(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 110969738 A
(43)申请公布日 2020.04.07

(21)申请号 202010046515.0

(22)申请日 2020.01.16

(71)申请人 河南国立信息科技有限公司
地址 458030 河南省鹤壁市淇滨区湘江南路北侧钜新路东侧创业创新园孵化楼611室

(72)发明人 朱明甫 马传琦 刘文奇 刁智华 段崇 王士斌 孙鹏 侯青霞 张廷杰 徐赵飞 陈亚飞 刘尚鑫 赵波 罗勇 王贵宾 马新 朱智丹

(74)专利代理机构 郑州优盾知识产权代理有限公司 41125
代理人 张真真

(51)Int.Cl.
G07C 9/20(2020.01)
G07C 9/25(2020.01)
G07C 9/27(2020.01)
H04W 4/70(2018.01)

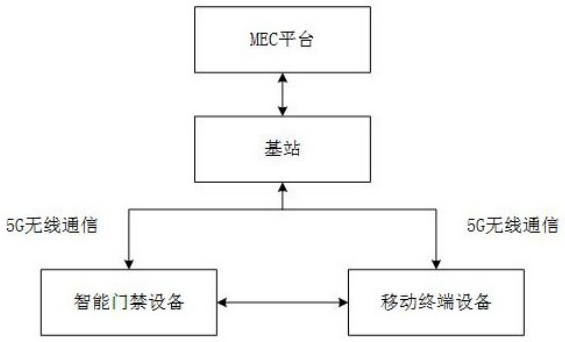
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种基于5G架构的智能安全门禁的控制系统及方法

(57)摘要

本发明提出了一种基于5G架构的智能安全门禁的控制系统及方法，所述控制系统包括MEC平台、5G基站、智能门禁设备和移动终端设备；所述MEC平台与5G基站相连接，5G基站通过5G无线通信分别与智能门禁设备和移动终端设备相连接；移动终端设备通过D2D通信与智能门禁设备相连接。本发明采用5G技术通过移动边缘计算域的就近的、快速的响应能力，提供了统一的更为准确的识别服务，解决了识别水平层次不齐的问题；本发明结合5G中的设备到设备之间的D2D通信方式，在生物识别的同时，增加硬件识别防止伪造欺骗，采用这种软硬结合的方式，能够进一步提高智能安全门禁的安全保障系数。



CN 110969738 A

1.一种基于5G架构的智能安全门禁的控制方法,其特征在于,其步骤如下:

步骤S101:建立移动终端设备与MEC平台的5G通信连接,通过移动终端设备上的APP软件登录控制系统绑定智能门禁设备与移动终端设备的标识,并将移动终端设备与智能门禁设备绑定的标识存储到MEC平台;

步骤S102:利用智能门禁设备或移动终端设备采集用户的生物样本数据,并通过APP软件登录控制系统将生物样本数据存储在MEC平台的用户特征样本库中;

步骤S103:利用智能门禁设备或移动终端设备采集待识别的数据信息,将数据信息上传到MEC平台,在MEC平台上,将数据信息与用户特征样本库中的生物样本数据进行比对,将比对结果反馈到智能门禁设备或移动终端设备;

步骤S104:智能门禁设备或移动终端设备接收到MEC平台的比对结果,如果对比结果正确,智能门禁设备通过D2D通信就近搜索绑定的移动终端设备或者移动终端设备通过D2D通信就近搜索绑定的智能门禁设备,执行步骤S105,否则,智能门禁设备保持上锁状态;

步骤S105:如果智能门禁设备通过D2D通信成功搜索到绑定的移动终端设备或移动终端设备通过D2D通信成功搜索到绑定的智能门禁设备,移动终端设备向智能门禁设备发送开锁指令,智能门禁设备执行门禁开锁指令打开智能锁,否则,智能门禁设备保持上锁状态,完成智能安全门禁的控制。

2.根据权利要求1所述的基于5G架构的智能安全门禁的控制方法,其特征在于,所述智能门禁设备的标识为智能门禁设备的硬件序列号,所述移动终端设备的标识为移动终端设备的硬件序列号。

3.根据权利要求1或2所述的基于5G架构的智能安全门禁的控制系统,其特征在于,包括MEC平台、5G基站、智能门禁设备和移动终端设备;所述MEC平台与5G基站相连接,5G基站通过5G无线通信分别与智能门禁设备和移动终端设备相连接;移动终端设备通过D2D通信与智能门禁设备相连接。

4.根据权利要求3所述的基于5G架构的智能安全门禁控制系统,其特征在于,所述智能门禁设备包括指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块和5G无线通信模块;所述指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块均通过5G无线通信模块与MEC平台相连接,所述指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块均通过5G无线通信模块与移动终端设备相连接。

5.根据权利要求1所述的基于5G架构的智能安全门禁控制系统,其特征在于,所述移动终端设备包括APP软件登录控制系统、采集模块和5G无线通信模块,APP软件登录控制系统和采集模块均通过5G无线通信模块与MEC平台相连接,APP软件登录控制系统通过D2D通信与智能门禁设备相连接。

一种基于5G架构的智能安全门禁的控制系统及方法

技术领域

[0001] 本发明涉及信息与通信技术领域，特别是指一种基于5G架构的智能安全门禁控制系统及方法。

背景技术

[0002] 智能化的安全门禁系统是一种新型现代化的数字化智能安全管理系统，被广泛应用于各类场合，现有智能化技术多采用虹膜、指纹、语音、人脸等生物识别，它不仅能够时刻自动记录人员的出入情况，限制内部人员的出入区域和出入时间，礼貌地拒绝不速之客，同时也将有效地保护财产不受侵犯。智能化的安全门禁系统由于各类技术的技术条件和应用成熟度层次不齐，导致识别差错率较高。此外，单纯的生物识别还存在被假冒伪造的风险。

[0003] 随着5G技术的成熟和推广，采用5G技术通过移动边缘计算域(MEC)的就近的、快速的响应能力，为现有门禁技术存在识别水平层次不齐的问题提供了新的解决方向。

发明内容

[0004] 针对上述背景技术中存在的不足，本发明提出一种基于5G架构的智能安全门禁控制系统及方法，解决了现有智能安全门禁识别技术误差大、技术水平层次不齐，以及单独的生物识别容易被伪造欺骗的技术问题。

[0005] 本发明的技术方案是这样实现的：

一种基于5G架构的智能安全门禁的控制方法，其步骤如下：

步骤S101：建立移动终端设备与MEC平台的5G通信连接，通过移动终端设备上的APP软件登录控制系统绑定智能门禁设备与移动终端设备的标识，并将移动终端设备与智能门禁设备绑定的标识存储到MEC平台；

步骤S102：利用智能门禁设备或移动终端设备采集用户的生物样本数据，并通过APP软件登录控制系统将生物样本数据存储在MEC平台的用户特征样本库中；

步骤S103：利用智能门禁设备或移动终端设备采集待识别的数据信息，将数据信息上传到MEC平台，在MEC平台上，将数据信息与用户特征样本库中的生物样本数据进行比对，将比对结果反馈到智能门禁设备或移动终端设备；

步骤S104：智能门禁设备或移动终端设备接收到MEC平台的比对结果，如果对比结果正确，智能门禁设备通过D2D通信就近搜索绑定的移动终端设备或者移动终端设备通过D2D通信就近搜索绑定的智能门禁设备，执行步骤S105，否则，智能门禁设备保持上锁状态；

步骤S105：如果智能门禁设备通过D2D通信成功搜索到绑定的移动终端设备或移动终端设备通过D2D通信成功搜索到绑定的智能门禁设备，移动终端设备向智能门禁设备发送开锁指令，智能门禁设备执行门禁开锁指令打开智能锁，否则，智能门禁设备保持上锁状态，完成智能安全门禁的控制。

[0006] 所述智能门禁设备的标识为智能门禁设备的硬件序列号，所述移动终端设备的标识为移动终端设备的硬件序列号。

[0007] 一种基于5G架构的智能安全门禁的控制系统，包括MEC平台、5G基站、智能门禁设备和移动终端设备；所述MEC平台与5G基站相连接，5G基站通过5G无线通信分别与智能门禁设备和移动终端设备相连接；移动终端设备通过D2D通信与智能门禁设备相连接。

[0008] 所述智能门禁设备包括指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块和5G无线通信模块；所述指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块均通过5G无线通信模块与MEC平台相连接，所述指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块均通过5G无线通信模块与移动终端设备相连接。

[0009] 所述移动终端设备包括APP软件登录控制系统、采集模块和5G无线通信模块，APP软件登录控制系统和采集模块均通过5G无线通信模块与MEC平台相连接，APP软件登录控制系统通过D2D通信与智能门禁设备相连接。

[0010] 本技术方案能产生的有益效果：本发明采用5G技术通过移动边缘计算域(MEC)的就近的、快速的响应能力，提供了统一的更为准确的识别服务，解决了识别水平层次不齐的问题；本发明结合5G中的设备到设备之间的D2D通信方式，在生物识别的同时，增加硬件识别防止伪造欺骗，采用这种软硬结合的方式，能够进一步提高智能安全门禁的安全保障系数。

附图说明

[0011] 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简单地介绍，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。

[0012] 图1为本发明的系统框图；

图2为本发明的基于5G架构的识别原理图；

图3为本发明的基于5G架构的原理图。

具体实施方式

[0013] 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，所描述的实施例仅仅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付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。

[0014] 实施例1，一种基于5G架构的智能安全门禁控制系统，如图1所示，包括MEC平台、5G基站、智能门禁设备和移动终端设备；所述MEC平台与5G基站相连接，5G基站通过5G无线通信分别与智能门禁设备和移动终端设备相连接；移动终端设备通过D2D通信与智能门禁设备相连接。

[0015] 所述MEC平台，通过5G基站与智能门禁设备建立无线连接，利用5G通信及移动边缘计算MEC平台提供的就近服务，快速响应智能门禁设备发出的生物识别请求，并提供准确的识别服务。

[0016] 所述智能门禁设备包括指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块和5G无线通信模块；所述指纹识别模块是用于采集用户的指纹信息，语音识别模块是用

于采集用户的声音信息，人脸识别模块是用于采集用户的人脸图像信息，虹膜识别模块是用于采集用户的虹膜信息。所述指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块均通过5G无线通信模块与MEC平台相连接，所述指纹识别模块、语音识别模块、人脸识别模块、虹膜识别模块均通过5G无线通信模块与移动终端设备相连接。

[0017] 所述移动终端设备，包括但不限于用户的智能手机设备，移动终端设备搭载无线通信模块，作为硬件设备充当硬件防伪，同时提供智能安全门禁控制系统的交互控制及设定。所述移动终端设备包括APP软件登录控制系统、采集模块和5G无线通信模块，所述采集模块是用于采集用户的生物数据。APP软件登录系统和采集模块均通过5G无线通信模块与MEC平台相连接，APP软件登录控制系统通过D2D通信与智能门禁设备相连接。

[0018] 实施例2，一种基于5G架构的智能安全门禁控制方法，智能门禁设备自带生物识别能力，如图2所示，实施例2中的MEC平台、智能门禁设备和移动终端设备之间的通信均采用5G技术。MEC平台主要提供通用生物识别算法，智能门禁设备通过生物识别硬件采集样本数据，移动终端设备主要作为硬件锁。具体步骤如下：

步骤S201：建立移动终端设备与MEC平台的5G连接关系，通过移动终端设备上的APP软件登录控制系统绑定智能门禁设备与移动终端设备的标识，并将移动终端设备与智能门禁设备绑定的标识存储到MEC平台；其中，智能门禁设备的标识为智能门禁设备的硬件序列号，移动终端设备的标识为移动终端设备的硬件序列号。

[0019] 步骤S202：建立智能门禁设备与MEC平台的5G通信连接，并通过智能门禁设备的指纹识别模块、语音识别模块、人脸识别模块或虹膜识别模块采集用户的生物样本数据，并通过APP软件登录控制系统将生物样本数据存储在MEC平台的用户特征样本库中。

[0020] 步骤S203：经过步骤S201与步骤S202的设置后，当用户需要打开智能安全门禁时，使用智能门禁设备采集待识别的数据信息，将数据信息上传到MEC平台，在MEC平台上，将数据信息与用户特征样本库中的生物样本数据进行比对，将比对结果反馈到智能门禁设备。

[0021] 步骤S204：智能门禁设备接收到MEC平台的比对结果，如果对比结果正确，智能门禁设备通过D2D通信就近搜索绑定的移动终端设备，执行步骤S205，否则，智能门禁设备保持上锁状态。智能门禁设备根据MEC平台系统反馈的比对结果，如果比对结果为不匹配，则拒绝开锁，如果比对结果为匹配，软件识别过程结束。但由于步骤S203中采集的数据信息可能是伪造的指纹或者非法行为下的强制采集行为，则需要进一步的硬件设备防伪识别。因此，为了避免该情况，或者为了增强安全系统，则需要进入步骤S205的硬件设备防伪识别过程；

步骤S205：如果智能门禁设备通过D2D通信成功搜索到绑定的移动终端设备，即找到了硬件防伪信息，如移动终端的CPU的UUID(通用唯一识别码)信息即为该移动终端的硬件防伪信息；结合获取的硬件防伪信息，同时对比步骤S204反馈的软件识别信息，软硬两个条件都满足，则执行开锁指令打开智能锁，否则，智能门禁设备保持上锁状态，完成智能安全门禁的控制。

[0022] 实施例3，一种基于5G架构的智能安全门禁控制方法，智能门禁设备不具备生物识别能力，而是将生物识别能力放置到移动终端设备中，如图3所示，实施例3中的MEC平台、智能门禁设备和移动终端设备之间的通信均采用5G技术。考虑硬件的发展，生物识别元器件缩微化可集成到移动终端设备，原有智能锁的采样功能均可以由移动终端设备完成，从而

避免元器件重复并降低用户成本。在实施例3中，MEC平台主要提供生物识别算法，智能门禁设备集成5G通信模块并提供接收开锁指令和开锁功能，移动终端设备集成了生物采集硬件模块，提供数据采用功能，同时又作为硬件锁。具体步骤如下：

步骤S301：建立移动终端设备与MEC平台的5G连接关系，通过移动终端设备上的APP软件登录控制系统绑定智能门禁设备与移动终端设备的标识，并将移动终端设备与智能门禁设备绑定的标识存储到MEC平台；其中，智能门禁设备的标识为智能门禁设备的硬件序列号，移动终端设备的标识为移动终端设备的硬件序列号。

[0023] 步骤S302：利用移动终端设备的采集模块采集用户的生物样本数据，并通过APP软件登录控制系统将生物样本数据存储在MEC平台的用户特征样本库中。

[0024] 步骤S303：经过步骤S201和步骤S202的设置后，当用户需要打开智能安全门禁时，使用移动终端设备采集待识别的数据信息，将数据信息上传到MEC平台，在MEC平台上，将数据信息与用户特征样本库中的生物样本数据进行比对，将比对结果反馈到移动终端设备。

[0025] 步骤S304：移动终端设备接收到MEC平台的比对结果，如果对比结果正确，移动终端设备通过D2D通信就近搜索绑定的智能门禁设备，执行步骤S305，否则，智能门禁设备保持上锁状态。移动终端设备根据MEC平台系统反馈的比对结果，如果比对结果为不匹配，则开锁失败。如果比对结果为匹配，软件识别过程结束。但由于步骤S302采集的数据信息采样可能是伪造的指纹或者非法行为下的强制采集行为，则需要进一步的硬件设备防伪识别。因此，为了避免该情况，或者为了增强安全系统，则需要进行硬件设备防伪识别过程。

[0026] 步骤S305：如果移动终端设备通过D2D通信成功搜索到绑定的智能门禁设备，即找到了硬件防伪信息，移动终端设备综合对比步骤S304获取的软件识别比对结果信息，如果两个条件都满足，移动终端设备通过D2D通信，直接向智能门禁设备发送开锁指令，智能门禁设备执行门禁开锁指令打开智能锁，否则，智能门禁设备保持上锁状态，完成智能安全门禁的控制。

[0027] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

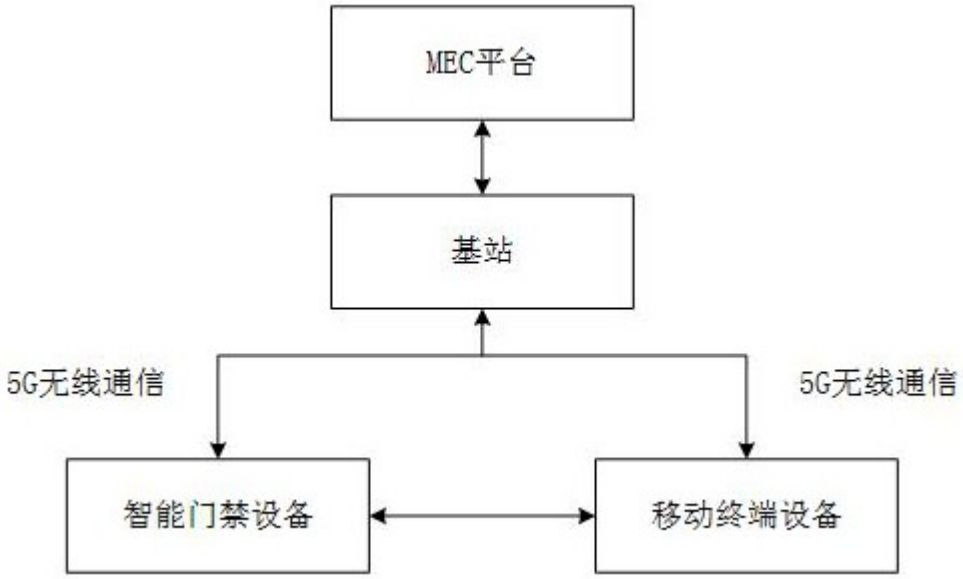

MEC平台
基站
5G无线通信
5G无线通信
智能门禁设备
移动终端设备

图1

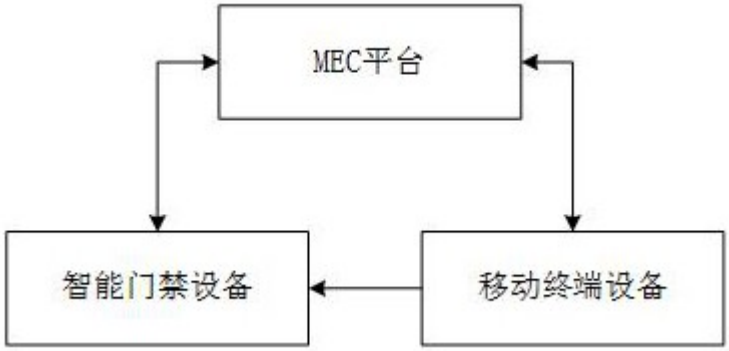

MEC平台
智能门禁设备
移动终端设备

图2

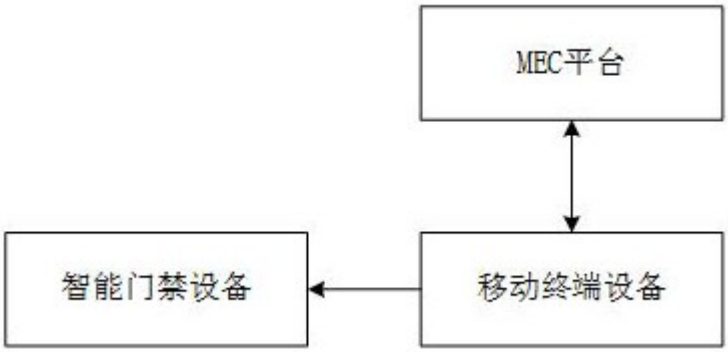

MEC平台
智能门禁设备
移动终端设备

图3