(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 107650863 A
(43)申请公布日 2018.02.02

(21)申请号 201710846252.X

(22)申请日 2017.09.19

(71)申请人 大陆汽车投资(上海)有限公司
地址 200082 上海市杨浦区大连路538号

(72)发明人 游道 张文晖 李文杰 梁龑

(74)专利代理机构 上海华诚知识产权代理有限公司 31300
代理人 徐颖聪

(51)Int.Cl.
B60R 25/23(2013.01)
B60R 25/24(2013.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G07C 9/00(2006.01)

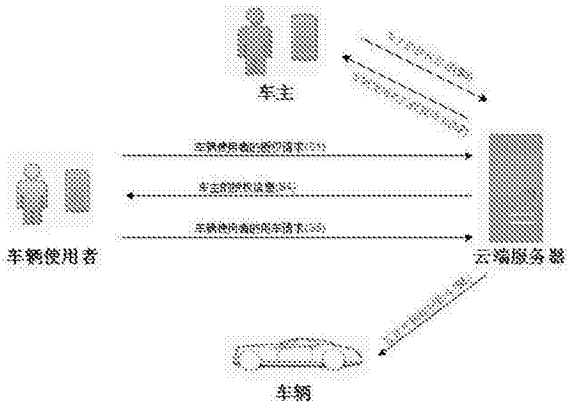
权利要求书2页 说明书6页 附图2页

(54)发明名称

车辆共享方法及系统

(57)摘要

本发明涉及车辆共享方法及系统，并公开了一种车辆共享方法包括：权限请求，包括响应于车辆使用者终端发送的使用车辆的授权请求，云端服务器向车主终端转发所述授权请求并接收车主终端发送的授权信息；及用车请求，包括响应于车辆使用者终端发送的第一车辆控制指令，云端服务器结合所述授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证，并在验证通过后，将与所述第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使所述车辆执行所述第二车辆控制指令。采用所述方法及系统可以无需携带钥匙即可对车辆进行控制，同时避免了传输信号被近距离截获的风险，提高了用车安全性及用户体验。



CN 107650863 A

1.一种车辆共享方法,其特征在于,包括:

权限请求,包括响应于车辆使用者终端发送的使用车辆的授权请求,云端服务器向车主终端转发所述授权请求并接收车主终端发送的授权信息;及

用车请求,包括响应于车辆使用者终端发送的第一车辆控制指令,云端服务器结合所述授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证,并在验证通过后,将与所述第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使所述车辆执行所述第二车辆控制指令。

2.根据权利要求1所述的车辆共享方法,其特征在于,所述权限请求还包括:接收与授权信息一起发送的车主数字证书,并依据所述车主数字证书对所述授权信息进行验证;所述车主数字证书与车主姓名、车主身份证号、车主电话中的一者或其组合对应,保存在云端服务器、车主终端及对应的车辆中。

3.根据权利要求2所述的车辆共享方法,其特征在于,对所述授权信息进行验证包括对车主终端的账户信息及设备信息进行验证。

4.根据权利要求1所述的车辆共享方法,其特征在于,所述授权信息包括车辆使用者身份及与车辆使用者身份对应的车辆控制时限及车辆控制指令的控制权限。

5.根据权利要求1所述的车辆共享方法,其特征在于,云端服务器结合所述授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证,包括:通过身份鉴权确认车辆使用者的身份;以及,验证第一车辆控制指令是否已包含在经确认的、与车辆使用者身份对应的授权信息中。

6.根据权利要求5所述的车辆共享方法,其特征在于,身份鉴权通过下述任一方式或组合:对所述使用者终端发送的数字签名进行验证、对所述使用者终端发送的验证码进行验证。

7.根据权利要求6所述的车辆共享方法,其特征在于,所述数字签名包括车辆使用者姓名、车辆使用者身份证号、车辆使用者电话中的一者或其组合。

8.根据权利要求1所述的车辆共享方法,其特征在于,所述车辆使用者终端将数字签名与所述第一车辆控制指令一起发送至所述云端服务器,或者,依据云端服务器针对第一车辆控制指令发送的身份鉴权请求,向云端服务器发送数字签名。

9.根据权利要求1所述的车辆共享方法,其特征在于,所述用车请求还包括:将所述第二车辆控制指令连同车主数字证书一起发送至对应车辆的车载通信单元中。

10.根据权利要求1所述的车辆共享方法,其特征在于,还包括:响应于所述云端服务器发送的所述第二车辆控制指令,所述车辆开始计时并在超出预设时长且未接收到车辆使用者的执行操作时,禁止响应所述第二车辆控制指令。

11.根据权利要求1所述的车辆共享方法,其特征在于,所述车辆控制指令为车门解锁指令、车门上锁指令、车辆启动指令、后备箱开启指令及后备箱上锁指令中的一者。

12.根据权利要求1所述的车辆共享方法,其特征在于,所述车辆使用者终端、所述车主终端及所述车辆中的任一者采用HTTPS方式与所述云端服务器进行通讯。

13.一种车辆共享系统,其特征在于,还包括:

云端服务器,包括响应于车辆使用者终端发送的第一车辆控制指令,所述云端服务器结合授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证,并在验证通过后,

将与所述第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使所述车辆执行所述第二车辆控制指令;及

车辆,所述车辆与所述云端服务器建立通讯,包括车载通信单元及车载控制单元,所述车载通信单元用于接收云端服务器发送的车辆控制指令,所述车载控制单元响应于所述车载通信单元的指令以执行所述车辆控制指令。

14.根据权利要求13所述的车辆共享系统,其特征在于,所述车载通信单元通过HTTPS方式与所述云端服务器建立通讯。

15.根据权利要求13所述的车辆共享系统,其特征在于,所述授权信息包括车辆使用者身份及与车辆使用者身份对应的车辆控制时限及车辆控制指令的控制权限。

16.根据权利要求13所述的车辆共享系统,其特征在于,云端服务器结合所述授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证,包括:通过身份鉴权确认车辆使用者的身份;以及,验证第一车辆控制指令是否已包含在经确认的、与车辆使用者身份对应的授权信息中。

17.根据权利要求16所述的车辆共享系统,其特征在于,身份鉴权通过下述任一方式或组合:对所述使用者终端发送的数字签名进行验证、对所述使用者终端发送的验证码进行验证。

18.根据权利要求17所述的车辆共享系统,其特征在于,所述数字签名包括车辆使用者姓名、车辆使用者身份证号、车辆使用者电话中的一者或其组合。

19.根据权利要求13所述的车辆共享系统,其特征在于,所述车辆使用者终端将数字签名与所述第一车辆控制指令一起发送至所述云端服务器,或者,依据云端服务器针对第一车辆控制指令发送的身份鉴权请求,向云端服务器发送数字签名。

20.根据权利要求13所述的车辆共享系统,其特征在于,所述车辆控制指令为车门解锁指令、车门上锁指令、车辆启动指令、后备箱开启指令及后备箱上锁指令中的一者。

21.根据权利要求13所述的车辆共享系统,其特征在于,所述车载通信单元还包括计时单元,响应于所述云端服务器发送的所述车辆控制指令,所述计时单元工作并在超出预设时长且未接收到车辆使用者的与所述车辆控制指令对应的执行操作时,禁止响应所述车辆控制指令。

车辆共享方法及系统

技术领域

[0001] 本发明涉及汽车控制技术领域，特别涉及车辆共享方法及系统。

背景技术

[0002] 汽车共享的概念最早起源于美国，从1999年ZiPCAR的上线至今发展近18年，然而，其在市场上却并未得到大规模的普及。近些年，尤其是在中国，随着共享经济的深入人心，共享汽车成为了下一个引爆点，一定程度上解决了城市交通拥堵、限行及停车位饱和的问题，另一方面，也解决了拥有驾照却买不起车人群的出行痛点。

[0003] 无钥匙进入和启动系统(Passive Entry and Passive Start,PEPS)是现有的一种车辆进入启动系统，该系统允许对车辆进行启动及其他操作，而无需使用传统的机械钥匙或者要求使用者做出任何其他明显的解锁动作。

[0004] 一种实现车辆无钥匙进入和启动的方式，即远程车辆控制(Remote Vehicle Control,RVC)，其通过移动通讯网络对车辆进行远程控制，实现智能设备、后台服务器以及车载通讯系统的数据交互，车主亦可以通过智能手机对车辆进行远程上锁、解锁等操作。基于无钥匙启动车辆技术的支持下，进行汽车共享，是未来的发展趋势，其解决了车主分享车辆的“最后一公里”问题。

[0005] 目前，车辆的解锁有如下几种方式：1)射频识别技术(Radio Frequency Identification,RFID)，这是一种非接触式的自动识别技术，其通过射频信号自动识别目标对象并获取相关数据，无须人工干预，且可以工作于任何恶劣环境中，通过汽车上的车载控制模块不断发出低频信号，当携带身份标识模块的车辆使用者在汽车附近时，身份标识模块感应到车载控制模块发出的低频信号，返回带有身份密码信息的信号，车载控制模块感应到该信号并通过身份识别后执行开锁动作；2)蓝牙识别技术，其采用跳频技术以及独特的鉴权和加密技术，相比于射频识别技术，提高了信号传输过程中被破解的难度，当使用者携带的设置有蓝牙芯片的钥匙或具有蓝牙功能的智能手机进入蓝牙的通讯范围内，车辆与钥匙或智能手机之间立即进行身份确认并交换资料，当信号强度达到使用者设定的强度时立即自动解锁，另一方面，使用者也可以在智能手机上安装相应的钥匙应用软件，通过在智能手机屏幕上点击“开锁”等虚拟按钮解锁车辆。

[0006] 然而，上述几种处理方式中：1)通过射频识别的方式解锁，由于通常采用固定密码加密，因而很容易通过中继攻击等方式被截获，缺乏必要的安全保障，另一方面，其对车主是否要进入汽车并没有判断，由于其自动识别的特性，当车辆使用者并不想进入车内而车载控制模块执行开锁操作后，如果车辆使用者没有注意到车已开锁，就会对用车造成安全隐患；2)尽管相比于射频识别技术，采用蓝牙识别技术进行车辆解锁一定程度上提高了安全性，但是其仍然不能避免与车辆进行近场通讯从而解锁车辆的方式，因而仍然存在传输信号被位于其信号范围内的其他设备所截获的安全隐患。

发明内容

[0007] 本发明解决的问题是提出一种车辆共享方法及系统，通过使用云端服务器控制及解锁车辆，免除了用户携带额外的钥匙以解锁车辆的烦恼，同时，由于智能设备与车辆没有直接的沟通，避免了车辆信号被近距离截获的危险，提高了用车安全性。

[0008] 为了解决上述问题，本发明提供一种车辆共享方法包括：

[0009] 权限请求，包括响应于车辆使用者终端发送的使用车辆的授权请求，云端服务器向车主终端转发所述授权请求并接收车主终端发送的授权信息；及

[0010] 用车请求，包括响应于车辆使用者终端发送的第一车辆控制指令，云端服务器结合所述授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证，并在验证通过后，将与所述第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使所述车辆执行所述第二车辆控制指令。

[0011] 本发明还提供一种车辆共享系统包括：

[0012] 云端服务器，包括响应于车辆使用者终端发送的第一车辆控制指令，所述云端服务器结合授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证，并在验证通过后，将与所述第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使所述车辆执行所述第二车辆控制指令；及

[0013] 车辆，所述车辆与所述云端服务器建立通讯，包括车载通信单元及车载控制单元，所述车载通信单元用于接收云端服务器发送的车辆控制指令，所述车载控制单元响应于所述车载通信单元的指令以执行所述车辆控制指令。

[0014] 与现有技术相比，上述方案具有以下优点：

[0015] 当智能设备与云端服务器建立通信连接后，由云端服务器完成与车主的授权认证，在授权期间，云端服务器根据车辆使用者的用车请求，控制车辆的解锁与上锁，从而可以无需携带钥匙即可对车辆进行控制，同时避免了智能设备与车辆之间的直接沟通。由于云端服务器可以设置特殊的安全协议，因而其安全性较近距离通讯高，也不存在传输信号被近距离截获的风险。

附图说明

[0016] 本发明的其他细节及优点将通过下文提供的详细描述而变得显而易见。下文将参照附图来进行详细描述，其中：

[0017] 图1是本发明车辆共享方法的一种实现示意图；

[0018] 图2是本发明车辆共享方法的一种用车请求实施例流程图。

具体实施方式

[0019] 在下面的描述中，阐述了许多具体细节以便使所属技术领域的技术人员更全面地了解本发明。但是，对于所属技术领域内的技术人员明显的是，本发明的实现可不具有这些具体细节中的一些。此外，应当理解的是，本发明并不限于所介绍的特定实施例。相反，可以考虑用下面的特征和要素的任意组合来实施本发明，而无论它们是否涉及不同的实施例。因此，下面的方面、特征、实施例和优点仅作说明之用而不应被看作是权利要求的要素或限定，除非在权利要求中明确提出。

[0020] 根据本发明的车辆共享方法一种实施方式，其包括：

[0021] 权限请求，包括响应于车辆使用者终端发送的使用车辆的授权请求，云端服务器向车主终端转发所述授权请求并接收车主终端发送的授权信息；及

[0022] 用车请求，包括响应于车辆使用者终端发送的第一车辆控制指令，云端服务器结合所述授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证，并在验证通过后，将与所述第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使所述车辆执行所述第二车辆控制指令。

[0023] 以下结合附图对本发明的一种车辆共享方法进一步举例说明。参照图1所示，以车辆共享方法为例，一共分为两部分，分别为权限请求过程，包括步骤S1至S4，以及用车请求过程，包括步骤S5至S6。

[0024] 对车主而言，可以通过使用智能设备安装特定的软件应用(APP)事先在云端服务器注册账号并输入姓名、手机号、身份证号、需要绑定的车辆识别码及车辆信息等一系列相关信息之后，云端服务器会接收到APP端发送的信息，并通过第三方数字证书认证机构生成车主数字证书，除了在云端服务器中保留该车主数字证书外，还将该数字证书分别发送至车主及车辆用于后续车辆共享时的匹配验证，完成上述步骤后，车主便有资格通过车主终端将车辆通过云端服务器共享给其他车辆使用者。对车辆使用者而言，可以通过使用智能设备安装特定的软件应用(APP)或者是通过网页端访问特定网址，完成注册及相关信息输入、认证之后获得账号及密码信息，随后，车辆使用者终端通过第三方数字证书认证机构获得车辆使用者数字证书，及与之对应的唯一的数字签名，云端服务器通过数据交互保存该车辆使用者数字证书，当车辆使用者需要发送用车请求时，将数字签名连同车辆控制指令一起发送至云端服务器，后者通过车辆使用者数字证书对该数字签名及车辆控制指令进行验证，以确保该车辆控制指令发送者的身份并执行相应的指令，完成上述步骤后，就可以使用车辆共享业务。

[0025] 每次使用车辆共享业务时，车辆使用者都要首先完成授权请求，从车主处获得相应的用车权限及时限，然后在给定的用车时限内有用车需求时，向云端服务器发送用车请求，云端服务器根据预先设定的用车权限和时限判断用车请求的合法性，在验证通过之后向车辆发送相应的指令以使车辆执行相应的操作，具体过程如下：

[0026] 步骤S1：车辆使用者终端发送授权请求至云端服务器。

[0027] 具体地，车辆使用者通过车辆使用者终端的APP端或者网页端，将指定车辆的用车请求发送至云端服务器。

[0028] 步骤S2：云端服务器转发车辆使用者终端发送的授权请求至车主终端。

[0029] 云端服务器，包括汽车远程服务提供商(TSP)后台，后者在这个过程中为车辆使用者及车主提供了一个通讯中转站，启到上传下达的作用。在步骤S2中，云端服务器仅在收到车辆使用者终端发送的授权请求后，转发至与之匹配的车主终端。

[0030] 步骤S3：云端服务器接收与授权信息一起发送的车主数字证书，并依据车主数字证书对授权信息进行验证。

[0031] 车主数字证书与车主姓名、车主身份证号、车主电话中的一者或其组合对应，保存在云端服务器、车主终端及对应的车辆中用于匹配验证。车主数字证书具有有效期内，在有效期内，可以用于后续多次车辆共享请求时的验证操作，当设定的车主数字证书时限到期之后，此次生成的车主数字证书自动失效，如果需要再次共享车辆，需要再次申请车主数字

证书。

[0032] 为了增强上述过程的安全性，云端服务器对该授权信息进行验证时还可以包括对车主终端的账户信息及设备信息进行验证。上述验证可以用于验证车主的账户信用历史等信息以确保车辆共享体系安全稳健的发展，例如，如果车主在发送授权信息时，其账户存在违法历史或者不良历史，除非车主在发送确认授权信息前弥补上述不良记录或者以一定的方式做出承诺，否则云端服务器可以选择拒绝接收车主的授权信息。

[0033] 其中，授权信息包括车辆使用者身份及与车辆使用者身份对应的车辆控制时限及车辆控制指令的控制权限，由车主在收到授权请求的时候决定是否授权及授权的内容。车主的授权时间及授权的权限根据实际的应用场景决定，以小时或者天、月为范围，在一定的场合，也可以根据车辆使用者的要求进行授权。

[0034] 步骤S4：云端服务器将车主的授权信息发送至车辆使用者终端。

[0035] 上述授权请求(S1至S4)仅需完成一次，在之后的授权期间内，车辆使用者可以任意多次向云端服务器发送用车请求。

[0036] 步骤S5：当有用车需求时，车辆使用者终端发送第一车辆控制指令至云端服务器。

[0037] 车辆控制指令为车门解锁指令、车门上锁指令、车辆启动指令、后备箱开启指令及后备箱上锁指令中的一者，车辆使用者能够使用的车辆控制指令范围，即控制权限，根据车主在授权时设定的范围而有所不同。

[0038] 步骤S6：云端服务器响应于车辆使用者终端发送的第一车辆控制指令，结合授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证，并在验证通过后，将与第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使车辆执行第二车辆控制指令。

[0039] 云端服务器结合授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证，包括：通过身份鉴权确认车辆使用者的身份；以及，验证第一车辆控制指令是否已包含在经确认的、与车辆使用者身份对应的授权信息中。身份鉴权通过下述任一方式或组合：对所述使用者终端发送的数字签名进行验证、对所述使用者终端发送的验证码进行验证。

[0040] 数字签名与车辆使用者数字证书相匹配，由第三方数字认证机构生成，数字签名可以包括车辆使用者姓名、车辆使用者身份证号、车辆使用者电话中的一者或其组合，也可以包括其他信息，以一定方式加密而成，用于确认车辆使用者身份的唯一性。车辆使用者数字证书保存在云端服务器及车辆使用者终端中，数字签名是唯一的，云端服务器接收到带有数字签名的车辆控制指令时，用保存在云端服务器的车辆使用者数字证书进行验证。上述方式中，车辆使用者终端可以将数字签名与第一车辆控制指令一起发送至云端服务器，或者，依据云端服务器针对第一车辆控制指令发送的身份鉴权请求，向云端服务器发送数字签名。

[0041] 验证码的比对是指，如果车辆使用者使用的是手机，就可以通过发送短信验证到手机，由于短信验证码具有时效性及唯一性，可以有效验证车辆使用者的身份，防止车辆的二次共享。当然，也可以是其他方式的验证码，本发明对此不作限制。

[0042] 具体地，步骤S6还包括第二车辆控制指令连同车主数字证书一起发送至对应车辆的车载通信单元中，便于后续车辆接收由云端发送的车辆控制指令时进行合法性验证。

[0043] 出于安全性的考量，上述提及的车辆使用者终端、车主终端及车辆中的任一者借助3G、4G等无线网络通信模式采用HTTPS方式与云端服务器进行通讯。

[0044] 上述过程中，无论是车主终端还是车辆使用者终端，每完成一个操作指令，网页端或APP端都会有相应的操作提示，特别地，当车主终端在提交授权信息前后以及车辆使用者在获得车主授权信息的前后，网页端或APP端的用户界面(UI)有不同的风格展示，具体用户界面的展示方式，本发明不做限定。

[0045] 由此可见，当智能设备与云端服务器建立通信连接后，由云端服务器完成与车主的授权认证，在授权期间，云端服务器根据车辆使用者的用车请求，控制车辆的解锁与上锁，从而可以无需携带钥匙即可对车辆进行控制，同时避免了智能设备与车辆之间的直接沟通。由于云端服务器可以设置特殊的安全协议，因而其安全性较近距离通讯高，也不存在传输信号被近距离截获的风险。

[0046] 参照图2所示，以发送车辆解锁的用车请求为例，通过下述方式设置：

[0047] (1)当车辆使用者需要解锁车门时，通过APP或者网页端连同数字签名一起向云端服务器发送第一解锁指令。

[0048] (2)云端服务器接收到第一解锁指令时，将车辆使用者数字证书与第一解锁指令及数字签名进行匹配验证，即使用车辆使用者数字证书与数字签名进行匹配验证，以确保车辆使用者身份的真实性及有效性，以及，该指令在从车辆使用者终端到云端服务器的传输过程中没有被拦截及篡改。再者，云端服务器将第一解锁指令与车主授权的授权信息进行匹配验证，以确保该车辆使用者的控制权限允许其发送第一解锁指令。

[0049] (3)在所有的匹配验证通过后，云端服务器发送与第一解锁指令对应的且以一定通信协议使得车辆可以识别的第二解锁指令至车主注册时候绑定的需要共享的车辆，具体来说，是车辆的车载通信单元中。

[0050] (4)车辆的车载通信单元，即T-Box，接收到云端服务器发送的第二解锁指令之后，先判断该指令的合法性，可以是通过移动供应商向车主发送短信验证码以验证第二解锁指令的合法性。另外，也可以通过验证已经保存的车主数字证书与此次指令发送时的车主数字证书是否匹配以判断该指令的合法性。当然，也可以是其他的判断方式，在此不做限定。

[0051] (5)T-Box在判断接收到合法的第二解锁指令之后，唤醒整车的CAN网络并通过CAN网络将第二解锁指令发送至BCM。BCM在接收到上述指令后，对该指令的有效性进行鉴权处理。T-Box及BCM中预先存储有相互匹配的密钥，鉴权处理主要是在BCM接收到控制指令后，将自身的密钥与T-Box中的密钥进行比对，从而判断密钥的真实性，以避免因故障等干扰造成的对第二解锁指令的干扰。

[0052] (6)当T-Box获取BCM鉴权成功的结果之后，向BCM发送第二解锁指令使其解锁车门，以及，T-Box中的计时单元开始计时。另外，T-Box也可以在接收到云端服务器发送的第二解锁指令时开始计时。对于何时开始计时，本发明不做限定。

[0053] (7)T-Box将获取的BCM发送的有关车门已解锁的执行结果发送至云端服务器，并由云端服务器转发来自车辆的执行结果以通知车辆使用者该车辆可以正常使用。

[0054] (8)当T-Box判断计时单元中的时长超出预设的时间且未接收到车辆使用者的开门动作时，禁止第二解锁指令并使车辆再次上锁，上述超时落锁的设置可以在一定程度上降低用车的安全隐患及车辆被盗的风险。

[0055] 上述描述仅围绕解锁指令进行展开，其他的车辆控制指令如车门上锁指令、车辆启动指令、后备箱开启指令及后备箱上锁指令等与上述控制方式可以参照车辆解锁指令的

方式执行，在此不作赘述。

[0056] 由此可见，上述用车请求的方式极大的提高了用车效率及用户体验，当用户需要长时间使用车辆时，由于云端服务器已经存储有车主对于此次车辆共享的授权信息，因而当第一次授权完成后，在授权期间内，都无需在每次需要解锁车辆时进行车主的授权认证，从而避免了重复授权。

[0057] 根据本发明的车辆共享系统的一种实施方式(附图中未示出)，其包括：

[0058] 云端服务器，包括响应于车辆使用者终端发送的第一车辆控制指令，云端服务器结合授权信息对车辆使用者的身份与第一车辆控制指令进行匹配验证，并在验证通过后，将与第一车辆控制指令对应的第二车辆控制指令发送至对应车辆以使车辆执行第二车辆控制指令；及

[0059] 车辆，车辆与云端服务器建立通讯，包括车载通信单元及车载控制单元，车载通信单元用于接收云端服务器发送的车辆控制指令，车载控制单元响应于车载通信单元的指令以执行车辆控制指令。

[0060] 具体地，车辆控制指令为车门解锁指令、车门上锁指令、车辆启动指令、后备箱开启指令及后备箱上锁指令中的一者。车辆控制指令的权限范围由车主在授权时决定。

[0061] 具体地，车载通信单元还包括计时单元，响应于云端服务器发送的车辆控制指令，计时单元工作并在超出预设时长且未接收到车辆使用者的与车辆控制指令对应的执行操作时，禁止响应车辆控制指令。

[0062] 车辆共享系统的其他内容，包括云端服务器对车辆控制指令进行验证方式等参照前述实施例，此处不再赘述。

[0063] 本领域技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序指令由相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：ROM、RAM、磁盘或光盘等。

[0064] 虽然本发明已以较佳实施例披露如上，但本发明并非限定于此。任何本领域技术人员，在不脱离本发明的精神和范围内所作的各种更动与修改，均应纳入本发明的保护范围内，因此本发明的保护范围应当以权利要求所限定的范围为准。

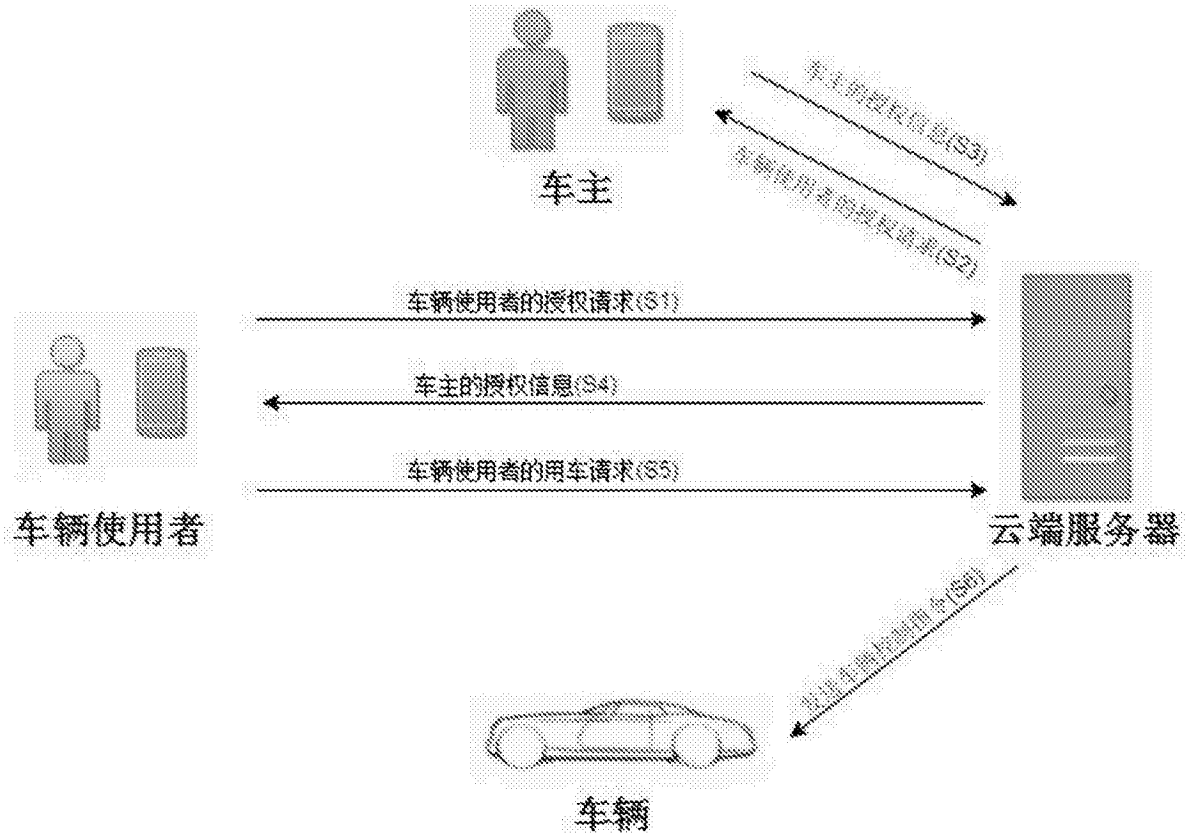


图1

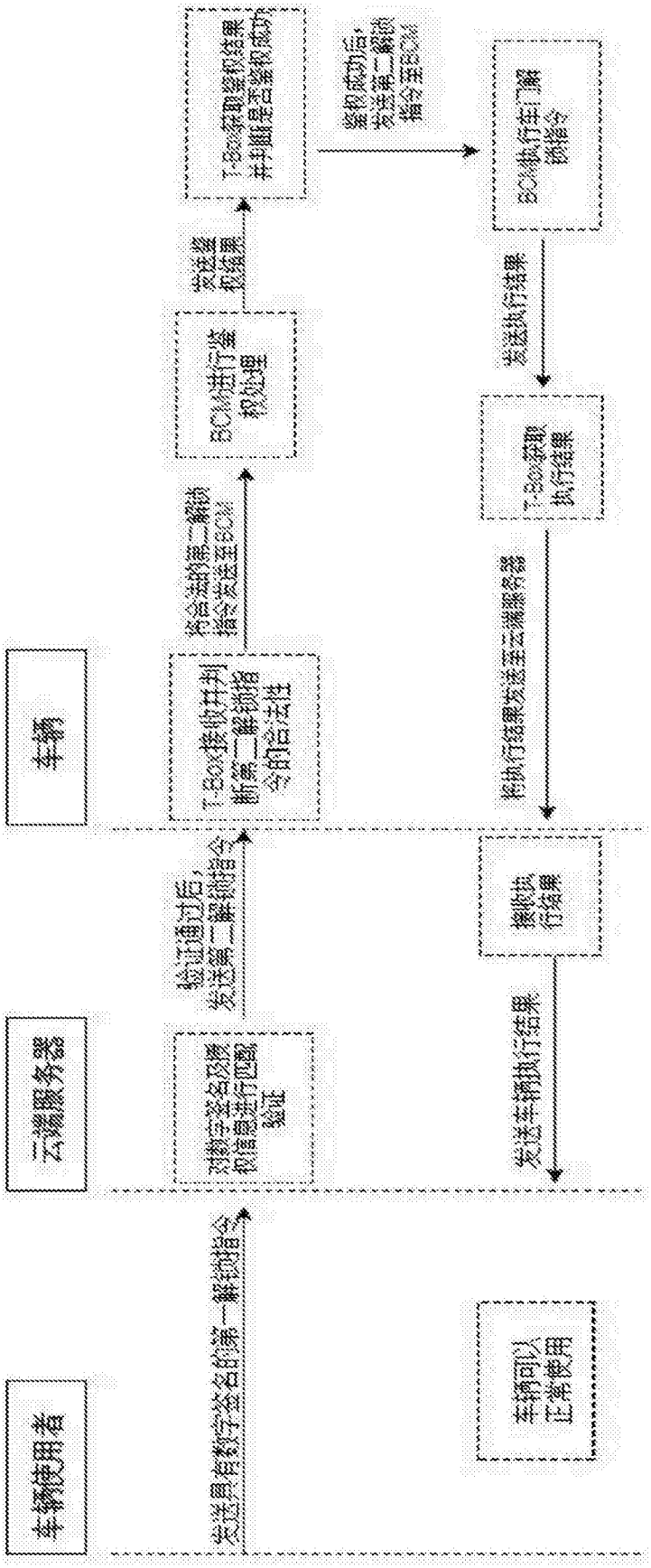

车辆使用者
云端服务器
车辆
发送具有数字签名的第一解锁指令
对数字签名及携带信息进行匹配验证
验证通过后，发送第二解锁指令
T-Box接收并判断第二解锁指令的合法性
符合法的第二解锁指令发送至ECM
ECM进行第二解锁权限处理
发送第二解锁结果
T-Box获取鉴权结果并判断是否鉴权成功
鉴权成功后，发送第二解锁指令至ECM
ECM执行车门解锁指令
发送执行结果
T-Box获取执行结果
将执行结果发送至云端服务器
接收执行结果
发送车辆执行结果
车辆可以正常使用

图2