(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 112804364 B
(45)授权公告日 2021.06.22

(21)申请号 202110385948.3

(22)申请日 2021.04.12

(65)同一申请的已公布的文献号
申请公布号 CN 112804364 A

(43)申请公布日 2021.05.14

(73)专利权人 南泽(广东)科技股份有限公司
地址 510700 广东省广州市黄埔区伴河路96号自编一栋2层203-A房

(72)发明人 郑晓璇

(74)专利代理机构 深圳至诚化育知识产权代理事务所(普通合伙) 44728
代理人 刘英

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 110990507 A,2020.04.10
CN 111882008 A,2020.11.03
CN 109788002 A,2019.05.21
CN 112399370 A,2021.02.23
CN 101416223 A,2009.04.22
US 2018336040 A1,2018.11.22
US 2019266346 A1,2019.08.29
赖成喆等.面向车队的安全且具备隐私保护的移动性管理框架.《信息网络安全》.2018,
罗章华.物联网技术在车辆管理中的运用.《电子世界》.2017,
Zhifei Wang等.Privacy-Protecting Reputation Management Scheme in IoV-based Mobile Crowdsensing.《IEEE》.2021,

审查员 罗恒

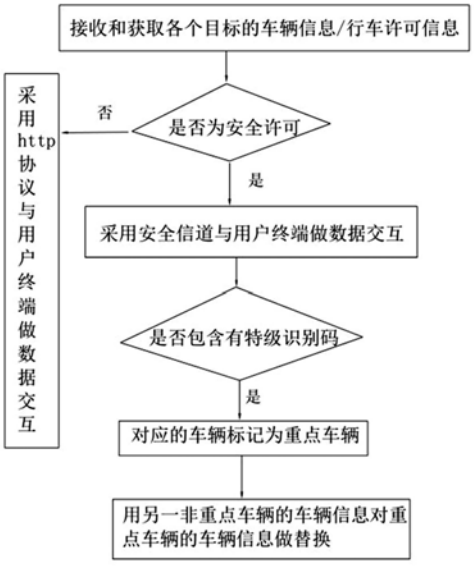
权利要求书1页 说明书5页 附图2页

(54)发明名称

公务用车安全管控方法及系统

(57)摘要

本发明公开了一种公务用车安全管控方法及系统,其包括公务用车安全管控方法:接收和获取各个目标的车辆信息和行车许可信息,并判断是否为安全许可,如果是,则采用安全信道与用户终端做数据交互;采用安全信道包括:通过https协议建立与预设的http协议页面的数据交互;https协议页面获取用户身份信息及访问时间;通过http协议从预设的https协议页面接收和获取用户身份信息及访问时间,验证用户身份信息是否符合,如果是,则累计访问时间与预设的T1许可时长,得到安全时间度长,并在安全时间度长内传输目标车辆信息至预设的https协议页面。本申请具有提高公务车监管的信息安全性的效果。



CN 112804364 B

1.一种公务用车安全管控方法,其特征在于,包括:

接收和获取各个目标的车辆信息;以及接收和获取行车许可信息,并判断是否为安全许可,如果是,则采用安全信道与用户终端做数据交互;如果否,则采用http协议与用户终端做数据交互;

其中,所述车辆信息包括车辆识别信息和位置信息;所述行车许可信息包括用于匹配目标车辆的车辆识别码、用车人身份信息以及许可识别码,所述许可识别码分为多类且至少一类为一级识别码,一类为二级识别码,一类为特级识别码;所述安全许可为:行车许可信息包含有二级识别码或特级识别码;

所述采用安全信道包括:

通过https协议建立与预设的http协议页面的数据交互;

https协议页面获取用户身份信息及访问时间;以及通过http协议从预设的https协议页面接收和获取用户身份信息及访问时间,验证用户身份信息是否符合,如果是,则累计访问时间与预设的T1许可时长,得到安全时间度长,并在安全时间度长内传输目标车辆信息至预设的https协议页面;

当所述行车许可是安全许可,判断行车许可信息是否包含有特级识别码,如果是,则将对应的车辆标记为重点车辆,并用另一非重点车辆的车辆信息对重点车辆的车辆信息做替换。

2.根据权利要求1所述的公务用车安全管控方法,其特征在于:所述用户身份信息包括账号信息及密码信息,且设置为调用WCF服务对传输信息加密,所述调用WCF服务对传输信息加密包括:

根据预设提供 WCF 服务的类;

确定所需解密的用户身份信息;以及,

根据预设的解/加密方式,处理用户身份信息并重新加密处理产生的信息,加密后所得到的流转换成字节数组,再用Base64编码将其转换为处理后字符串,处理后字符串作为用户身份信息于安全时间度长内通过http协议传输至与之建立连接的https协议页面。

3.根据权利要求2所述的公务用车安全管控方法,其特征在于:所述解/加密方式包括在重新加密的过程中通过使用基于HMACSHA1 的伪随机数生成器,实现基于密码的密钥派生功能,通过密码和 salt派生密钥。

4.根据权利要求1所述的公务用车安全管控方法,其特征在于:所述目标车辆的位置信息的获取包括:接收目标车辆车载单元发送的位置信息,所述位置信息由车载单元从卫星定位系统接收定位信息处理得到。

5.根据权利要求1所述的公务用车安全管控方法,其特征在于,还包括:

统计各个目标车辆的行车时间,并生成用车时间排名表;以及接收和获取各个目标车辆的维修时间、原因以及次数,并汇总形成车辆维修记录;

所述用车时间排名表和车辆维修记录均采用http协议与用户终端做数据交互。

6.一种公务用车安全管控系统,包括车载单元、后台及用户终端,其特征在于:所述后台包括存储器和处理器,所述存储器上存储有能够被处理器加载并执行如权利要求1-5中任一种方法的计算机程序。

公务用车安全管控方法及系统

技术领域

[0001] 本申请涉及车辆管控技术领域,尤其是涉及一种公务用车安全管控方法及系统。

背景技术

[0002] 政府单位为人民服务,但出现一些情况时,难免会影响在人民群众心中的印象,例如:公务车私用是最常出现的,有的工作人员公车去做私人事情,甚至的不良驾驶,醉酒、超速等,造成不好的社会影响;另外政府单位的公务车还有管理使用混乱、超编,导致有的车辆被闲置,使用效率低下,资源浪费。

[0003] 市场上目前有出现数字化行政后勤管理平台,依靠强大的数据化、智能化的功能全面覆盖公务车使用的方方面面,让公务车的使用更加便利,现有的公务车管理系统存在以下缺点:信息安全差,公务人员出行信息易暴露,存在安全隐患。

发明内容

[0004] 为了提高公务车监管的信息安全性,本申请提供一种公务用车安全管控方法及系统。

[0005] 第一方面,本申请提供一种公务用车安全管控方法,采用如下的技术方案:

[0006] 一种公务用车安全管控方法,包括:

[0007] 接收和获取各个目标的车辆信息;以及接收和获取行车许可信息,并判断是否为安全许可,如果是,则采用安全信道与用户终端做数据交互;如果否,则采用http协议与用户终端做数据交互;

[0008] 其中,所述车辆信息包括车辆识别信息和位置信息;所述行车许可信息包括用于匹配目标车辆的车辆识别码、用车人身份信息以及许可识别码,所述许可识别码分为多类且至少一类为一级识别码,一类为二级识别码,一类为特级识别码;

[0009] 所述安全许可为:行车许可信息包含有二级识别码或特级识别码;

[0010] 所述采用安全信道包括:

[0011] 通过https协议建立与预设的http协议页面的数据交互;

[0012] https协议页面获取用户身份信息及访问时间;以及通过http协议从预设的https协议页面接收和获取用户身份信息及访问时间,验证用户身份信息是否符合,如果是,则累计访问时间与预设的T1许可时长,得到安全时间度长,并在安全时间度长内传输目标车辆信息至预设的https协议页面;

[0013] 当所述行车许可是安全许可,判断行车许可信息是否包含有特级识别码,如果是,则将对应的车辆标记为重点车辆,并用另一非重点车辆的车辆信息对重点车辆的车辆信息做替换。

[0014] 可选的,所述用户身份信息包括账号信息及密码信息,且设置为调用WCF服务对传输信息加密,所述调用WCF服务对传输信息加密包括:

[0015] 根据预设提供 WCF 服务的类;

[0016] 确定所需解密的用户身份信息；

[0017] 根据预设的解/加密方式，处理用户身份信息并重新加密处理产生的信息，加密后所得到的流转换成字节数组，再用Base64编码将其转换为处理后字符串，处理后字符串作为用户身份信息于安全时间度长内通过http协议传输至与之建立连接的https协议页面。

[0018] 可选的，所述解/加密方式包括在重新加密的过程中通过使用基于HMACSHA1 的伪随机数生成器，实现基于密码的密钥派生功能，通过密码和 salt派生密钥。

[0019] 可选的，所述目标车辆的位置信息的获取包括：接收目标车辆车载单元发送的位置信息，所述位置信息由车载单元从卫星定位系统接收定位信息处理得到。

[0020] 可选的，还包括：

[0021] 统计各个目标车辆的行车时间，并生成用车时间排名表；以及接收和获取各个目标车辆的维修时间、原因以及次数，并汇总形成车辆维修记录；

[0022] 所述用车时间排名表和车辆维修记录均采用http协议与用户终端做数据交互。

[0023] 第二方面，本申请提供一种公务用车安全管控系统，采用如下的技术方案：

[0024] 一种公务用车安全管控系统，包括车载单元、后台及用户终端，所述后台包括存储器和处理器，所述存储器上存储有能够被处理器加载并执行如上述任一种方法的计算机程序。

[0025] 综上所述，本申请包括以下至少一种有益技术效果：

[0026] 1、根据行车许可信息是否为安全许可，分两种方式与用户终端做数据交互；当是安全许可时，通过https协议通信，且根据T1许可时长，设有允许访问时间，以提高信息安全；

[0027] 2、调用WCF服务对传输信息加密，更新用户身份信息，从而进一步提高信息安全；

[0028] 3、将行车许可信息中的行车许可码分出特级识别码，并将其对应的车辆标位重点车辆，将其车辆信息和非重点车辆做调换，以“掩护”重点车辆出行，从而进一步提高信息安全。

附图说明

[0029] 图1是本申请一个实施例的方法流程图；

[0030] 图2是本申请另一个实施例的系统框图。

具体实施方式

[0031] 以下结合附图对本申请作进一步详细说明。

[0032] 本申请实施例公开一种公务用车安全管控方法，其可选择通过服务器实现。参照图1，公务用车安全管控方法包括：

[0033] 接收和获取各个目标的车辆信息；以及接收和获取行车许可信息，并判断是否为安全许可，如果是，则采用安全信道与用户终端做数据交互；如果否，则采用http协议与用户终端做数据交互。

[0034] 其中，车辆信息由车载单元(如：车载主机)发送至实现本方法的服务器；车辆信息包括车辆识别信息和位置信息，车辆识别信息由工作人员人工录入车载单元，以用于识别各个车辆；位置信息可以为：车载单元根据从卫星定位系统接收的定位信息处理得到，如：

车载GPS定位单元接收GPS卫星、北斗卫星发送的定位信号并处理得到经纬度信息;还如:车载单元通过收发器从导航系统(高德地图、百度地图等)获取位置信息。

[0035] 上述行车许可信息包括用于匹配目标车辆的车辆识别码、用车人身份信息以及许可识别码;其中,许可识别码分为多类,且一类为一级识别码,一类为二级识别码,一类为特级识别码 ;上述安全许可为:行车许可信息包含有二级识别码或特级识别码。

[0036] 使用时,用户通过用户终端(如:Web浏览器对应的硬件设备)访问服务器,以获取车辆信息,知悉各个目标车辆的位置;相应的要求,用户访问服务器需要输入用户身份信息,其包括账号和密码;当用户身份信息匹配预设的权限库中入档的用户身份信息,则允许访问,从而实现初步的信息安全管控。

[0037] 根据上述可知,本申请出于信息安全考虑,还根据行车许可信息是否为安全许可将用户终端访问方式分为两类;

[0038] 其中,当行车许可信息不含有二级识别码或特级识别码,即为非安全许可,此时用户终端采用http协议与服务器做数据交互; http协议为超文本传输协议,其为明文方式发送内容,不提供数据加密,相对而言,信息安全性较差,其一般用于公务车日常使用过程,例如:街道/园区走访等环境。

[0039] 当行车许可信息包含二级识别码或特级识别码,此时用户终端采用安全信道与服务器做数据交互,该环节包括:

[0040] 通过https协议建立与预设的http协议页面的数据交互;

[0041] https协议页面获取用户身份信息及访问时间;以及通过http协议从预设的https协议页面接收和获取用户身份信息及访问时间,验证用户身份信息是否符合,如果是,则累计访问时间与预设的T1许可时长,得到安全时间度长,并在安全时间度长内传输目标车辆信息至预设的https协议页面。

[0042] 首先,https是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议,而非常态传输的http协议的明文传输,因此其相对不易被直接抓包获取信息,也更为安全;

[0043] 其次,上述第二种数据交互方式,其并非单纯的https协议通信,还选择通过http协议的页面做跳转,即用户可通过https登录访问,再跳转http协议的页面做访问,从而提高数据交互的流畅性;

[0044] 再次,第二种数据交互方式设定有T1(如:2分钟)许可时长,并根据每次的访问时间分别确定安全时间度长,只有在此时间内才会将目标车辆信息发送至https协议页面,以进一步提高信息安全。

[0045] 为了更进一步提高信息安全性,本申请还选择调用WCF服务对传输信息加密,调用WCF服务对传输信息加密包括:

[0046] 根据预设提供 WCF 服务的类;

[0047] 即“ [ServiceContract]

[0048] [AspNetCompatibilityRequirements(RequirementsMode=AspNetCompatibilityRequirementsMode.Allowed)]

[0049] public class WCFService”

[0050] 确定所需解密的用户身份信息;

[0051] 根据预设的解/加密方式,处理用户身份信息并重新加密处理产生的信息,加密后

所得到的流转换成字节数组，再用Base64编码将其转换为处理后字符串，处理后字符串作为用户身份信息于安全时间度长内通过http协议传输至与之建立连接的https协议页面。

[0052] 其中，解/加密方式包括在重新加密的过程中通过使用基于HMACSHA1 的伪随机数生成器，实现基于密码的密钥派生功能，通过密码和 salt派生密钥，即对每次的用户身份信息及对应信息做更新。

[0053] 解/加密简易示例：

[0054] /// 解密数据

[0055] public string Decrypt(string input)

[0056] {

[0057] // 盐值(与加密时设置的值一致)

[0058] string saltValue = "saltValue";

[0059] // 密码值(与加密时设置的值一致)

[0060] string pwdValue = "pwdValue";

[0061] byte[]encryptBytes = Convert.FromBase64String(input);

[0062] byte[] salt = Encoding.UTF8.GetBytes(saltValue);

[0063] AesManaged aes = new AesManaged();

[0064] Rfc2898DeriveBytes rfc = new Rfc2898DeriveBytes(pwdValue, salt);

[0065] aes.BlockSize = aes.LegalBlockSizes[0].MaxSize;

[0066] aes.KeySize = aes.LegalKeySizes[0].MaxSize;

[0067] aes.Key = rfc.GetBytes(aes.KeySize / 8);

[0068] aes.IV = rfc.GetBytes(aes.BlockSize / 8);

[0069] 后续，用当前的 Key 属性和初始化向量 IV 创建对称解密器对象，得到解密后的输出，再将解密后的目标流与解密转换相连接，将一个字节序列写入当前 CryptoStream(完成解密的过程)。

[0070] }

[0071] /// 加密数据

[0072] private string Encrypt(string input)

[0073] {

[0074] // 盐值

[0075] string saltValue = "saltValue";

[0076] // 密码值

[0077] string pwdValue = "pwdValue";

[0078] byte[] data = UTF8Encoding.UTF8.GetBytes(input);

[0079] byte[] salt = UTF8Encoding.UTF8.GetBytes(saltValue);

[0080] // AesManaged - 高级加密标准(AES) 对称算法的管理类

[0081] AesManaged aes = new AesManaged();

[0082] 后续，先通过使用基于HMACSHA1 的伪随机数生成器，实现基于密码的密钥派生功能，通过密码和 salt派生密钥，再用当前的 Key 属性和初始化向量 IV 创建对称加密器对象，得到加密后输出，将加密后输出与加密转换连接，最后再用Base64编码将其转换为处

理后字符串。

[0083] }

[0084] 上述之所以将代表安全许可的许可识别码分出二级识别码或特级识别码，是因为考虑到公务车的特殊行车需求，对应的本申请还设置为：

[0085] 当所述行车许可是安全许可，判断行车许可信息是否包含有特级识别码，如果是，则将对应的车辆标记为重点车辆，并用另一非重点车辆的车辆信息对重点车辆的车辆信息做替换；替换的规律，可直接通过现行的随机点名(抽号)程序实现，库中的名为当前所有非重点车辆；从而通过将重点车辆的信息将任一非重点车辆做调换，实现“掩护”重点车辆的目的，有效提高信息安全。

[0086] 为提高本方法的使用效果，本方法还包括：

[0087] 统计各个目标车辆的行车时间，并生成用车时间排名表；以及接收和获取各个目标车辆的维修时间、原因以及次数，并汇总形成车辆维修记录；

[0088] 用车时间排名表和车辆维修记录均采用http协议与用户终端做数据交互。

[0089] 其中，用车时间排名表可提供给相关人员，使其能更为合理的调配所有公务车，减小资源浪费和公务车损坏几率；用车时间排名表，则可方便相关人员了解公务车的维修规律，预先做好检修，防止公务车使用过程中，意外损坏而影响正常工作。

[0090] 本申请实施例公开一种公务用车安全管控系统，参照图2，包括车载单元、后台及用户终端，其中，车载单元如上述连接有车载定位单元，后台包括存储器和处理器，存储器上存储有能够被处理器加载并执行如上述方法的计算机程序。

[0091] 以上均为本申请的较佳实施例，并非依此限制本申请的保护范围，故：凡依本申请的结构、形状、原理所做的等效变化，均应涵盖于本申请的保护范围之内。

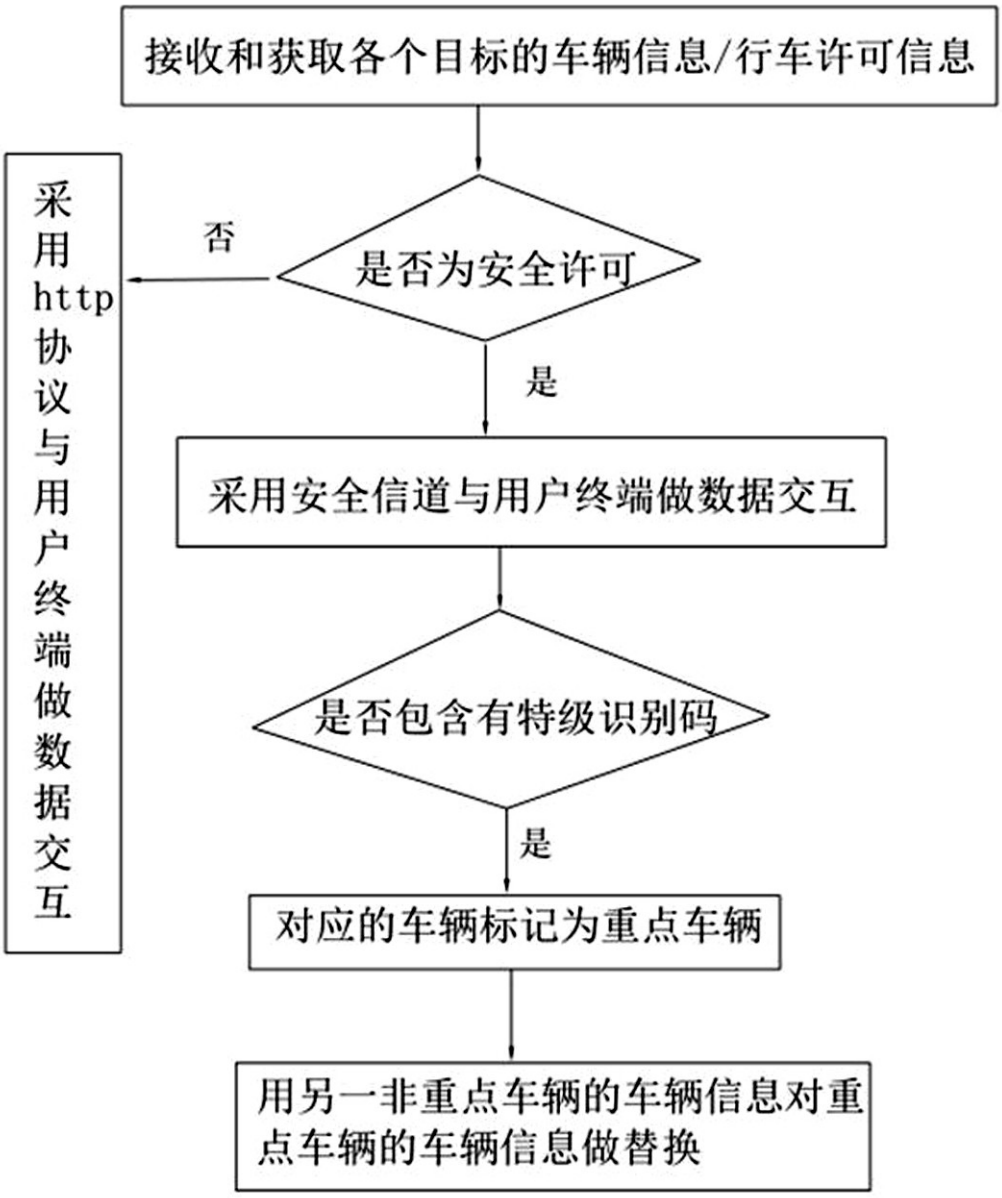

接收和获取各个目标的车辆信息/行车许可信息
是否为安全许可
否
采用http协议与用户终端做数据交互
是
采用安全信道与用户终端做数据交互
是否包含有特级识别码
是
对应的车辆标记为重点车辆
用另一非重点车辆的车辆信息对重点车辆的车辆信息做替换

图1

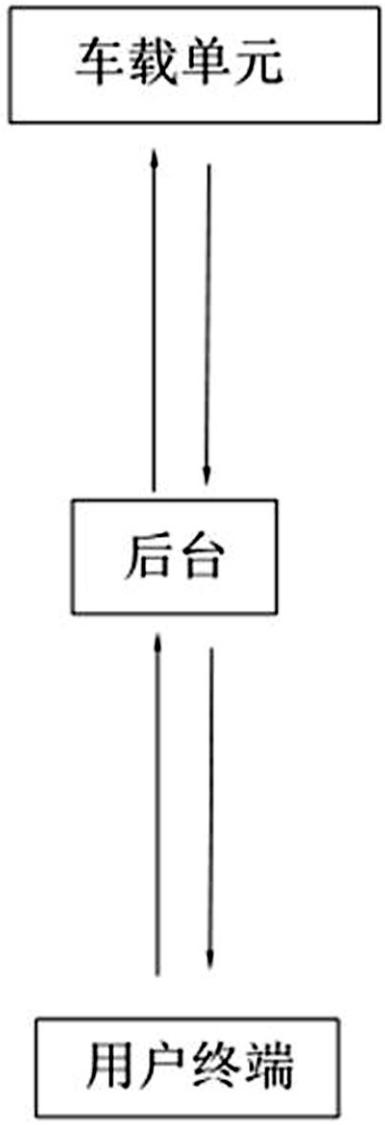


图2