(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 109088848 A
(43)申请公布日 2018.12.25

(21)申请号 201810566520.7

(22)申请日 2018.06.04

(71)申请人 佛吉亚好帮手电子科技有限公司
地址 331100 江西省宜春市丰城市高新技术产业园区高新大道12号

(72)发明人 马鑫 顾焰 甘茂煌

(74)专利代理机构 佛山市智汇聚晨专利代理有限公司 44409
代理人 张宏威

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 29/08(2006.01)

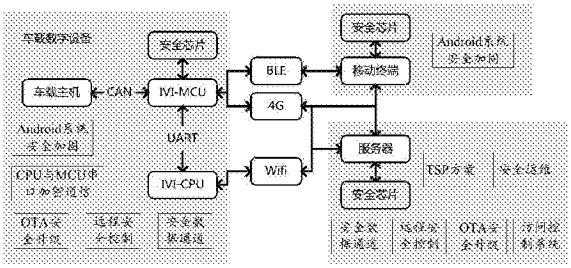
权利要求书1页 说明书4页 附图4页

(54)发明名称

一种智能网联汽车信息安全保护方法

(57)摘要

本发明涉及一种智能网联汽车信息安全保护方法，在车载主机、车载影音控制设备、远程服务器、车主的移动终端中，通过下列步骤对智能网联汽车的信息安全进行保护：S1部署安全芯片；S2平台物理隔离；S3系统签名加固；S4部署硬件通信安全协议；S5系统安全保护；S6数据通信加密；S7运维系统部署；本系统相比现有的安全防护方案，有更全面的防护效果及更高的安全级别，从多点防御、纵深防御、深入化的把汽车与安全相结合，并不只是单纯的在某个点做安全防护，具有更完善的系统性、完整性和高效性的安全防护效果。



CN 109088848 A

1.一种智能网联汽车信息安全保护方法，其特征在于，包括下列步骤：

S1部署安全芯片，在车载主机、车载影音控制设备、远程服务器、车主的移动终端中部署安全芯片；

S2平台物理隔离，通过安全隔离网闸、访问控制代理系统将汽车企业的基础数据服务器与互联网进行物理隔离；

S3系统签名加固，使用安全芯片内置的硬签名证书替换系统证书，并部署配套的安全认证管理系统；

S4部署硬件通信安全协议，在CPU和MCU的系统内嵌入数据传输的加密和解码程序；

S5系统安全保护，对车载系统、服务器系统、移动终端系统进行安全升级；

S6数据通信加固，通过标准SSL协议建立安全接入通信链路，通过安全芯片内置的加密算法，对OTA安全升级、汽车远程控制安全以及各系统软件的网络数据通信内容进行加密与解码；

S7运维系统部署，对信息安全保护系统进行实时监控、检测审计、系统管理。

2.根据权利要求1所述的一种智能网联汽车信息安全保护方法，其特征是：所述的步骤S4系统安全保护，包括针对Android系统部署安全引导程序、进程控制程序、网络控制程序、应用程序权限控制程序、接口授权程序，服务器端部署网络防火墙、安全隔离系统、身份认证系统、证书管理系统。

一种智能网联汽车信息安全保护方法

技术领域

[0001] 本发明涉及一种智能网联汽车信息安全保护方法，尤其是针对Android系 统、车载电子设备、网络数据传输、远程数据机房等系统的信息安全保护方法。

背景技术

[0002] 随着移动互联网的发展和嵌入式处理器性能的提升，汽车安全不再是过去 华而不实的宣传噱头，已经从深度和广度上颠覆了汽车的运行与驾驶方式。目 前包含远程分析、远程检修、远程寻车、实时路况预警、自动驾驶、自动躲避、 自动预警、自动更新等基于云技术的功能已经逐步实现，并可将智能终端(智 能手机、平板电脑)通过云平台与车载系统建立连接，通过智能设备查看车辆 信息、控制车载系统，以实现遥控泊车、自动驾驶等功能，让驾驶员从复杂的 操作中解脱出来，提高了安全性和舒适度，增强了驾车体验，也是目前各车企 宣传推广的重要特点。

[0003] 但是车联网在带来方便快捷的功能和高效的信息通信服务的同时，也带来 了更多的安全隐患。近年来，公开报道的汽车安全漏洞事件频繁发生，这些被 报道的“主角”当中不乏豪华车辆品牌。车联网安全的脆弱性，集中表现在以 下方面：

[0004] 病毒、木马入侵；

[0005] 网络攻击；

[0006] 信息拦截、数据窃取车载系统通过移动互联网与云端服务系统通信；

[0007] 非法访问，越权管理。

[0008] 如果没有严格、安全的身份标识认证，识别体系存在同平台内，用户误操 作或因用户名、密码丢失造成的非法登录、非法操作等，而这种攻击来自系统 内部，无法触发正常的安全防护机制，很难被即时发现或制止，造成用户数据 或车车信息非法访问，影响用户数据和车辆安全。

[0009] 随着移动互联网的发展和嵌入式处理器性能的提升，车辆的智能化和网联 化使车厂能为用户提供更方便、更舒适的驾乘体验。汽车网联化和智能化提供 方便快捷的功能和高效信息通信服务的同时，也带来了更多的安全隐患。根据 行业发展趋势，结合行业痛点，为厂商提供安全、智能、网联的整体解决方案。

发明内容

[0010] 为了克服现有的智能网联汽车安全漏洞事件频繁发生，汽车数据安全防护 漏洞较多的问题，本实用新提供一种智能网联汽车信息安全保护方法。

[0011] 本发明采用的技术方案是包括下列步骤：

[0012] S1部署安全芯片，在车载主机、车载影音控制设备、远程服务器、车主的 移动终端中部署安全芯片；

[0013] S2平台物理隔离，通过安全隔离网闸、访问控制代理系统将汽车企业的基 础数据服务器与互联网进行物理隔离；

[0014] S3系统签名加固，使用安全芯片内置的硬签名证书替换系统证书，并部署 配套的安全认证管理系统；

[0015] S4部署硬件通信安全协议，在CPU和MCU的系统内嵌入数据传输的加密 和解码程序；

[0016] S5系统安全保护，对车载系统、服务器系统、移动终端系统进行安全升级；

[0017] S6数据通信加固，通过标准SSL协议建立安全接入通信链路，通过安全芯 片内置的加密算法，对OTA安全升级、汽车远程控制安全以及各系统软件的网 络数据通信内容进行加密与解码；

[0018] S7运维系统部署，对信息安全保护系统进行实时监控、检测审计、系统管 理。

[0019] 作为优选的，所述的步骤S4系统安全保护，包括针对Android系统部署安 全引导程序、进程控制程序、网络控制程序、应用程序权限控制程序、接口授 权程序，服务器端部署网络防火墙、安全隔离系统、身份认证系统、证书管理 系统。

[0020] 本发明的有益效果是：本系统相比现有的安全防护方案，有更全面的防护 效果及更高的安全级别，从多点防御、纵深防御、深入化的把汽车与安全相结 合，并不只是单纯的在某个点做安全防护，具有更完善的系统性、完整性和高 效性的安全防护效果。

附图说明

[0021] 图1是本发明的系统安全结构图。

[0022] 图2是本发明的基于安全芯片的系统框架图。

[0023] 图3是本发明的OTA安全升级原理结构图。

[0024] 图4是本发明的硬件通信安全协议示意图。

[0025] 图5是本发明的平台物理隔离拓扑图。

[0026] 图6是本发明的安全运维系统结构图。

[0027] 图7是本发明的Android系统安全加固结构原理图。

具体实施方式

[0028] 本发明具体通过下列方法保护智能网联汽车的信息安全：

[0029] 参见图1、图2和图4，部署安全芯片：在车载主机、车载影音控制设备、 远程服务器、车主的移动终端中部署安全芯片。车载终端MCU主板贴装安全 芯片，MCU通过SPI与安全芯片相连，CUP核心板通过SPI与安全芯片相连， CPU核心板与MCU主板通过UART进行数据交互，MCU通过UART连接3、 4G通信模组，进行数据收发，CPU通过USB连接3、4G通信模组，进行数据 收发。

[0030] 参见图5，平台物理隔离，通过访问控制系统将汽车服务的基础数据服务 器进行物理隔离，保证即便当车联网业务区被攻破，车企基础数据也不会造成 数据泄露和数据破坏。该系统由访问控制代理系统和安全隔离网闸组成，具体 如下：

[0031] 1、访问控制代理系统：分为B/S和C/S代理，主要由访问前置、访问后置 系统组成，分别部署在接入区和应用服务区之间，对需要访问的数据资源服务 进行书册配置和共享交换，在网络信息隔离设备的基础上，对数据资源进行封 装，实现接入区和基础数据服务区之间的资源访问和数据交换，实现两个网络 间的数据交换和信息同步；

[0032] 2、安全隔离网闸：用于移动网络边界安全，实现接入区和基础数据服务区 的网络安全隔离，实现两个平台之间的数据高速传递，并对数据内容进行过滤， 保证信息网络不受外部攻击。

[0033] 参见图2和图4，部署硬件通信安全协议，在CPU和MCU的系统内嵌入 数据传输的加密和解码程序，在软件应用程序、用户自定义协议封装/解析层之 间加入加解密程序，当前MCU和Android端需要通过Uart口进行一定的数据 交互时，Uart串口数据如果在传输过程中被篡改，同样会威胁到整个系统的安 全，为了提高整体系统的安全性能，需要在这些数据的交互过程进行加密及验 证完整性处理，防止非法人员进行数据的篡改。

[0034] 系统签名加固，使用安全芯片内置的硬签名证书替换系统证书，并部署配 套的安全认证管理系统，如基于PKI体系的CA认证体系，可以根据安全防护 的需要来完成数字证书的签发、使用和撤销等全生命周期的证书操作。其中CA 结构可以选择目前现有的CA认证系统或者使用第三方的CA认证系统。

[0035] 数据通信加密，通过安全芯片内置的加密算法，对各系统以及软件的网络 数据包进行加密与解码。网络安全通信采用标准SSL协议建立安全接入通信链 路，实现双向身份认证、数据机密性和完整性保护；安全数据通道包含下列内 容：

[0036] 1、安全接入网关：内置SJK1308PCI密码卡，提供密码运算和设备数字证 书支持；支持移动终端采用SSL协议建立安全通信链路，实现双向身份认证、 数据机密性和完整性保护；

[0037] 2、数据接入安全代理：为了兼容没有搭载安全芯片的终端和系统，通过代 理后将数据转入安全接入网关，来保证兼容已经打在安全芯片的终端和系统不 受影响；

[0038] 3、安全芯片：采用SSX1207安全芯片；

[0039] 4、安全接入客户端：用于使用安全芯片配合安全网关建立安全通道；

[0040] 5、证书管理服务：用于证书签发、撤销、CRL列表查询等服务；

[0041] 6、鉴别评估服务：接入身份的认证和鉴别服务；

[0042] 7、设备用户服务：接入终端设备用户存储、查询等管理服务；

[0043] 8、监控管理服务：接入终端和网关行为的监控管理服务。

[0044] 参见图7，Android系统安全保护：从车载终端以及Android系统的个人终 端的系统层次上对其启动和运行环境进行安全加固，体现在Android系统的整 个生命周期，是一套基于黑白名单策略机制并实时生效的安全增强防护系统。安全加固的策略可根据车型和具体车辆划分，并通过后台配置下发实时生效。其内容包括系统签名、安全引导、进程控制、网络控制、应用权限控制、接口 授权和安全无线升级，在系统内核和框架层实现策略管理和权限控制，加上应 用安装签名审核服务来实现整个系统的安全可控。具体内容如下：

[0045] 1、系统签名：使用安全芯片内置的硬签名证书替换系统证书，可有效避免 系统证书泄露；

[0046] 2、安全引导：针对终端系统引导过程，增加系统镜像文件签名效验过程， 保证系统引导固件、内核、系统核心固件的有效性、完整性和一致性，防止对 系统文件修改和替换，有效杜绝病毒和木马，保证系统安全、可信；

[0047] 3、进程控制：除系统本地进程和可信的本地进程外，都不能执行，可信的 进程同样可动态的由后台进行配置，实时更新到车载终端，有效的防止系统被 Root；

[0048] 4、网络控制：包括主动访问的网络控制和被动访问的网络控制，其中主动 访问可根据被访问地址的不同进行控制，也可根据不同的进程设置不用的控制 策略；被动访问控制是监控本地对外提供的网络服务，从而防止外部通过接入 本地有漏洞的服务，进而攻击和破坏系统；

[0049] 5、应用权限控制：通过后台配置可对各应用的各个权限进行相应控制，结 合应用分发系统可以做到通过应用商店发布的程序对高机密等级的权限是默认 开放，而其它来源的应用是默认不开放；

[0050] 6、接口授权：对于高机密等级的接口，比如获取车速、设置车速、控制刹 车等接口除Android系统本身自带的权限机制外，还可以为这些接口提供动态 授权，这样即使破解了Android系统本身的权限控制，依然会受到该机制的控 制，保证这些接口的安全性。

[0051] 远程安全控制是对于远程控制等指令加密传输时，终端和云端分别集成相 应的SDK或代理程序，借助该SDK或代理程序实现双向的身份认证、密钥协 商和数据加解密，保护远程控制的数据安全。本方案通过安全芯片对数据加解 密和效验，服务器端可采用远程控制安全服务器或者远程控制安全服务器代理 来实现，服务器和代理服务均内嵌安全芯片，通过网络接口对外提供安全服务。

[0052] 参见图3，OTA安全升级是车载终端需要升级某ECU时，通过安全芯片和 KMS的安全机制将该ECU的升级包进行加密后，安全传递到要升级的车载设 备或者个人终端，通过对应的解码程序后进行ECU升级的过程。通过安全芯片 对密钥因子生成密钥，解密升级包，可有效防止升级程序被篡改和泄漏，从而 达到安全的远程升级，减少线下升级的成本。

[0053] 参见图6，运维系统部署，用于实现实时监控、检测审计、系统管理等功 能，该系统主要包括网络探针、数据探针和监控管理服务器：

[0054] 1、网络探针：采集车载终端和两万服务设备、网络的相关运行信息，并上 传给本区域部署的监控管理服务器。网络探针可以主动发起信息采集命令，实 时采集监控对象的相关信息；

[0055] 2、数据探针：针对业务环境下的数据库操作行为进行细粒度审计的合规性 管理。它通过对被授权人员和系统的数据库操作行为进行解析、分析、记录、 汇报，针对不用的应用协议，提供基于应用操作的审计，提供数据库操作与已 解析审计，实现对违规行为的及时监控和告警，以帮助用户事前规划防御、事 中实时监视、违规行为响应、事后合规报告、事故追踪溯源；

[0056] 3、监控管理服务器：实现平台运行网络及设备的系统管理、防护及联动策 略的安全管理、应用网络及用户的审计分析、车载终端设备管理，并可以进行 级联上报。

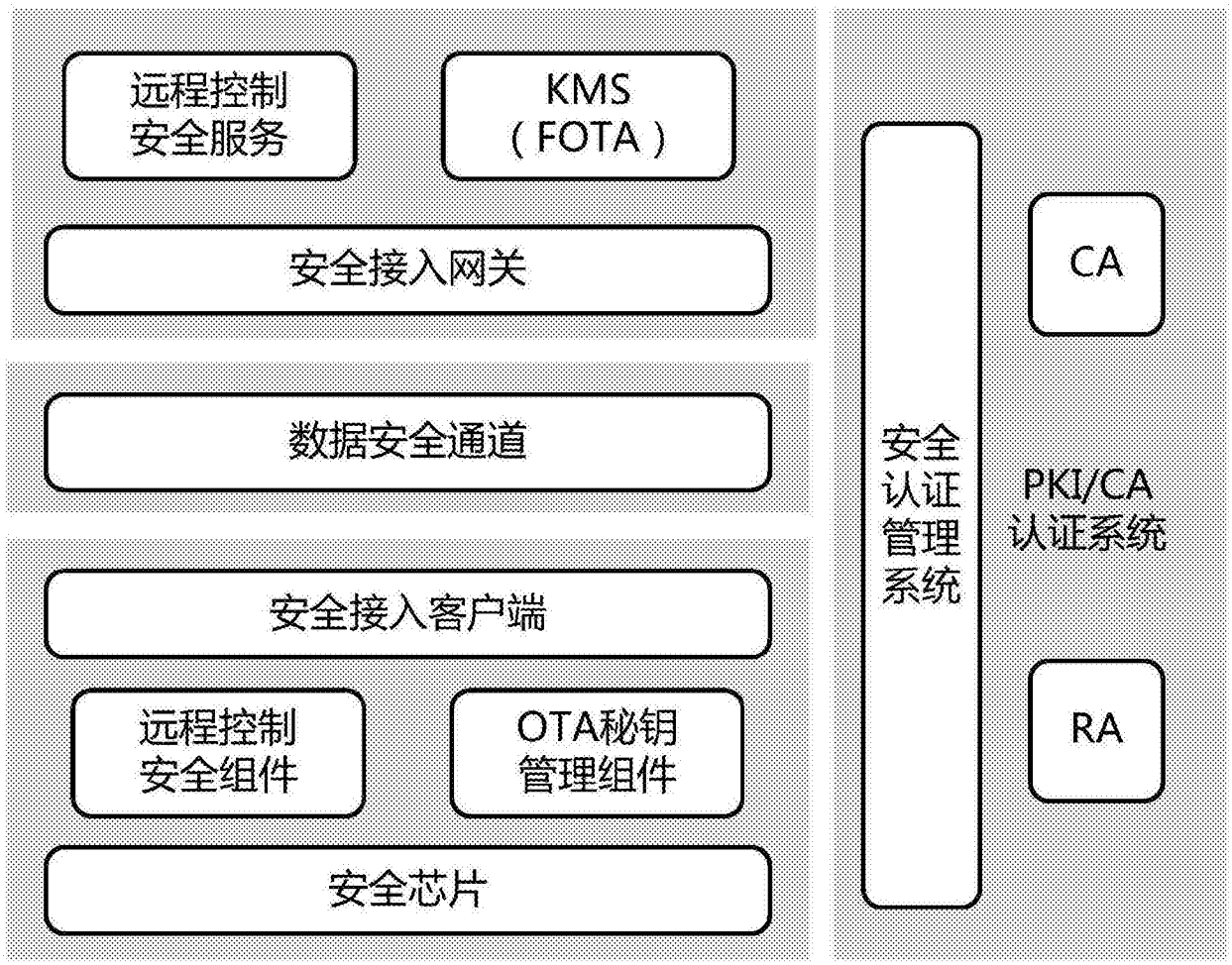

远程控制
安全服务
KMS
（FOTA）
安全接入网关
数据安全通道
安全接入客户端
远程控制
安全组件
OTA秘钥
管理组件
安全芯片
安全
认证
管理
系统
CA
PKI/CA
认证系统
RA

图1

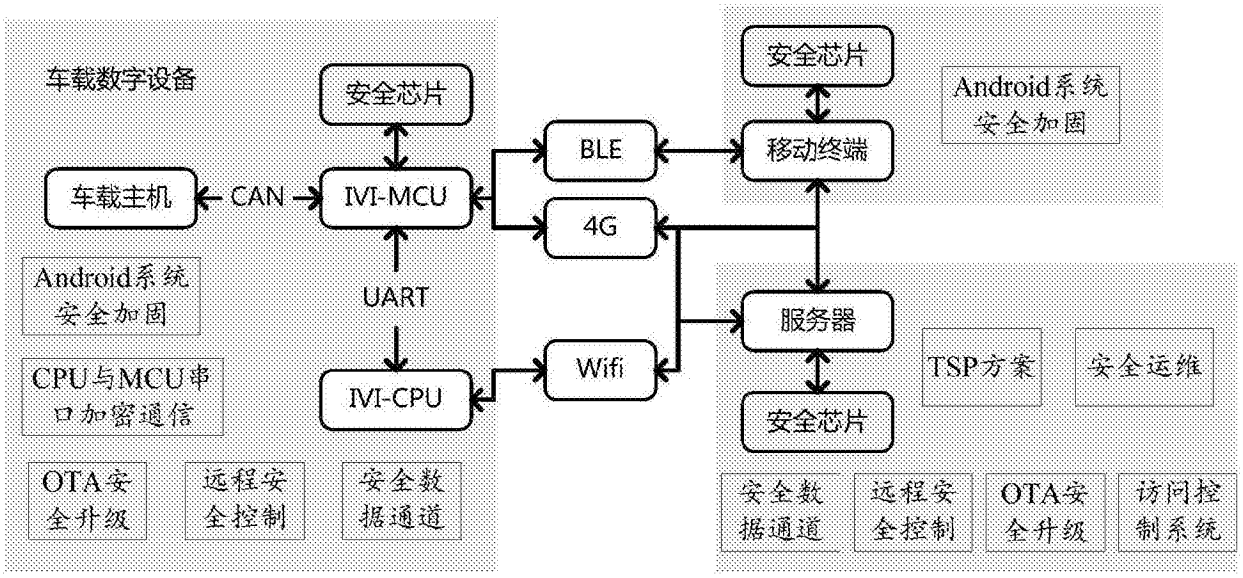

车载数字设备
安全芯片
车载主机
CAN
IVI-MCU
UART
IVI-CPU
BLE
4G
Wifi
Android系统
安全加固
CPU与MCU串
口加密通信
OTA安
全升级
远程安
全控制
安全数
据通道
安全芯片
移动终端
Android系统
安全加固
服务器
安全芯片
TSP方案
安全运维
安全数
据通道
远程安
全控制
OTA安
全升级
访问控
制系统

图2

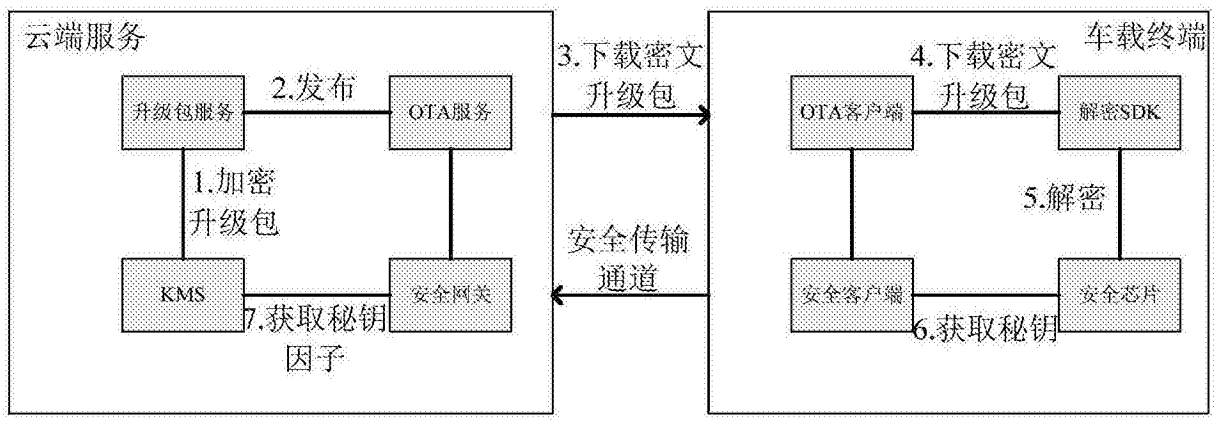

云端服务
升级包服务
2.发布
OTA服务
1.加密
升级包
KMS
7.获取秘钥
因子
安全网关
3.下载密文
升级包
安全传输
通道
车载终端
4.下载密文
升级包
OTA客户端
解密SDK
5.解密
安全客户端
6.获取秘钥
安全芯片

图3

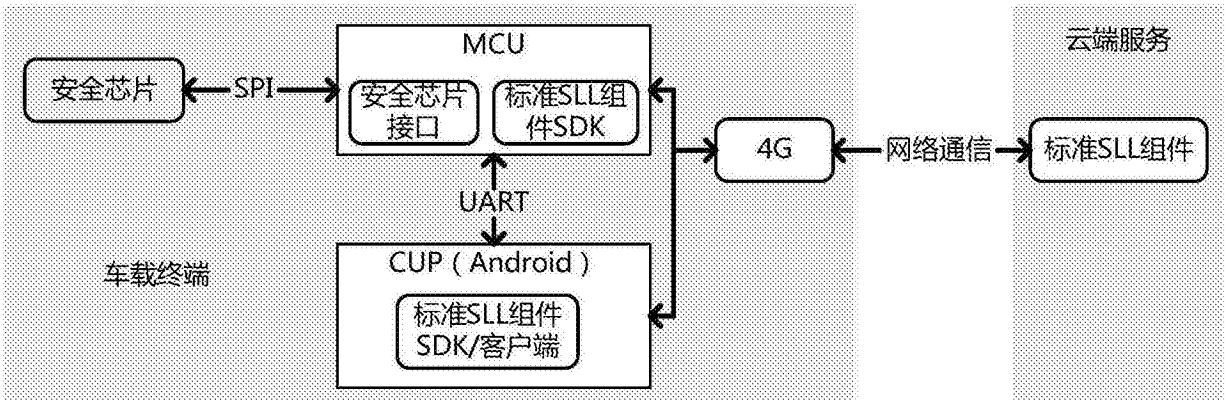

安全芯片
SPI
MCU
安全芯片
接口
标准SLL组
件SDK
UART
CUP（Android）
标准SLL组件
SDK/客户端
车载终端
4G
网络通信
云端服务
标准SLL组件

图4

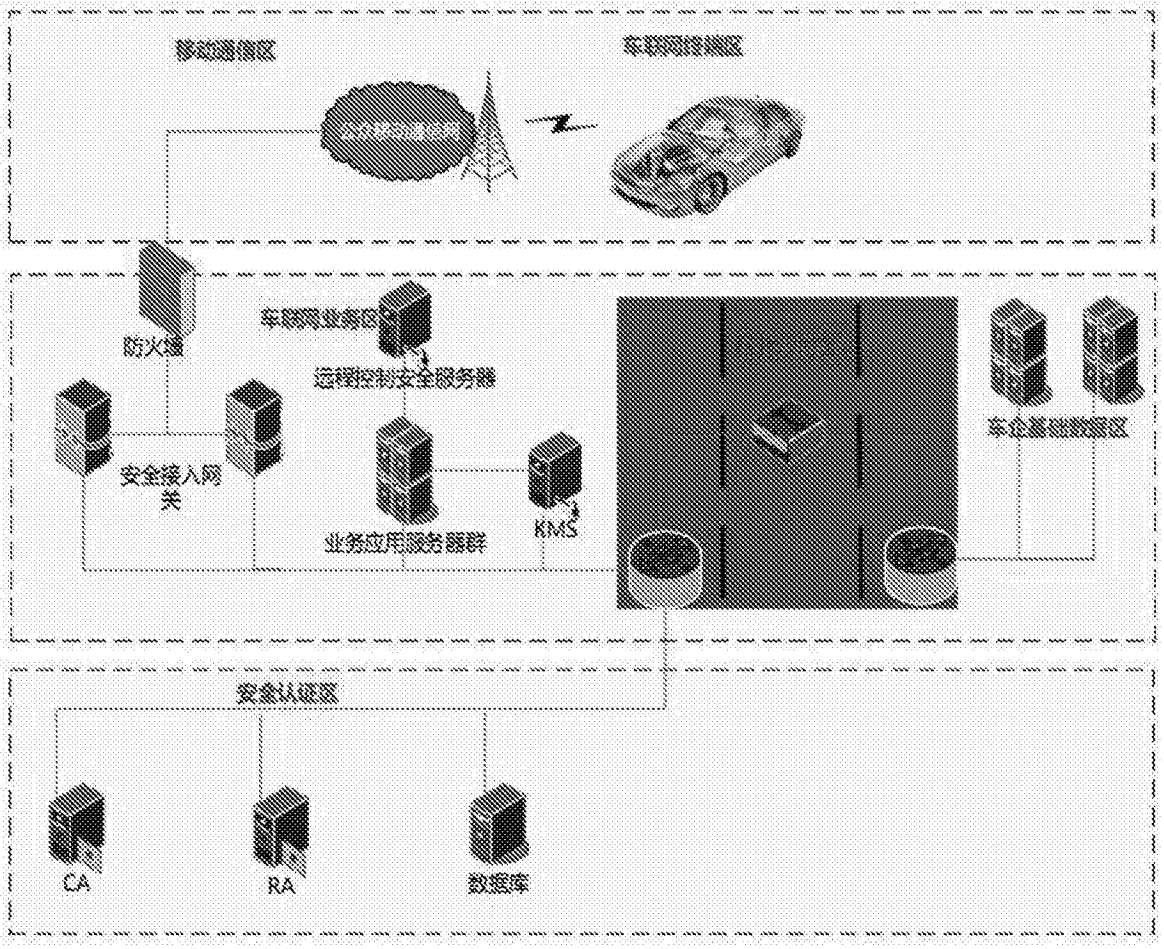

移动通信区
车联网终端区
防火墙
车联网业务应
远程控制安全服务器
安全接入网关
业务应用服务器群
KMS
安全认证区
CA
RA
数据库

图5

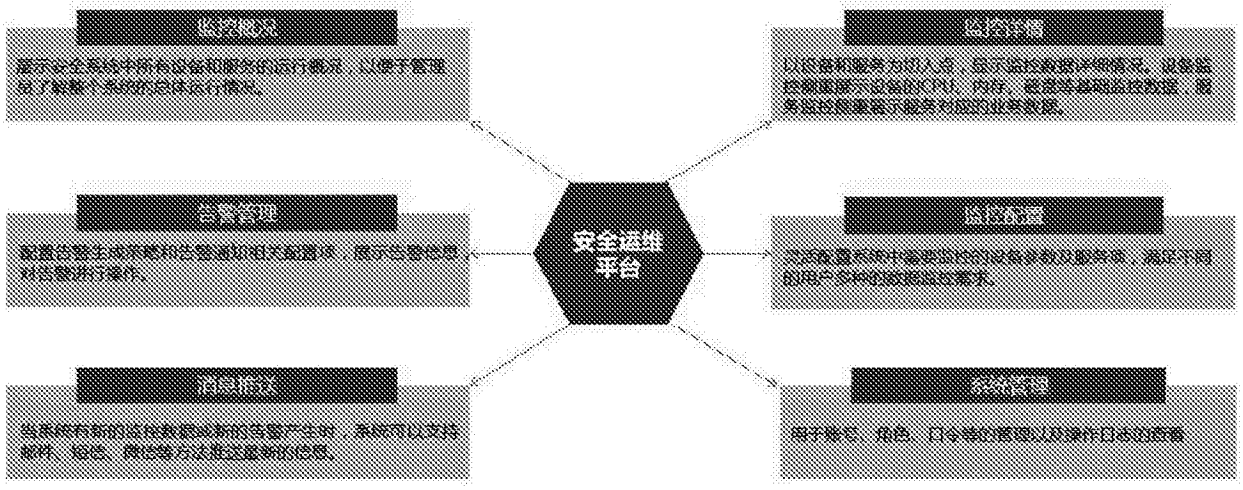

安全运维平台

图6

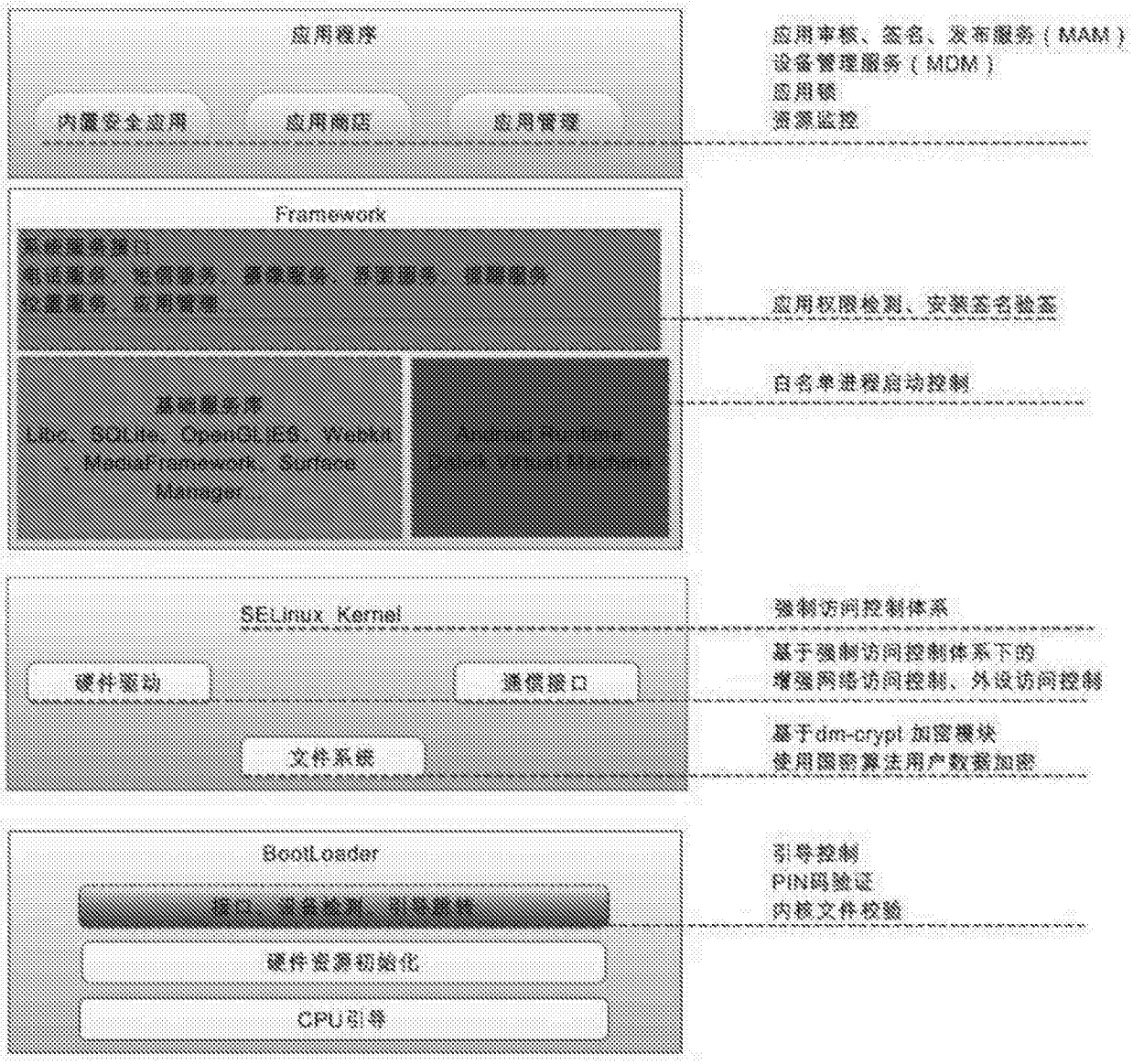

应用程序
内置安全应用
应用商店
应用管理
Framework
SELinux Kernel
硬件驱动
通信接口
文件系统
BootLoader
硬件资源初始化
CPU引导
应用审核、签名、发布服务（MAM）
设备管理服务（MDM）
应用锁
资源监控
应用权限检测、安装签名验签
白名单进程启动控制
强制访问控制体系
基于强制访问控制体系下的
增强网络访问控制、外设访问控制
基于dm-crypt 加密模块
使用国密算法用户数据加密
引导控制
PIN码验证
内核文件校验

图7