子单元,所述注册子单元获取所述租户的身份信息,并基于ID注册协议对所述租户的账户进行建立,并通过所述授权单元生成授权码,其

中,若当前注册时所采用的设备为移动终端,则读取该设备的识别码并与授权码进行绑定;若当前的注册设备非移动终端,则等待下一次用移动终端登录时,授予其授权码;

所述ID创建子单元用于对所述租户的身份或者ID进行创建,并将生成的ID发送至所述传输网络中;

所述注册子单元还被构造为在所述租户进行注册或者进行登录时,获取与登录账户有关的移动终端的位置,以获取对应的租户信息;

所述备份模块包括识别单元和备份单元,所述识别单元基于所述租户的数据进行识别,以识别出数据是否为隐私数据,若为所述隐私数据则通过所述备份单元进行备份;所述备份单元用于对所述隐私数据进行备份,并通过安全模块对其进行防护;

所述识别单元通过隐私策略确定数据是否为隐私数据,其中,所述隐私策略包括在固有存储空间中开辟有若干个存储单元,各个存储单元分别存储有至少一条关于租户的个人数据;当各个所述存储单元被存储且满足打包阈值后生成打包指令,所述存储单元将会被打包,并通过所述备份单元进行备份;其中,所述备份单元基于所述打包指令执行备份操作;

所述备份单元基于所述备份ID以及识别单元的打包指令的数据,在租户的存储空间中开辟出供所述隐私数据存放的存储区域;其中,被存储后生成备份指令,所述备份指令用于在传输网络中与其他租户进行数据的交互;

所述同步模块包括同步单元和提取单元,所述同步单元基于所述提取单元对租户的需求清单进行同步,且所述同步单元在执行同步操作时,响应搜索的标签触发对数据的同步显示;

其中,同步操作包括:

建立搜索数据库,所述搜索数据库中包含各个租户的数据;

通过搜索引擎对租户的需求进行搜索,当在所述搜索数据库中存在与所述租户的需求相匹配的数据后,生成相对应的搜索结果;

基于搜索结果,显示出相应的租户信息,并把租户信息发送至提交需求的租户的移动终端上,其中,租户信息包括租户租赁地址、与需求提交设备实时的预估距离、联系电话;

所述安全模块用于对租户的数据进行防护,且当所述租户在所述传输网络中上传数据时,所述安全模块对数据进行加密操作;所述安全模块对所述搜索结果非必要公布的数据进行隐藏,以防护所述租户的信息安全;

所述加密操作包括:

获取租户的数据容量,并对该数据容量分配隶属度,其中,所述隶属度根据租户的身份信息或者所述授权码进行生成;获取一个需要加密操作的数据序列 $U = \{C_1, C_2, C_3, \dots, C_m\}$ ,  $m \in \mathbb{R}$ ;所述安全模块根据下式执行加密:

$$MI = [C_1, C_2, C_3, \dots, C_m] \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = w_1 C_1 + \dots + w_n C_m$$

其中,  $\begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{bmatrix}$  为加密明文序列, MI为加密的密钥; m为数据序列的元素数量; n为加密明文

序列的元素数量; 且m=n。

## 一种面向公有云租户业务敏感数据的分布式备份同步系统

### 技术领域

[0001] 本发明涉及租赁技术领域,尤其涉及一种面向公有云租户业务敏感数据的分布式备份同步系统。

### 背景技术

[0002] 随着个人信息与单位信息的价值越来越高,信息安全保障已越来越被企业重视。如何规避日常生产运行所涉及的大量敏感信息,成为信息安全首要考虑问题,而承载核心业务系统的生产数据库更是重中之重。在日常信息化建设中,不可避免的需要从生产库迁移大量业务测试数据至开发/测试库,如何在满足信息化建设基础上,最大限度地保护敏感信息,是当前面临的重要挑战。

[0003] 如CN105740722B现有技术公开了一种数据库敏感数据的伪装方法,无法避免的是数据需要来源于生产系统,为了保护数据安全性又不影响开发测试的要求,所以要提供一些相同类型但不同值的数据或数据库,实际就是生成数据的“替代品”。这个替代数据有时是假的,但更多的是一种混乱的真实数据。使用数据伪装,能够帮助企业防止未经授权的个人敏感数据被获取。同时,数据伪装提供代替真实数据测试的目的,开发、或更改数据库或配置管理。

[0004] 为了解决本领域普遍存在数据安全性差、无法进行隐藏、无法进行备份、被恶意访问和保护手段缺乏等等问题,作出了本发明。

### 发明内容

[0005] 本发明的目的在于,针对目前敏感数据处理所存在的不足,提出了一种面向公有云租户业务敏感数据的分布式备份同步系统。

[0006] 为了克服现有技术的不足,本发明采用如下技术方案:

[0007] 一种面向公有云租户业务敏感数据的分布式备份同步系统,包括采集模块、安全模块、备份模块、同步模块、核验模块和处理器,

[0008] 所述处理器分别与所述采集模块、所述安全模块、所述备份模块、同步模块和核验模块控制连接,其中,所述采集模块用于对租户的数据进行采集,以实现与所述租户的业务以及身份ID进行采集;所述核验模块用于对所述租户身份和访问的移动终端进行核验;所述安全模块用于对所述租户的数据进行防护,以配合所述备份模块对租户的数据进行备份;所述备份模块用于对各个租户的数据进行备份,并存储在所述租户的个人数据库中;

[0009] 所述同步模块在接收经过核验模块的核验过的访问请求时,触发对所述租户数据的同步;

[0010] 所述采集模块包括联网单元和数据库,所述联网单元用于与所述租户的移动终端进行联网,组建传输网络,其中,所述传输网络在连接前通过所述核验模块对各个租户对应的移动终端的授权许可进行核验;所述数据库用于对所述联网单元采集的各个租户信息进行存储,并反馈存储序列号;

[0011] 所述采集模块还包括管理单元,所述管理单元利用租户提供的身份信息生成相应的通行码,当使用所述通行码则需要访问的位置进行核验,若通行码符合通行条件,则对所需业务进行访问;

[0012] 所述管理单元还包括通行码生成器,所述通行码生成器用于自动生成通行码以及备份ID,所述通行码生成器通过下式公式生成通行码 $pass_i$ :

$$[0013] \quad Pass_i = \frac{(z_i - d_i)}{w_i} \left( \frac{task_i}{u_i} + k_i \right)$$

[0014] 其中, $u_i$ 为租户*i*访问总次数; $task_i$ 为当天访问的次数; $z_i$ 为当前时间; $d_i$ 为截止时间; $w_i$ 为访问时触发的等待时间; $k_i$ 为上一次访问的通行码,

$$k_i = \sum_{v=1}^N series \quad , \quad 0 \leq series \leq 9$$

[0015] 其中,series为租户的身份ID;且当生成新的通行码后,对通行码进行更新;

[0016] 所述通行码生成器通过下式生成备份ID:

$$[0017] \quad Backup_i = ag_i + bk_i$$

[0018] 其中,Backup<sub>*i*</sub>为备份ID;a和b为系数,其值跟租户发布的项目或者需求有关; $g_i$ 为租户上传的数据总存储量; $k_i$ 为上一次访问的通行码;

[0019] 所述管理单元在响应所述租户的访问请求前,需要利用所述通行器生成器生成新的通行码和备份ID,且新下发所述通行码和备份ID与原来的通行码和备份ID需不一致才有效,使访问请求的记录可被追溯。

[0020] 可选的,所述核验模块包括核验单元和授权单元,所述核验单元用于对所述租户的身份进行核验,若并未进行注册,则向所述租户反馈其结果;

[0021] 所述核验单元包括注册子单元和ID创建子单元,所述注册子单元获取所述租户的身份信息,并基于ID注册协议对所述租户的进行账户的建立,并通过所述授权单元生成授权码,其中,若当前的注册时所采用的设备为移动终端,则读取该设备的识别码并与授权码进行绑定;若当前的注册设备非移动终端,则等待下一次用移动终端登录时,授予其授权码;

[0022] 所述ID创建子单元用于对所述租户的身份或者ID进行创建,并将生成的ID发送至所述传输网络中;

[0023] 所述注册子单元还被构造为在所述租户进行注册或者进行需求清单提交时,获取与登录账户有关的移动终端的位置,以获取对应的租户信息。

[0024] 可选的,所述备份模块包括识别单元和备份单元,所述识别单元基于所述租户的数据进行识别,以识别出数据是否为隐私数据,若为所述隐私数据则通过所述备份数据进行备份;所述备份单元用于对所述隐私数据进行备份,并通过安全模块对其进行防护;

[0025] 所述识别单元通过隐私策略确定数据是否为隐私数据,其中,所述隐私策略包括在固有存储空间中开辟有若干个存储单元,各个存储单元分别存储有至少一条关于租户的个人数据;当各个所述存储单元被存储且满足打包阈值后生成打包指令,所述存储单元将会被打包,并通过所述备份单元进行备份;其中,所述备份单元基于所述打包指令执行备份



操作；

[0026] 所述备份单元基于所述备份ID以及识别单元的打包指令的数据，并在租户的存储空间中开辟出供所述隐私数据存放的存储区域；其中，被存储后生成备份指令，所述备份指令用于在传输网络中与其他租户或者寻租户进行数据的交互。

[0027] 可选的，所述同步模块包括同步单元和提取单元，所述同步单元基于所述提取单元对租户的需求清单进行同步，且所述同步单元在执行同步操作时，响应搜索的标签触发对数据的同步显示；

[0028] 其中，同步操作包括：

[0029] 建立搜索数据库，所述数据库中包含各个租户的数据；

[0030] 通过搜索引擎对租户的需求进行搜索，当在所述搜索数据库中存在与所述租户的需求相匹配的数据后，生成相对应的检索结果；

[0031] 基于搜索结果，显示出相应的租户信息，并把租户信息发送至提交需求的租户的移动终端或需求提交设备上，其中，租户信息包括租户租赁地址、与需求提交设备实时的预估距离、联系电话。

[0032] 可选的，所述安全模块用于对租户的数据进行防护，且当所述租户在所述传输网络中上传数据时，所述安全模块对数据进行加密操作；所述安全模块在对所述搜索结果进行非必要公布的数据进行隐藏，以防护所述租户的信息安全。

[0033] 可选的，所述加密操作包括：

[0034] 获取租户的数据容量，并对该数据容量分配隶属度，其中，所述隶属度根据租户的身份信息或者所述授权码进行生成；获取一个需要加密操作的数据序列 $U = \{C_1, C_2, C_3, \dots, C_m\}$ ， $m \in \mathbb{R}$ ；所述安全模块根据下式执行加密：

$$[0035] \quad MI = [C_1, C_2, C_3, \dots, C_m] \begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{bmatrix} = W_1 C_1 + \dots + W_n C_m$$

[0036] 其中， $\begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{bmatrix}$  为加密明文序列，MI为加密的密钥；m为数据序列的元素数量；n为加密明文序列的元素数量；且 $m=n$ 。

密明文序列的元素数量；且 $m=n$ 。

[0037] 本发明所取得的有益效果是：

[0038] 1. 通过采用所述管理单元在响应所述租户的访问请求前，需要利用所述通行码生成器生成新的通行码和备份ID，且新下发所述通行码和备份ID与原来的通行码和备份ID需不一致才有效，使访问请求的记录可被追溯，同时，通过备份ID则可以对所述租户的数据进行备份，并基于所述备份使得租户的数据能够有效的进行防护；

[0039] 2. 通过对所述租户的数据进行备份操作、以及对备份的数据进行标记，使得所有

的操作均能被追溯,以确保整个数据的安全;

[0040] 3. 通过采用通过搜索引擎对租户的需求进行搜索,当在所述搜索数据库中存在与所述租户的需求相匹配的数据后,生成相对应的检索结果;

[0041] 4. 通过所述安全模块在对所述搜索结果进行非必要公布的数据进行隐藏,以防护所述租户的信息安全;

[0042] 5. 通过上述加密明文序列、授权码的行列式和隶属度的行列式之间的配合,以实现所述数据进行加密,保证数据能够进行有效的防护;

[0043] 6. 通过对满足的需求清单且挑选出最优的匹配度,以使得所述租户在进行租赁或者发布的过程中能够获取最优质的资源,也最大限度的降低了对隐私数据的保护。

## 附图说明

[0044] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制,而是将重点放在示出实施例的原理上。在不同的视图中,相同的附图标记指定对应的部分。

[0045] 图1为本发明的控制流程示意图。

[0046] 图2为本发明所述采集模块的控制流程示意图。

[0047] 图3为本发明所述核验模块的控制流程示意图。

[0048] 图4为本发明所述备份模块的控制流程示意图。

[0049] 图5为本发明所述同步模块的控制流程示意图。

## 具体实施方式

[0050] 为了使得本发明的目的、技术方案及优点更加清楚明白,以下结合其实施例,对本发明进行进一步详细说明;应当理解,此处所描述的具体实施例仅用于解释本发明,并不用于限定本发明。对于本领域技术人员而言,在查阅以下详细描述之后,本实施例的其它系统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内、包括在本发明的范围内,并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征,并且这些特征根据以下将详细描述将是显而易见的。

[0051] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件;在本发明的描述中,需要理解的是,若有术语“上”、“下”、“左”、“右”等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或组件必须具有特定的方位、以特定的方位构造和操作,因此附图中描述位置关系的用语仅用于示例性说明,不能理解为对本专利的限制,对于本领域的普通技术人员而言,可以根据具体情况理解上述术语的具体含义。

[0052] 实施例一:根据图1-图5,提供一种面向公有云租户业务敏感数据的分布式备份同步系统,包括采集模块、安全模块、备份模块、同步模块、核验模块和处理器,所述处理器分别与所述采集模块、所述安全模块、所述备份模块、同步模块和核验模块控制连接,并基于所述处理器的集中控制下对各个租户的数据进行精准的备份或者防护。另外,同步系统还包括服务器,所述服务器与所述处理器进行连接,并与通过所述服务器与外部的系统或者网络进行联网,以实现各个租户进行数据的保护。其中,所述采集模块用于对租户的数据进行采集,以实现所述租户的业务以及身份ID进行采集;所述核验模块用于对所述租户



身份和访问的移动终端进行核验；所述安全模块用于对所述租户的数据进行防护，以配合所述备份模块对租户的数据进行备份；所述备份模块用于对各个租户的数据进行备份，并存储在所述租户的个人数据库中；

[0053] 所述同步模块在接收经过核验模块的核验过的访问请求时，触发对所述租户数据的同步；

[0054] 所述采集模块包括联网单元和数据库，所述联网单元用于与所述租户的移动终端进行联网，以组建传输网络，其中，所述传输网络在连接前通过所述核验模块对各个租户对应的移动终端的授权许可进行核验；所述数据库用于对所述联网单元采集的各个租户信息进行存储，并反馈存储序列号；当所述移动终端的未被授权，则对所述租户进行提示，以使得所述租户获得最佳使用体验。

[0055] 所述采集模块还包括管理单元，所述管理单元利用租户提供的身份信息生成相应的通行码，当使用所述通行码则需要访问的位置进行核验，若通行码符合通行条件，则对所需业务进行访问；

[0056] 所述身份信息包括但是不局限于以下列举的几种：身份证（身份ID）和不动产权证、不动产权登记证、公证的租赁合同等，用于确保租户的租赁资源为准确且可靠的。另外，在本实施例中，所述联网单元也可与所述服务器数据连接，以获取不动产权的证明材料等数据，以核验上述的信息是否为准确。同时，当上述提供的身份信息为租赁合同，则对租赁人以及承租人进行必要的核验，以确保双方提供的身份信息的可靠。

[0057] 所述管理单元还包括通行码生成器，所述通行码生成器用于自动生成通行码以及备份ID，所述通行码生成器通过下式公式生成通行码 $pass_i$ ：

$$[0058] \quad Pass_i = \frac{(z_i - d_i)}{w_i} \left( \frac{task_i}{u_i} + k_i \right)$$

[0059] 其中， $u_i$ 为租户i访问总次数； $task_i$ 为当天访问的次数； $z_i$ 为当前时间； $d_i$ 为截止时间； $w_i$ 为访问时触发的等待时间； $k_i$ 为上一次访问的通行码，

$$k_i = \sum_{v=1}^N series, \quad 0 \leq series \leq 9$$

[0060] 其中，series为租户的身份ID；且当生成新的通行码后，对通行码进行更新；

[0061] 所述通行码生成器通过下式生成备份ID：

$$[0062] \quad Backup_i = ag_i + bk_i$$

[0063] 其中， $Backup_i$ 为备份ID；a和b为系数，其值跟租户发布的项目或者需求有关； $g_i$ 为租户上传的数据总存储量； $k_i$ 为上一次访问的通行码；若所述租户此前并未发布任何的项目或者需求，则a和b均为1；若所述租户发布的项目或者提交的需求不为0，则a、b满足以下的关系： $a = G/g_i$ ， $b = f/G$ ，其中，G为所有项目或者需求的总项目数；f为当前备份的次数；在本实施例中，设置为设定的时间间隔内，触发对所述通行码的重新下发，以保证租户的个人数据能够进行备份。在其他的实施例中，也可以采用所述备份模块依据设定的备份时间间隔，自动进行备份。

[0064] 若上述的通行码为首次申请，则对其置零即可；另外，在对 $k_i$ 的验证过程中，通过

对所述租户的身份信息进行采集,同时,对身份证中存在的特殊字母,如:出现的“X”进行抛弃,用0~9的数据进行通行码的生成。

[0065] 所述管理单元在响应所述租户的访问请求前,需要利用所述通行码生成器生成新的通行码和备份ID,且新下发所述通行码和备份ID与原来的通行码和备份ID需不一致才有效,使访问请求的记录可被追溯。通过备份ID则可以对所述租户的数据进行备份,并基于所述备份使得租户的数据能够有效的进行防护。

[0066] 可选的,所述核验模块包括核验单元和授权单元,所述核验单元用于对所述租户的身份进行核验,若并未进行注册,则向所述租户反馈其结果;在对所述租户进行结果反馈的过程中,反馈的结果中均不包含任何非必要的信息,以实现对个人信息的保护。同时,通过所述核验单元和所述授权单元之间的配合使用,使得能兼顾核验和对新租户的注册请求。其中,所述核验单元包括注册子单元和ID创建子单元,所述注册子单元获取所述租户的身份信息,并基于ID注册协议对所述租户的进行账户的建立,并通过所述授权单元生成授权码,其中,若当前的注册时所采用的设备为移动终端,则读取该设备的识别码并与授权码进行绑定,绑定后所述移动终端则被授予与所述租户账户对应,且能够进行访问或者需求的提交;若当前的注册设备非移动终端,则等待下一次用移动终端登录时,授予其授权码;所述ID创建子单元用于对所述租户的身份或者ID进行创建,并将生成的ID发送至所述传输网络中;

[0067] 所述注册子单元还被构造为在所述租户进行注册或者进行需求清单提交时,获取与登录账户有关的移动终端的位置,以获取对应的租户信息。另外,所述登录信息和位置信息也可以根据所述租户手动进行添加,以实现对该位置附近的租赁信息进行获取,通过上述的获取方式也极大的方便租户能够对所述租赁提供场所进行确定。

[0068] 可选的,所述备份模块包括识别单元和备份单元,所述识别单元基于所述租户的数据进行识别,以识别出数据是否为隐私数据,若为所述隐私数据则通过所述备份数据进行备份;所述备份单元用于对所述隐私数据进行备份,并通过安全模块对其进行防护;

[0069] 所述识别单元通过隐私策略确定数据是否为隐私数据,其中,所述隐私策略包括在固有存储空间中开辟有若干个存储单元,各个存储单元分别存储有至少一条关于租户的个人数据;当各个所述存储单元被存储且满足打包阈值后生成打包指令,所述存储单元中的数据将会被打包,并通过所述备份单元进行备份操作;其中,所述备份单元基于所述打包指令执行备份操作;

[0070] 所述备份单元基于所述备份ID以及识别单元的打包指令的数据,并在租户的存储空间中开辟出供所述隐私数据存放的存储区域;其中,被存储后生成备份指令,所述备份指令用于在传输网络中与其他租户或者寻租户进行数据的交互。

[0071] 在备份指令中包含所述备份ID和设定的阈值信息,当两者满足上述的条件后,则执行备份操作。另外,在进行备份后的数据单元被进行标记,标记的信息包括但是不局限于以下列举的几种:执行设备、执行备份的时间、操作者的身份ID等。通过对所述租户的数据进行备份操作、以及对备份的数据进行标记,使得所有的操作均能被追溯,以确保整个数据的安全。

[0072] 可选的,所述同步模块包括同步单元和提取单元,所述同步单元基于所述提取单元对租户的需求清单进行同步,且所述同步单元在执行同步操作时,响应搜索的标签触发

对数据的同步显示;所述需求清单由所述租户进行提交,所述需求清单中包括租赁需求位置、租赁的类型或者其他需求。

[0073] 其中,同步操作包括:建立搜索数据库,所述数据库中包含各个租户的数据;特别的,所述租户的数据中包括租赁者和出租者的数据,同时,在租赁者进行租赁的过程中,需要通过搜索引擎进行需求的搜索,以实现能满足需求的位置或者出租信息。另外,在搜索出的数据中,仅仅显示一些非隐私数据,其中,非隐私数据指的是可以获知对方的出租信息的数据。同时,建立的搜索数据库基于所属服务器,使得大载量的租户访问能被满足。

[0074] 通过搜索引擎对租户的需求进行搜索,当在所述搜索数据库中存在与所述租户的需求相匹配的数据后,生成相对应的检索结果;其中,经过所述核验模块核验且已授予授权码的设备能执行搜索操作,若设备并未被授予授权码,则无法执行搜索操作,此时,反馈给所述租户进行实名认证或者进行设备的绑定。通过对访问记录进行记录,使得访问者能够被记录,有效提升数据的安全。另外,所述搜索引擎的搜索范围是基于所述租户提交的需求清单,且所述数据库也是经过系统进行初步筛选后,满足所述租户的需求后生成的新的子数据库。

[0075] 基于搜索结果,显示出相应的租户信息,并把租户信息发送至提交需求的租户的移动终端或需求提交设备上,其中,租户信息包括租户租赁地址、与需求提交设备实时的预估距离、联系电话。通过对部分的租户信息进行显示能兼顾满足需求和租赁业务的满足,也能最大限度的满足隐私数据的保护。

[0076] 可选的,所述安全模块用于对租户的数据进行防护,且当所述租户在所述传输网络中上传数据时,所述安全模块对数据进行加密操作;所述安全模块在对所述搜索结果非必要公布的数据进行隐藏,以防护所述租户的信息安全。

[0077] 可选的,所述加密操作包括:获取租户的数据容量,并对该数据容量分配隶属度,其中,所述隶属度根据租户的身份信息或者所述授权码进行生成,另外,针对不同的数据容量分配的隶属度也不一致,当存储的数据发生变化时,会引起数据容量产生变化,也会带来所述隶属度的变化;同时,所述隶属度的确定根据各个所述数据的权重进行确定。

[0078] 获取一个需要加密操作的数据序列 $U = \{C_1, C_2, C_3, \dots, C_m\}$ ,  $m \in \mathbb{R}$ ;所述安全模块根据下式执行加密:

$$[0079] \quad MI = [C_1, C_2, C_3, \dots, C_m] \begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{bmatrix} = w_1 C_1 + \dots + w_n C_m$$

[0080] 其中,  $\begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{bmatrix}$  为加密明文序列,MI为加密的密钥; $m$ 为数据序列的元素数量; $n$ 为加

密明文序列的元素数量;且 $m=n$ ;  $m \in \mathbb{R}$ ,  $n \in \mathbb{R}$ 。另外,所述加密明文序列均出现在加密和解密的过程。同时,所述加密明文序列与所述租户的信息相关,且根据所述租户的授权码有关,

具体的，

$$[0081] \quad \begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{bmatrix} = \frac{1}{2^{2n}} D \times H$$

[0082]  $D \times H$  为根据明文获取密文； $D$  为授权码的行列式； $H$  为隶属度的行列式。通过上述加密明文序列、授权码的行列式和隶属度的行列式之间的配合，以实现对上述数据进行加密，保证数据能够进行有效的防护。另外，所述明文序列可以根据  $D$  和  $H$  进行确定，且在解密的过程中，也能根据上述的公式进行解密，在此不再一一赘述。

[0083] 实施例二：本实施例应当理解为至少包含前述任一个实施例的全部特征，并在其基础上进一步改进，根据图1-图5，还在于对需求提交设备实时的预估距离进行确定，其中，所述租户的提供位置和所述需求提供位置的预估距离基于所述租户提供的需求并通过搜索引擎对满足需求清单中的位置进行确定，并对需求提交设备实时的预估距离进行确定，所述预估距离依据下面的公式进行确定：

$$[0084] \quad distance(u_i, u_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

[0085] 其中，在  $distance(u_i, u_j)$  中， $u_i$  表示所述移动终端或者所述租户的位置坐标，其坐标用  $(x_i, y_i)$  表示； $u_j$  表示满足需求清单的位置坐标，其坐标用  $(x_j, y_j)$  表示；

[0086] 坐标位置根据租赁者发布的位置进行确定，其坐标位置由GPRS所确定；

$$[0087] \quad MATH_i = \frac{distance(u_{ture}, u_i)}{\sum_{j=1}^k distance(u_{ture}, u_j)}, i=1, \dots, k; j=1, \dots, k$$

[0088] 其中， $MATH_i$  为所述搜索的匹配度； $u_{ture}$  为待选的租户位置坐标；

$$[0089] \quad MATH_{max} = \arg_{i \in (1, \dots, k)}^{\max} \{MATH_i\}$$

[0090] 其中， $MATH_{max}$  为在搜索的最佳匹配度。通过上述的对满足的需求清单且挑选出最优的匹配度，以使得所述租户在进行租赁或者发布的过程中能够获取最优质的资源，也最大限度的降低了对隐私数据的保护。另外，通过对数据进行分布式的方式对双方或者多方的数据进行隐私数据的保护，使得在进行数据的搜索的过程中，能对非隐私数据进行公开，其他的隐私数据的能够被有效的防护。

[0091] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中未详述或记载的部分，可以参见其它实施例的相关描述。

[0092] 虽然上面已经参考各种实施例描述了本发明，但是应当理解，在不脱离本发明的范围的情况下，可以进行许多改变和修改。也就是说上面讨论的方法，系统和设备是示例。各种配置可以适当地省略，替换或添加各种过程或组件。例如，在替代配置中，可以以与所

描述的顺序不同的顺序执行方法,和/或可以添加,省略和/或组合各种部件。而且,关于某些配置描述的特征可以以各种其他配置组合,如可以以类似的方式组合配置的不同方面和元素。此外,随着技术发展其中的元素可以更新,即许多元素是示例,并不限制本公开或权利要求的范围。

[0093] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而,可以在没有这些具体细节的情况下实践配置例如,已经示出了众所周知的电路,过程,算法,结构和技术而没有不必要的细节,以避免模糊配置。该描述仅提供示例配置,并且不限制权利要求的范围,适用性或配置。相反,前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下,可以对元件的功能和布置进行各种改变。

[0094] 综上,其旨在上述详细描述被认为是例示性的而非限制性的,并且应当理解,以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后,技术人员可以对本发明作各种改动或修改,这些等效变化和修饰同样落入本发明权利要求所限定的范围。

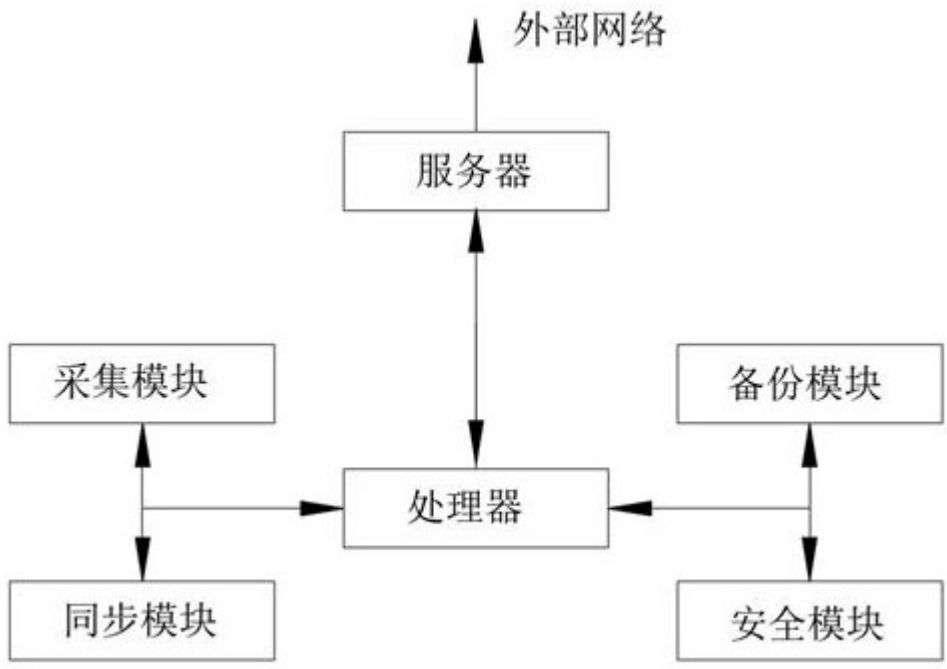


图1

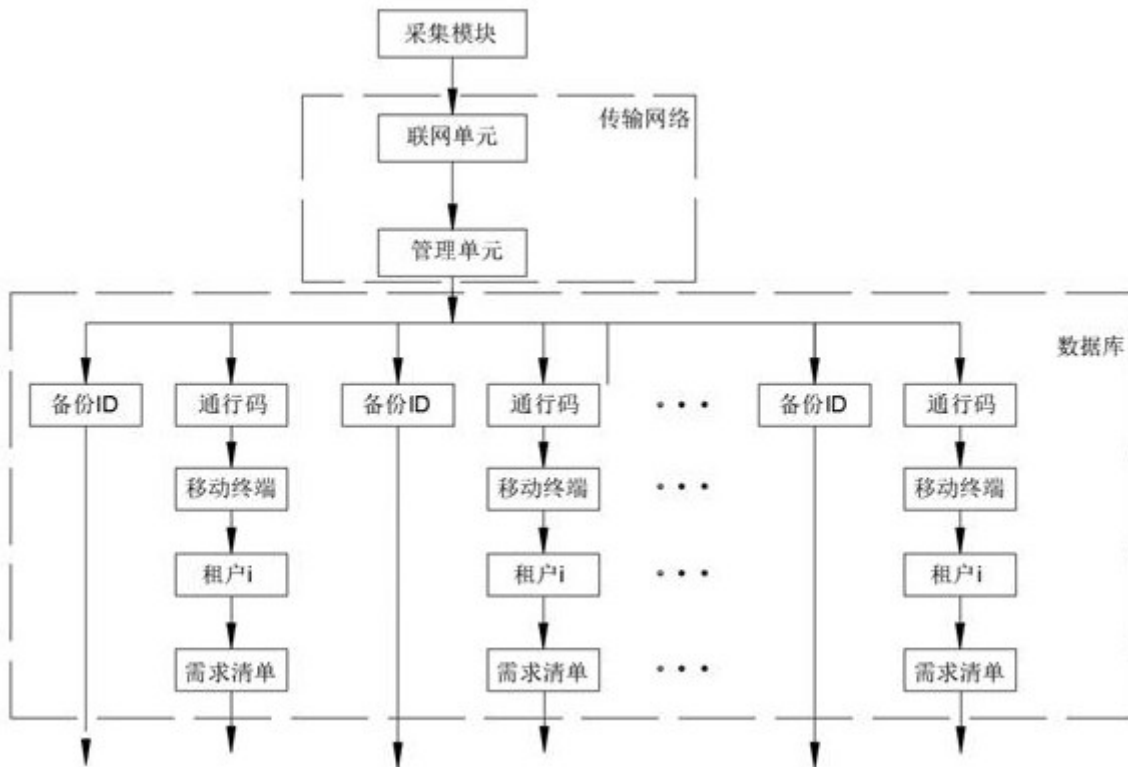


图2



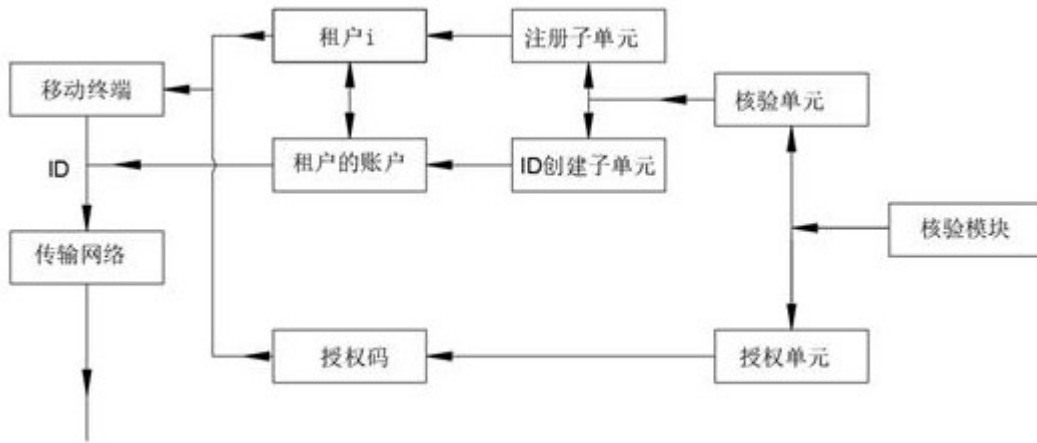


图3

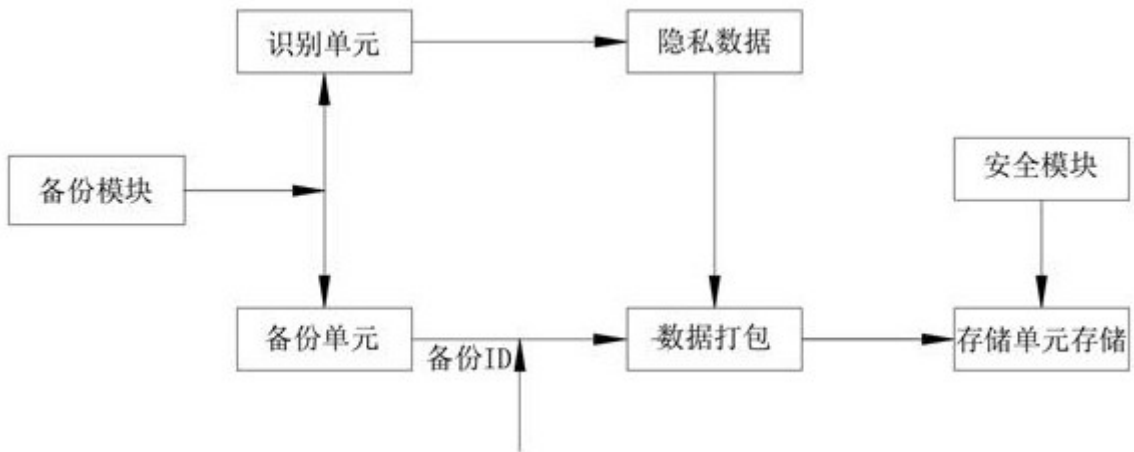


图4

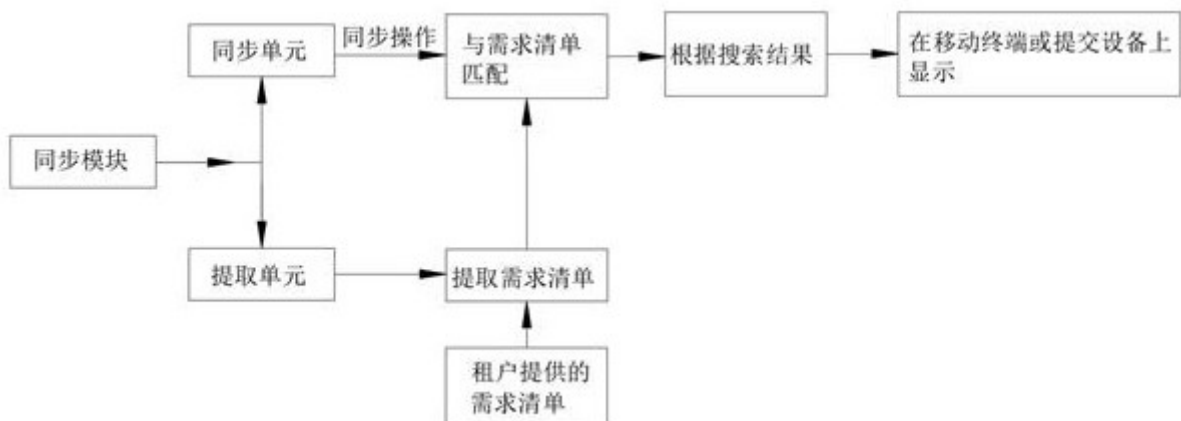


图5