(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112422866 A
(43)申请公布日 2021.02.26

(21)申请号 201910777602.0

(22)申请日 2019.08.22

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)

(72)发明人 毛宏

(74)专利代理机构 北京律诚同业知识产权代理有限公司 11006
代理人 王玉双

(51)Int.Cl.
H04N 5/781(2006.01)

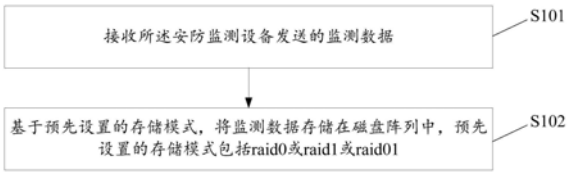
权利要求书1页 说明书9页 附图2页

(54)发明名称

一种数据存储方法及安防中控设备

(57)摘要

本发明公开了一种数据存储方法，应用于安防中控设备，所述安防中控设备内设置有磁盘阵列，所述安防中控设备与多个安防监测设备连接，所述方法包括：接收所述安防监测设备发送的监测数据；基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。本发明解决了现有技术中的安防监控设备在进行数据存储时，存储方式单一，存在严重数据安全隐患的技术问题，实现了丰富数据存储方式，提高数据存储速率，降低数据丢失风险的技术效果。同时，本发明还公开了一种安防中控设备。



CN 112422866 A

1.一种数据存储方法,其特征在于,应用于安防中控设备,所述安防中控设备内设置有磁盘阵列,所述安防中控设备与多个安防监测设备连接,所述方法包括:

接收所述安防监测设备发送的监测数据;

基于预先设置的存储模式,将所述监测数据存储在所述磁盘阵列中,所述预先设置的存储模式包括raid0或raid1或raid01。

2.如权利要求1所述的方法,其特征在于,所述安防中控设备设置有第一网络接口和第二网络接口,所述第一网络接口用于连接所述安防监测设备,所述第二网络接口用于连接互联网。

3.如权利要求1所述的方法,其特征在于,所述磁盘阵列中包括2至4块硬盘。

4.如权利要求1～3任一所述的方法,其特征在于,所述基于预先设置的存储模式,将所述监测数据存储在所述磁盘阵列中,包括:

基于用户的配置信息,从所述多个安防监测设备中确定出第一安防监测设备;

从所述监测数据中筛选出与所述第一安防监测设备对应的第一监测数据;

基于所述预先设置的存储模式,将所述第一监测数据存储到所述磁盘阵列中。

5.如权利要求4所述的方法,其特征在于,所述基于预先设置的存储模式,将所述监测数据存储在所述磁盘阵列中之后,还包括:

基于所述配置信息,从所述多个安防监测设备中确定出第二安防监测设备,其中,所述第二安防监测设备的安全级别高于所述第一安防监测设备;

从所述监测数据中筛选出与所述第二安防监测设备对应的第二监测数据;

通过第二网络接口将所述第二监测数据发送至指定云端服务器,以将所述第二监测数据保存在所述云端服务器中。

6.一种安防中控设备,其特征在于,所述安防中控设备与多个安防监测设备连接,所述安防中控设备,包括:

磁盘阵列;

处理器,与所述磁盘阵列连接,用于接收所述安防监测设备发送的监测数据;基于预先设置的存储模式,将所述监测数据存储在所述磁盘阵列中,所述预先设置的存储模式包括raid0或raid1或raid01。

7.如权利要求6所述的安防中控设备,其特征在于,所述安防中控设备,还包括:

第一网络接口,用于连接所述安防监测设备,

第二网络接口,用于连接互联网。

8.如权利要求6所述的安防中控设备,其特征在于,所述磁盘阵列中包括2至4块硬盘。

9.如权利要求6～8任一所述的安防中控设备,其特征在于,所述处理器,具体用于:

基于用户的配置信息,从所述多个安防监测设备中确定出第一安防监测设备;从所述监测数据中筛选出与所述第一安防监测设备对应的第一监测数据;基于所述预先设置的存储模式,将所述第一监测数据存储到所述磁盘阵列中。

10.一种安防监测系统,其特征在于,包括:

一个或多个安防监测设备;以及

如权利要求6～9任一所述的安防中控设备。

一种数据存储方法及安防中控设备

技术领域

[0001] 本发明涉及安防技术领域，尤其涉及一种数据存储方法及安防中控设备。

背景技术

[0002] 近些年，人们的安全意识不断提升，安防监测设备(例如：智能摄像头、烟雾报警器、红外报警器、等等)越来越受到人们的重视。现如今，很多人都会在家中安装一个或多个安防监控设备。

[0003] 但是，随着安防监测设备的数量与种类的增加，其需要存储的数据也越来越多，且越来越复杂，而目前的安防监测设备在进行数据存储时，存储方式比较单一，容易出现数据丢失或数据存储较慢的情况，严重影响数据安全和设备运行效率。

发明内容

[0004] 本申请实施例通过提供一种数据存储方法及安防中控设备，解决了现有技术中的安防监控设备在进行数据存储时，存储方式单一，存在严重数据安全隐患的技术问题，实现了丰富数据存储方式，提高数据存储速率，降低数据丢失风险的技术效果。

[0005] 第一方面，本申请通过本申请的一实施例提供如下技术方案：

[0006] 一种数据存储方法，其特征在于，应用于安防中控设备，所述安防中控设备内设置有磁盘阵列，所述安防中控设备与多个安防监测设备连接，所述方法包括：

[0007] 接收所述安防监测设备发送的监测数据；

[0008] 基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。

[0009] 优选地，所述安防中控设备设置有第一网络接口和第二网络接口，所述第一网络接口用于连接所述安防监测设备，所述第二网络接口用于连接互联网。

[0010] 优选地，所述磁盘阵列中包括2至4块硬盘。

[0011] 优选地，所述基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，包括：

[0012] 基于用户的配置信息，从所述多个安防监测设备中确定出第一安防监测设备；

[0013] 从所述监测数据中筛选出与所述第一安防监测设备对应的第一监测数据；

[0014] 基于所述预先设置的存储模式，将所述第一监测数据存储到所述磁盘阵列中。

[0015] 优选地，所述基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中之后，还包括：

[0016] 基于所述配置信息，从所述多个安防监测设备中确定出第二安防监测设备，其中，所述第二安防监测设备的安全级别高于所述第一安防监测设备；

[0017] 从所述监测数据中筛选出与所述第二安防监测设备对应的第二监测数据；

[0018] 通过第二网络接口将所述第二监测数据发送至指定云端服务器，以将所述第二监测数据保存在所述云端服务器中。

[0019] 第二方面，本申请通过本申请的一实施例，提供如下技术方案：

[0020] 一种安防中控设备，所述安防中控设备与多个安防监测设备连接，所述安防中控设备，包括：

[0021] 磁盘阵列；

[0022] 处理器，与所述磁盘阵列连接，用于接收所述安防监测设备发送的监测数据；基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。

[0023] 优选地，所述安防中控设备，还包括：

[0024] 第一网络接口，用于连接所述安防监测设备，

[0025] 第二网络接口，用于连接互联网。

[0026] 优选地，所述磁盘阵列中包括2至4块硬盘。

[0027] 优选地，所述处理器，具体用于：

[0028] 基于用户的配置信息，从所述多个安防监测设备中确定出第一安防监测设备；从所述监测数据中筛选出与所述第一安防监测设备对应的第一监测数据；基于所述预先设置的存储模式，将所述第一监测数据存储到所述磁盘阵列中。

[0029] 优选地，所述处理器，还用于：

[0030] 在所述基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中之后，基于用户的配置信息，从所述多个安防监测设备中确定出第二安防监测设备，其中，所述第二安防监测设备的安全级别高于所述第一安防监测设备；从所述监测数据中筛选出与所述第二安防监测设备对应的第二监测数据；通过第二网络接口将所述第二监测数据发送至指定云端服务器，以将所述第二监测数据保存在所述云端服务器中。

[0031] 第三方面，本申请通过本申请的一实施例，提供如下技术方案：

[0032] 一种安防监测系统，包括：

[0033] 一个或多个安防监测设备；以及

[0034] 如上述第一方面任一所述的安防中控设备。

[0035] 本申请实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

[0036] 在本申请实施例中，公开了一种数据存储方法，应用于安防中控设备，所述安防中控设备内设置有磁盘阵列，所述安防中控设备与多个安防监测设备连接，所述方法包括：接收所述安防监测设备发送的监测数据；基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。如此，解决了现有技术中的安防监控设备在进行数据存储时，存储方式单一，存在严重数据安全隐患的技术问题，实现了丰富数据存储方式，提高数据存储速率，降低数据丢失风险的技术效果。

附图说明

[0037] 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的前提下，还可以根据这些附图获得其他的附图。

[0038] 图1为本申请实施例中一种安防监测系统的架构图；；

[0039] 图2为本申请实施例中一种数据存储方法的流程图；

[0040] 图3为本申请实施例中一种安防中控设备的结构图。

具体实施方式

[0041] 本申请实施例通过提供一种数据存储方法及安防中控设备，解决了现有技术中的安防监控设备在进行数据存储时，存储方式单一，存在严重数据安全隐患的技术问题，实现了丰富数据存储方式，提高数据存储速率，降低数据丢失风险的技术效果。

[0042] 本申请实施例的技术方案为解决上述技术问题，总体思路如下：

[0043] 一种数据存储方法，应用于安防中控设备，所述安防中控设备内设置有磁盘阵列，所述安防中控设备与多个安防监测设备连接，所述方法包括：接收所述安防监测设备发送的监测数据；基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。

[0044] 为了更好的理解上述技术方案，下面将结合说明书附图以及具体的实施方式对上述技术方案进行详细的说明。

[0045] 首先说明，本文中出现的术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0046] 实施例一

[0047] 本实施例提供了一种数据存储方法，应用于安防中控设备，安防中控设备与一个或多个安防监测设备连接，安防中控设备内设置有一磁盘阵列，所述方法包括：

[0048] 步骤S101：接收安防监测设备发送的监测数据。

[0049] 在具体实施过程中，如图3所示，所述安防监测设备，包括：监控摄像头、智能摄像头、智能门铃、红外报警器、扫地机器人、智能音响、烟雾报警器、等等。这些安防监测设备与安防中控设备共同组成了安防监测系统，该安防监测系统可以为家庭提供安全监测服务。

[0050] 其中，安防监测设备可以用于对房屋的不同区域进行监测。安防中控设备作为家庭安全大脑，与每一个安防监测设备连接，启到总控制作用，同时也会存储每个安防监测设备所采集到的监测数据。

[0051] 下面，以别墅用户为例，对上述安防监测系统进行简要介绍：

[0052] 红外报警器，可以安装在别墅的围墙上，用于监测是否有入侵者翻墙进入，若监测到有入侵者，则发出报警。红外报警器可以通过数据线或无线网络与安防中控设备连接，从而将监测到的数据(即：图像数据)发给安防中控设备。

[0053] 智能门铃，也叫可视门铃，可以安装在别墅的大门上，智能门铃不但具有普通门铃的功能(即：来访者可以触发智能门铃上的预设按钮，例如“呼叫”按钮，控制智能门铃发出铃声，从而呼叫室内的主人)，智能门铃还具有危险识别功能(例如：在智能门铃上设置有摄像头，用于采集门前区域的图像，并进行分析，在分析出门外有可疑人员或危险人员逗留时，发出报警信息)。智能门铃可以通过数据线或无线网络与安防中控设备连接，从而将监测到的数据(即：图像数据)发给安防中控设备。

[0054] 监控摄像头，可以安装在室内，也可以安装在别墅的外墙上，用于采集对应监测区域的视频图像。监控摄像头可以通过数据线或无线网络与安防中控设备连接，从而将监测

到的数据(即:图像数据)发给安防中控设备。

[0055] 智能摄像头,与监控摄像头功能基本一致,但体积更小,通常安装在室内。另外,智能摄像头还可以将采集到的视频图像上传到云端服务器,用户可以使用任一用户终端(例如:智能手机或平板电脑等)访问云端服务器,观看到该视频图像。智能摄像头可以通过数据线或无线网络与安防中控设备连接,从而将监测到的数据(即:图像数据)发给安防中控设备。

[0056] 扫地机器人,通常位于室内,且具有摄像头,可以在室内行走和清扫,其所携带的摄像头可对室内进行图像采集。扫地机器人可以通过数据线或无线网络与安防中控设备连接,从而将监测到的数据(即:图像数据)发给安防中控设备。

[0057] 烟雾报警器,用于对烟雾进行检测,并在检测到烟雾时进行报警,其可以有效地在火灾发生初期报警,从而警示用户及时灭火或逃生。烟雾报警器可以通过数据线或无线网络与安防中控设备连接,从而将监测到的数据(即:烟雾数据)发给安防中控设备。

[0058] 智能音响,一般具有麦克风和扬声器,麦克风可以用于采集环境中的声音数据。智能音响可以通过数据线或无线网络与安防中控设备连接,从而将监测到的数据(即:声音数据)发给安防中控设备。

[0059] 安防中控设备可以基于上述一个或多个安防监测设备发来的监测数据进行综合分析,判断别墅当前是否存在风险(例如:是否有陌生人入侵,是否有火灾、等等),在确定存在风险时,可以进行报警。例如,向用户终端(例如:别墅用户的智能手机、平板电脑、PC)和/或智能音响发送报警信息,其中,智能音响可以通过其自带的扬声器输出报警信息。

[0060] 在具体实施过程中,上述一个或多个安防监测设备可以实时或定时将各自所采集到的监测数据发送给安防中控设备,由安防中控设备进行存储。

[0061] 步骤S102:基于预先设置的存储模式,将监测数据存储在磁盘阵列中,预先设置的存储模式包括raid0或raid1或raid01。

[0062] 在具体实施过程中,在安防中控设备内设置有一磁盘阵列。磁盘阵列是由很多块独立的磁盘,组合成一个容量巨大的磁盘组,利用个别磁盘提供数据所产生加成效果提升整个磁盘系统效能。利用这项技术,将数据切割成许多区段,分别存放在各个硬盘上。磁盘阵列还能利用同位检查(Parity Check)的观念,在数组中任意一个硬盘故障时,仍可读出数据,在数据重构时,将数据经计算后重新置入新硬盘中。

[0063] 磁盘阵列具有如下优点:

[0064] (1)提高传输速率。磁盘阵列通过在多个磁盘上同时存储和读取数据来大幅提高存储系统的数据吞吐量(Throughput)。在磁盘阵列中,可以让很多磁盘驱动器同时传输数据,而这些磁盘驱动器在逻辑上又是一个磁盘驱动器,所以使用磁盘阵列可以达到单个磁盘驱动器几倍、几十倍甚至上百倍的速率。

[0065] (2)通过数据校验提供容错功能。磁盘阵列容错是建立在每个磁盘驱动器的硬件容错功能之上的,所以它提供更高的安全性。在很多磁盘阵列模式中都有较为完备的相互校验/恢复的措施,甚至是直接相互的镜像备份,从而大大提高了磁盘阵列系统的容错度,提高了系统的稳定冗余性。

[0066] 在具体实施过程中,安防中控设备可以支持多种存储模式(例如:raid0、或raid1、或raid01),用户可以自由设置。其中,raid0可以提高数据的存储速率,raid1可以实现数据

的自动备份，raid01可以同时实现提高数据的存储速率和数据的自动备份。

[0067] 具体来讲：

[0068] raid0：连续以位或字节为单位分割数据，并行读/写于多个磁盘上，因此具有很高的数据传输率。

[0069] raid1：它是通过磁盘数据镜像实现数据冗余，在成对的独立磁盘上产生互为备份的数据。当原始数据繁忙时，可直接从镜像拷贝中读取数据，因此raid1可以提高读取性能。raid1提供了很高的数据安全性和可用性。当一个磁盘失效时，系统可以自动切换到镜像磁盘上读写，而不需要重组失效的数据。

[0070] raid01：是将raid0和raid1标准结合的产物，在连续地以位或字节为单位分割数据并且并行读/写多个磁盘的同时，为每一块磁盘作磁盘镜像进行冗余。它的优点是同时拥有raid0的超凡速度和raid1的数据高可靠性。

[0071] 当然，安防中控设备还可以支持其他的数据存储模式(例如：raid2、raid3、raid4、raid5、raid6、等等)，可以由用户自由设置，本实施例不做具体限定。

[0072] 在具体实施过程中，磁盘阵列中包括2至4块硬盘。当然，还可以设置更多的硬盘(例如：5块、6块、8块、10块、20块等等)，此处不做具体限定。

[0073] 作为一种可选的实施例，安防中控设备设置有第一网络接口和第二网络接口，第一网络接口用于连接安防监测设备，第二网络接口用于连接互联网。

[0074] 在具体实施过程中，在安防中控设备上设置有两个网络接口，一个用于通过数据线连接安防监测设备，另一个用于通过数据线接入互联网，从而将安防监测设备与互联网隔离，进而避免安防监测设备受到来自互联网的攻击。

[0075] 在具体实施过程中，安防中控设备需要通过第一网络接口接收每个安防监测设备发送的监测数据。

[0076] 作为一种可选的实施例，安防中控设备设置有一无线网卡，其可以同时支持两个无线网络(例如：第一无线网络和第二无线网络)，第一无线网络用于通过无线方式连接安防监测设备，第二无线网络用于通过无线方式接入互联网，如此，减少了布线，且可以将安防监测设备与互联网隔离，进而避免安防监测设备受到来自互联网的攻击。

[0077] 作为一种可选的实施例，步骤S102，包括：

[0078] 基于用户的配置信息，从多个安防监测设备中确定出第一安防监测设备；从监测数据中筛选出与第一安防监测设备对应的第一监测数据；基于预先设置的存储模式，将第一监测数据存储到磁盘阵列中。

[0079] 在具体实施过程中，用户可以针对每个安防监测设备选择器存储位置，例如，可以选择存储在安防中控设备的磁盘阵列上，也可以存储在云端服务器。

[0080] 在具体实施过程中，可以基于用户的设置操作生成配置信息，该配置信息中记录有需要将监测数据存储在磁盘阵列中的安防监控设备(即：第一安防监测设备)，这些设备的安全级别较低，不宜存储在云端存储器上，容易出现数据安全隐患。因此，在进行数据存储时，安防中控设备可以从众多监测设备中识别出第一安防监测设备，进一步基于预先设置的存储模式，将第一安防监测设备对应的第一监测数据存储到磁盘阵列中。

[0081] 具体来讲，在安防监测设备发给安防中控设备的监测数据中，会携带有该安防监测设备的标识信息(例如：设备ID)，在配置信息中存储有第一安防监测设备的标识信息(例

如:设备ID),如此,安防中控设备可以基于配置信息中记载的标识信息,从众多监测设备中识别出第一安防监测设备,并基于监测数据所携带的标识信息,从接收到的众多监测数据识别出第一安防监测设备对应的第一监测数据。

[0082] 作为一种可选的实施例,在步骤S102之后,还包括:

[0083] 基于用户的配置信息,从多个安防监测设备中确定出第二安防监测设备,其中,第二安防监测设备的安全级别高于第一安防监测设备;从监测数据中筛选出与第二安防监测设备对应的第二监测数据;通过第二网络接口(或第二无线网络)将第二监测数据发送至指定的云端服务器,以将第二监测数据保存在云端服务器中。

[0084] 在具体实施过程中,对于安全级别比较高的安防监测设备(即:第二安防监测设备),用户比较放心,可以允许将第二安防监测设备发送的监测数据(即:第二监测数据)存储在云端服务器中。

[0085] 上述本申请实施例中的技术方案,至少具有如下的技术效果或优点:

[0086] 在本申请实施例中,公开了一种数据存储方法,应用于安防中控设备,所述安防中控设备内设置有磁盘阵列,所述安防中控设备与多个安防监测设备连接,所述方法包括:接收所述安防监测设备发送的监测数据;基于预先设置的存储模式,将所述监测数据存储在所述磁盘阵列中,所述预先设置的存储模式包括raid0或raid1或raid01。如此,解决了现有技术中的安防监控设备在进行数据存储时,存储方式单一,存在严重数据安全隐患的技术问题,实现了丰富数据存储方式,提高数据存储速率,降低数据丢失风险的技术效果。

[0087] 实施例二

[0088] 基于同一发明构思,如图2所示,本实施例提供了一种安防中控设备200,安防中控设备200与多个安防监测设备连接,安防中控设备200,包括:

[0089] 磁盘阵列201;

[0090] 处理器202,与磁盘阵列201连接,用于接收所述安防监测设备发送的监测数据;基于预先设置的存储模式,将所述监测数据存储在所述磁盘阵列201中,所述预先设置的存储模式包括raid0或raid1或raid01。

[0091] 作为一种可选的实施例,安防中控设备200,还包括:

[0092] 第一网络接口203,用于连接所述安防监测设备,

[0093] 第二网络接口204,用于连接互联网。

[0094] 作为一种可选的实施例,所述磁盘阵列201中包括2至4块硬盘。

[0095] 作为一种可选的实施例,处理器202,具体用于:

[0096] 基于用户的配置信息,从所述多个安防监测设备中确定出第一安防监测设备;从所述监测数据中筛选出与所述第一安防监测设备对应的第一监测数据;基于所述预先设置的存储模式,将所述第一监测数据存储到所述磁盘阵列中。

[0097] 作为一种可选的实施例,处理器202,还用于:

[0098] 在所述基于预先设置的存储模式,将所述监测数据存储在所述磁盘阵列中之后,基于用户的配置信息,从所述多个安防监测设备中确定出第二安防监测设备,其中,所述第二安防监测设备的安全级别高于所述第一安防监测设备;从所述监测数据中筛选出与所述第二安防监测设备对应的第二监测数据;通过第二网络接口(或第二无线网络)将所述第二监测数据发送至指定云端服务器,以将所述第二监测数据保存在所述云端服务器中。

[0099] 由于本实施例所介绍的安防中控设备为实施本申请实施例一中数据存储方法所采用的设备，故而基于本申请实施例中所介绍的数据存储方法，本领域所属技术人员能够了解本实施例的安防中控设备的具体实施方式以及其各种变化形式，所以在此对于该安防中控设备如何实现本申请实施例中的方法不再详细介绍。只要本领域所属技术人员实施本申请实施例中数据存储方法所采用的装置，都属于本申请所欲保护的范围。

[0100] 上述本申请实施例中的技术方案，至少具有如下的技术效果或优点：

[0101] 在本申请实施例中，公开了一种安防中控设备，所述安防中控设备与多个安防监测设备连接，所述安防中控设备，包括：磁盘阵列；处理器，与所述磁盘阵列连接，用于接收所述安防监测设备发送的监测数据；基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。如此，解决了现有技术中的安防监控设备在进行数据存储时，存储方式单一，存在严重数据安全隐患的技术问题，实现了丰富数据存储方式，提高数据存储速率，降低数据丢失风险的技术效果。

[0102] 实施例三

[0103] 基于同一发明构思，如图3所示，本实施例提供了一种安防监测系统，包括：

[0104] 一个或多个安防监测设备；以及

[0105] 安防中控设备(如实施例二所示)，与一个或多个安防监测设备连接。

[0106] 在具体实施过程中，所述安防监测设备，包括：监控摄像头、智能摄像头、智能门铃、红外报警器、扫地机器人、智能音响、烟雾报警器、等等。这些设备和安防中控设备共同组成了一安防监测系统，该安防监测系统可以为家庭提供安全监测服务。

[0107] 其中，安防监测设备可以用于对房屋的不同区域进行监测。安防中控设备作为家庭安全大脑，与每一个安防监测设备连接，启到总控制作用，同时也会存储各个安防监测设备所采集到的监测数据。

[0108] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0109] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0110] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0111] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单

元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0112] 此外，本领域的技术人员能够理解，尽管在此的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0113] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的一种安防中控设备、安防监测系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0114] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0115] 本发明公开了，A1、一种数据存储方法，其特征在于，应用于安防中控设备，所述安防中控设备内设置有磁盘阵列，所述安防中控设备与多个安防监测设备连接，所述方法包括：

[0116] 接收所述安防监测设备发送的监测数据；

[0117] 基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。

[0118] A2、如A1所述的方法，其特征在于，所述安防中控设备设置有第一网络接口和第二网络接口，所述第一网络接口用于连接所述安防监测设备，所述第二网络接口用于连接互联网。

[0119] A3、如A1所述的方法，其特征在于，所述磁盘阵列中包括2至4块硬盘。

[0120] A4、如A1～A3任一所述的方法，其特征在于，所述基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，包括：

[0121] 基于用户的配置信息，从所述多个安防监测设备中确定出第一安防监测设备；

[0122] 从所述监测数据中筛选出与所述第一安防监测设备对应的第一监测数据；

[0123] 基于所述预先设置的存储模式，将所述第一监测数据存储到所述磁盘阵列中。

[0124] A5、如A4所述的方法，其特征在于，所述基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中之后，还包括：

[0125] 基于所述配置信息，从所述多个安防监测设备中确定出第二安防监测设备，其中，所述第二安防监测设备的安全级别高于所述第一安防监测设备；

[0126] 从所述监测数据中筛选出与所述第二安防监测设备对应的第二监测数据；

[0127] 通过第二网络接口将所述第二监测数据发送至指定云端服务器，以将所述第二监测数据保存在所述云端服务器中。

[0128] B6、一种安防中控设备，其特征在于，所述安防中控设备与多个安防监测设备连接，所述安防中控设备，包括：

[0129] 磁盘阵列；

[0130] 处理器，与所述磁盘阵列连接，用于接收所述安防监测设备发送的监测数据；基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中，所述预先设置的存储模式包括raid0或raid1或raid01。

[0131] B7、如B6所述的安防中控设备，其特征在于，所述安防中控设备，还包括：

[0132] 第一网络接口，用于连接所述安防监测设备，

[0133] 第二网络接口，用于连接互联网。

[0134] B8、如B6所述的安防中控设备，其特征在于，所述磁盘阵列中包括2至4块硬盘。

[0135] B9、如B6～B8任一所述的安防中控设备，其特征在于，所述处理器，具体用于：

[0136] 基于用户的配置信息，从所述多个安防监测设备中确定出第一安防监测设备；从所述监测数据中筛选出与所述第一安防监测设备对应的第一监测数据；基于所述预先设置的存储模式，将所述第一监测数据存储到所述磁盘阵列中。

[0137] B10、如B9所述的安防中控设备，其特征在于，所述处理器，还用于：

[0138] 在所述基于预先设置的存储模式，将所述监测数据存储在所述磁盘阵列中之后，基于所述配置信息，从所述多个安防监测设备中确定出第二安防监测设备，其中，所述第二安防监测设备的安全级别高于所述第一安防监测设备；从所述监测数据中筛选出与所述第二安防监测设备对应的第二监测数据；通过第二网络接口将所述第二监测数据发送至指定云端服务器，以将所述第二监测数据保存在所述云端服务器中。

[0139] C11、一种安防监测系统，其特征在于，包括：

[0140] 一个或多个安防监测设备；以及

[0141] 如B6～B10任一所述的安防中控设备。

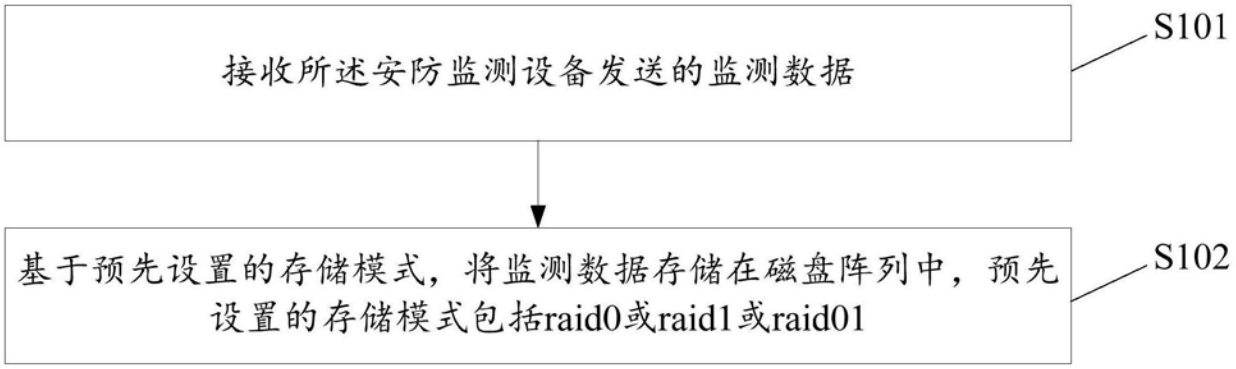


图1

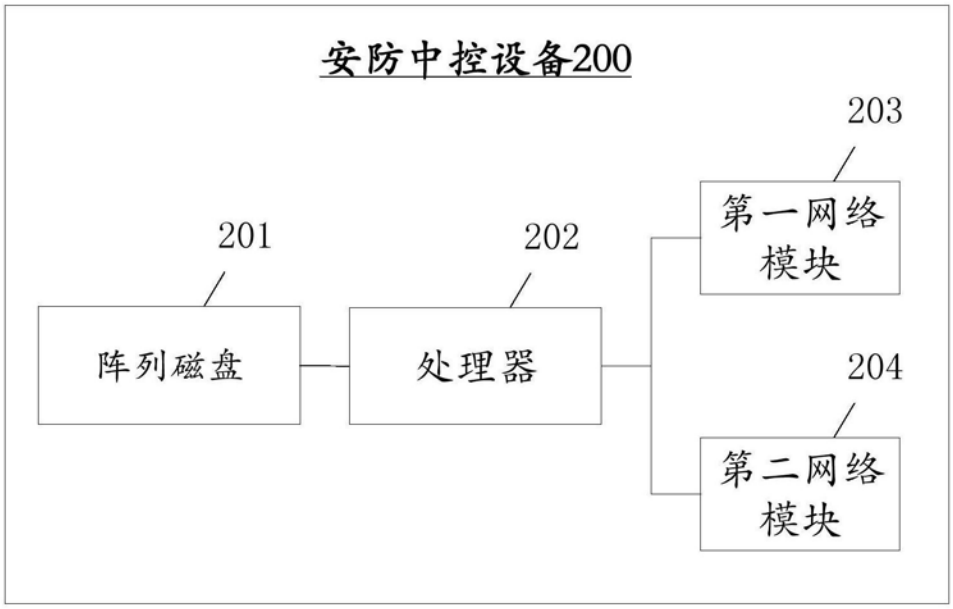


图2

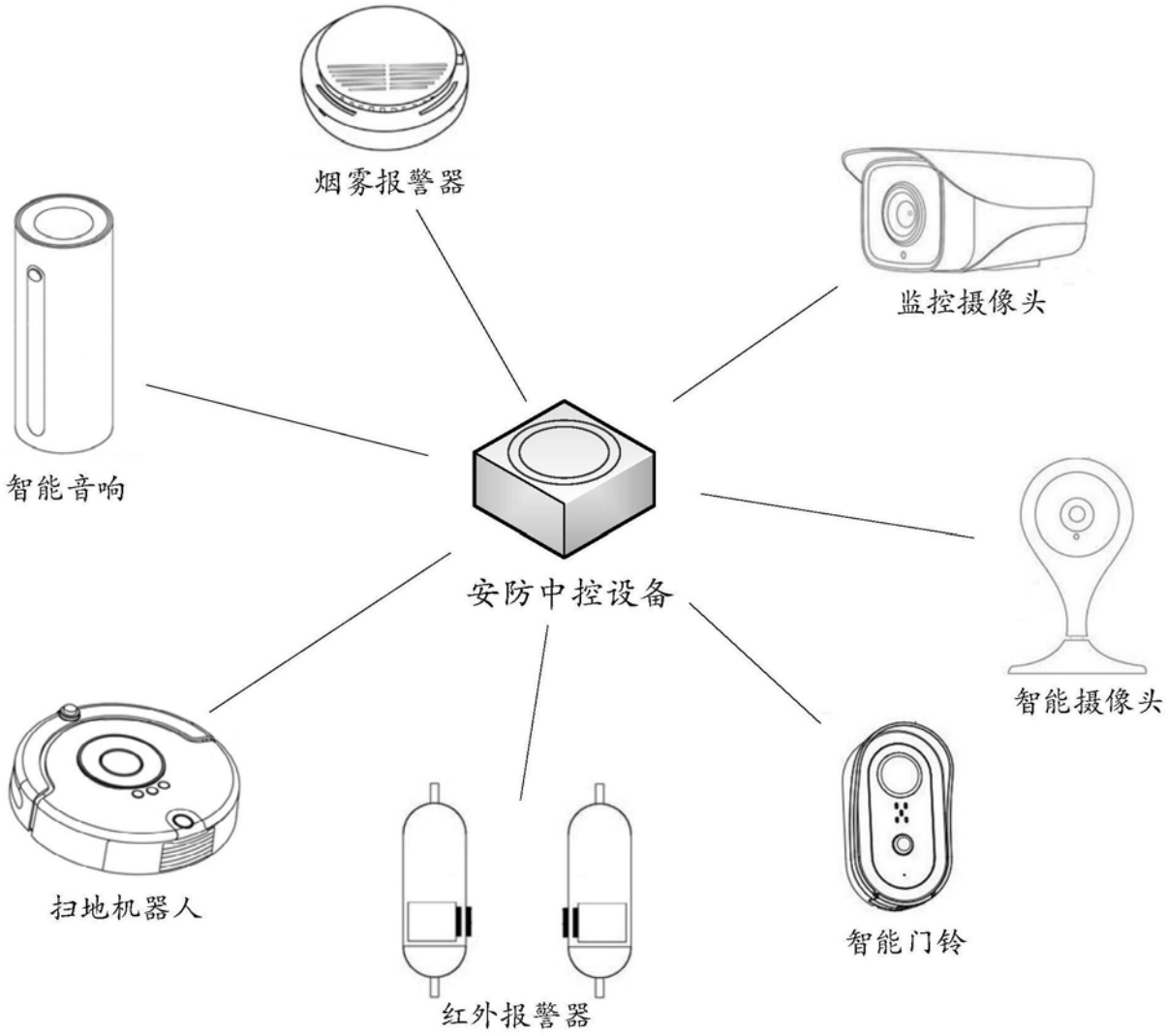


图3