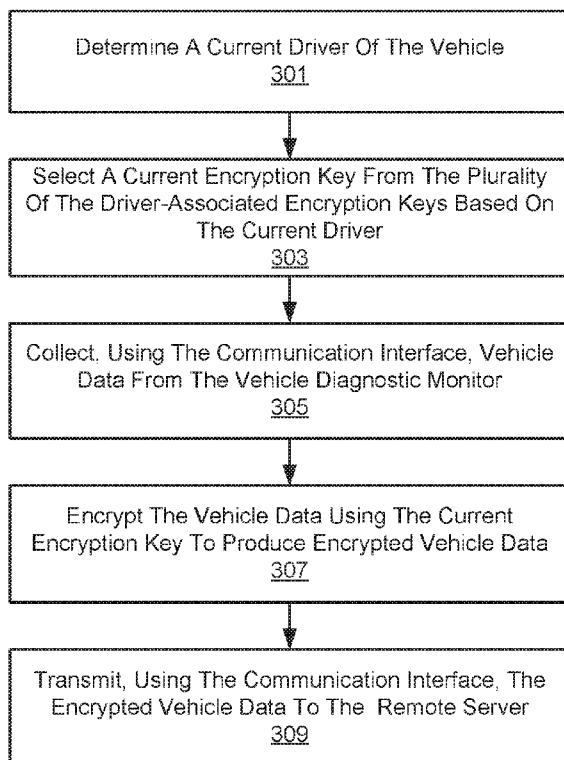




- (51) **International Patent Classification:**
G07C 5/00 (2006.01) *B60W 40/09* (2012.01)
G07C 5/08 (2006.01)
- (21) **International Application Number:**
PCT/US2017/013002
- (22) **International Filing Date:**
11 January 2017 (11.01.2017)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
14/992,805 11 January 2016 (11.01.2016) US
- (71) **Applicant (for all designated States except US):** **BLACK-BERRY LIMITED** [CA/CA]; 2200 University Avenue East, Waterloo, Ontario N2K 0A7 (CA).
- (72) **Inventor; and**
- (73) **Applicant (for US only):** **CHENNAKESHU, Sandeep** [US/US]; 2816 Waterbank Cove, Austin, Texas 78746 (US).
- (74) **Agents:** **STALFORD, Terry J.** et al.; FISH & RICHARDSON P.C., P.O. Box 1022, Minneapolis, Minnesota 55440-1022 (US).
- (81) **Designated States (unless otherwise indicated, for every kind of national protection available):** AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) **Title:** A DEVICE, METHOD AND SYSTEM FOR COLLECTING USER-BASED INSURANCE DATA IN VEHICLES



300

Fig. 3

(57) **Abstract:** A device, method and system for collecting user-based insurance data in vehicles is provided, including a device comprising: a processor, a memory storing a plurality of driver-associated encryption keys and a communication interface configured to communicate with a vehicle diagnostic monitor and a remote server, the processor configured to: determine a current driver of the vehicle; select a current encryption key from the plurality of the driver-associated encryption keys based on the current driver; collect, using the communication interface, vehicle data from the vehicle diagnostic monitor; encrypt the vehicle data using the current encryption key to produce encrypted vehicle data; and, transmit, using the communication interface, the encrypted vehicle data to the remote server.



(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE,

SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

A DEVICE, METHOD AND SYSTEM FOR COLLECTING USER-BASED INSURANCE DATA IN VEHICLES

CLAIM OF PRIORITY

[0001] This application claims priority to U.S. Patent Application No. 14/992,805
5 filed on January 11, 2016, the entire contents of which are hereby incorporated by
reference.

FIELD

[0002] The specification relates generally to computing devices in vehicles, and
specifically to a device, method and system for collecting user-based insurance data in
10 vehicles.

BACKGROUND

[0003] User-based vehicle insurance is becoming more common, where insurance
companies base insurance rates on driving habits rather than on traditional rating
methods. In such methods, telematics systems can collect data about operational use
15 of the vehicle and send the data to a remote computing device. However, such systems
may not reliably distinguish between multiple drivers of a single vehicle, may
unreliably distinguish between different data sets for multiple drivers, and/or may have
security and/or privacy concerns.

BRIEF DESCRIPTIONS OF THE DRAWINGS

[0004] For a better understanding of the various implementations described herein and
to show more clearly how they may be carried into effect, reference will now be made,
by way of example only, to the accompanying drawings in which:

[0005] Fig. 1 depicts a system for collecting user-based insurance data in vehicles,
25 according to non-limiting implementations.

[0006] Fig. 2 depicts a schematic block diagram of the system of Fig. 1, according to
non-limiting implementations.

[0007] Fig. 3 depicts a block diagram of a flowchart of a method for collecting user-
based insurance data in vehicles, according to non-limiting implementations.

30 [0008] Fig. 4 depicts the system of Fig. 1, where log-in data is received, according to
non-limiting implementations.

[0009] Fig. 5 depicts the system of Fig. 1, where driver identification data is received,
according to non-limiting implementations.

[0010] Fig. 6 depicts the system of Fig. 1, where vehicle data is received, according to non-limiting implementations.

[0011] Fig. 7 depicts the system of Fig. 1, where vehicle data is encrypted according to non-limiting implementations.

5 [0012] Fig. 8 depicts the system of Fig. 1, where encrypted vehicle data is transmitted to a server, according to non-limiting implementations.

[0013] Fig. 9 depicts a block diagram of a flowchart of a method for securely remotely controlling devices in vehicles, according to non-limiting implementations.

10

DETAILED DESCRIPTION

[0014] In general, this disclosure is directed to a device, method and system for collecting user-based insurance data in vehicles. In particular a device in a vehicle selects a current encryption key, from a plurality of driver-associated encryption keys, based on the current driver, and encrypts vehicle data from a vehicle diagnostic monitor using the current encryption key. The encryption keys can be provisioned at the device, for example when a new driver is detected and/or when a new driver signs into an input device. The encryption keys can be private keys respectively associated with each driver of the vehicle, such that the encrypted collected data is particularly associated with given drivers of the vehicle. Hence, when the encrypted collected data is transmitted to a remote server (e.g. associated with and/or operated by an insurance company), the driver associated with the encrypted collected data can be identified when an associated public key, associated with the driver, successfully decrypts the encrypted collected data. Furthermore, the device can be implemented as a dongle which can communicate with a second device, such as a mobile device, smartphone, and the like, located in the vehicle; for example, the dongle can be plugged into a vehicle diagnostic port, such as an on-board diagnostics (OBD) port or an OBD-II port of the vehicle. The dongle may collect and encrypt the vehicle data (such as fuel consumption, speed, braking, engine diagnostics, odometer, location (GPS), etc.), and transmit the encrypted collected data to the second device which can, in turn, transmit the encrypted collected data to a remote server and data base or Internet of Things (IoT) Platform. Alternatively, the dongle can communicate directly with the remote server. While certain such systems exist, they often suffer from one or more limitations. For example, the data may not be encrypted, or the driver may not be uniquely identified. Similarly, in such implementations, a cost

20

25

30

of a dongle can be reduced by using a mobile device to communicate with the remote server, rather than include cell-phone circuits, and the like, in the dongle. Furthermore, transmitting the encrypted vehicle data using the mobile device can lead to better ease of use and/or deployment of such dongles; for example, as compared to dongles that
5 have to be removed from a vehicle and interfaced with a computer and/or mailed to an insurance company.

[0015] In this specification, elements may be described as “configured to” perform one or more functions or “configured for” such functions. In general, an element that is configured to perform or configured for performing a function is enabled to perform the
10 function, or is suitable for performing the function, or is adapted to perform the function, or is operable to perform the function, or is otherwise capable of performing the function.

[0016] It is understood that for the purpose of this specification, language of “at least one of X, Y, and Z” and “one or more of X, Y and Z” can be construed as X only, Y
15 only, Z only, or any combination of two or more items X, Y, and Z (e.g., XYZ, XY, XZ, YZ, and the like). Similar logic can be applied for two or more items in any occurrence of “at least one ...” and “one or more...” language.

[0017] An aspect of the specification provides a device comprising: a processor, a memory storing a plurality of driver-associated encryption keys and a communication
20 interface configured to communicate with a vehicle diagnostic monitor and a remote server, the processor configured to: determine a current driver of the vehicle; select a current encryption key from the plurality of the driver-associated encryption keys based on the current driver; collect, using the communication interface, vehicle data from the vehicle diagnostic monitor; encrypt the vehicle data using the current
25 encryption key to produce encrypted vehicle data; and, transmit, using the communication interface, the encrypted vehicle data to the remote server.

[0018] The device can further comprise a removable dongle configured to removably connect to a communication bus.

[0019] The communication interface can comprise one or more of: an OBD (on-board
30 diagnostics) connector, an OBD-II connector, a USB (universal serial bus) connector, an Ethernet bus connector, and a CAN (controller area network) Bus connector.

[0020] Each of the driver-associated encryption keys can comprise a respective private encryption key.

[0021] Each of the driver-associated encryption keys can comprise an ECC (elliptical curve cryptography) key.

[0022] The processor can be further configured to determine the current driver of the vehicle by receiving log-in data from an input device of one or more of the vehicle, a mobile device, and the device.

[0023] The processor can be further configured to determine the current driver of the vehicle by receiving driver identification data from an input device of one or more of the vehicle, a mobile device, and the device.

[0024] The processor can be further configured to combine the vehicle data with user data prior to encrypting the vehicle data.

[0025] The processor can be further configured to place the device in a read-only mode when the communication interface is connected to the vehicle diagnostic monitor.

[0026] Another aspect of the specification provides a method comprising: at a device comprising: a processor, a memory storing a plurality of driver-associated encryption keys and a communication interface configured to communicate with a vehicle diagnostic monitor and a remote server: determining, at the processor, a current driver of the vehicle; selecting, at the processor, a current encryption key from the plurality of the driver-associated encryption keys based on the current driver; collecting, at the processor, using the communication interface, vehicle data from the vehicle diagnostic monitor; encrypting, at the processor, the vehicle data using the current encryption key to produce encrypted vehicle data; and, transmitting, at the processor, using the communication interface, the encrypted vehicle data to the second device.

[0027] The communication interface can comprise one or more of: an OBD (on-board diagnostics) connector, an OBD-II (on-board diagnostics) connector, a USB (universal serial bus) connector, an Ethernet bus connector, and a CAN (controller area network) Bus connector.

[0028] Each of the driver-associated encryption keys can comprise a respective public encryption key.

[0029] Each of the driver-associated encryption keys can comprise an ECC (elliptical curve cryptography) key.

[0030] The method can further comprise determining the current driver of the vehicle by receiving log-in data from an input device of one or more of the vehicle, a mobile device, and the device.

[0031] The method can further comprise determining the current driver of the vehicle by comparing the vehicle data with stored vehicle data associated with the current driver.

[0032] The method can further comprise determining the current driver of the vehicle by receiving driver identification data from an input device of one or more of the vehicle, a mobile device, and the device.

[0033] The method can further comprise combining the vehicle data with user data received from a mobile device prior to encrypting the vehicle data.

[0034] The method can further comprise placing the device in a read-only mode when the communication interface is connected to the vehicle diagnostic monitor.

[0035] A further aspect of the specification provides a computer-readable medium storing a computer program, wherein execution of the computer program is for: at a device comprising: a processor, a memory storing a plurality of driver-associated encryption keys and a communication interface configured to communicate with a vehicle diagnostic monitor and a remote server: determining, at the processor, a current driver of the vehicle; selecting, at the processor, a current encryption key from the plurality of the driver-associated encryption keys based on the current driver; collecting, at the processor, using the communication interface, vehicle data from the vehicle diagnostic monitor; encrypting, at the processor, the vehicle data using the current encryption key to produce encrypted vehicle data; and, transmitting, at the processor, using the communication interface, the encrypted vehicle data to the second device. The computer-readable medium can comprise a non-transitory computer-readable medium.

[0036] Attention is next directed to Fig. 1 and Fig. 2 which respectively depict a schematic perspective view, and a block diagram, of a system 100 for collecting user-based insurance data in vehicles. System 100 comprises: a device 101 which interfaces with a vehicle diagnostic monitor 103, and a remote server 150 (as depicted in Fig. 2). While in some implementations device 101 can communicate directly with remote server 150, in other implementations device 101 can communicate with remote server 150 via a mobile device 105. In particular, Fig. 1 depicts a schematic interior

view of a passenger area of a vehicle 107. Devices 101, 105 and vehicle diagnostic monitor 103 are located in vehicle 107, which includes a windshield 108, a steering wheel 109, and a dashboard 110, dashboard 110 optionally comprising an infotainment and/or entertainment system 111 (referred to hereafter as infotainment system 111)
5 that can include a display 112 and an input device (not depicted), which can include a touchscreen of display 112. While vehicle diagnostic monitor 103 is depicted in Fig. 1, vehicle diagnostic monitor 103 can generally be hidden from view from the passenger area of vehicle 107. As depicted, device 101 comprises a removable dongle that is connected to a communication bus 113 of vehicle 107 (as depicted in Fig. 2),
10 device 101 in communication with vehicle diagnostic monitor 103 via communication bus 113. Device 101 is further in communication with mobile device 105 via a link 115. However, in other implementations, device 101 can be in communication with server 150 via a wireless network, without intervening mobile device 105.

Alternatively, system 100 can comprise an Internet of Things (IoT) platform (e.g. a
15 platform that can collect, process and store data) configured to communicate with both device 101 and server 150, and/or server 150 can comprise an IoT platform.

[0037] In particular, as depicted, device 101 is removably connected to communication bus 113 via a port 116. Port 116 may comprise a connector, such as an OBD-II connector. Additionally or alternatively, port 116 may include one or more
20 of an OBD (on-board diagnostics) connector, an Ethernet bus connector, and a CAN (controller area network) Bus connector. In one implementation, device 101 is removably connected to communication bus 113 via an OBD-II connector. In another implementation device 101 may be removably connected to communication bus 113 via a USB (universal serial bus) connector, for example at a USB port at
25 infotainment unit 111, and/or another USB port, assuming that vehicle 107 comprises a communication interface between the USB port and/or infotainment unit 111, and communication bus 113. In other words, device 101 can be removably connected to any port that has access to a communication bus where vehicle data can be collected from a vehicle diagnostics monitor.

30 [0038] With reference to Fig. 2, device 101 further comprises a processor 120, a memory 122 and communication interface 124. In some implementations, device 101 further comprises an input device 128, depicted in stippled lines in Fig. 2 to indicate that such an input device 128 is optional; while input device 128 is not depicted in the

dongle implementation depicted in Fig. 1, such a dongle can be adapted to include input device 128. Memory 122 stores a plurality of driver-associated encryption keys 125-1, 125-2, 125-3...125-n, which are interchangeably referred to hereafter, collectively, as keys 125 and, generically, as a key 125. Communication interface 124 is configured to communicate with vehicle diagnostic monitor 103 and mobile device 105. Processor 120 is configured to: determine a current driver of vehicle 107; select a current encryption key from plurality of the driver-associated encryption keys 125 based on the current driver; collect, using communication interface 124, vehicle data from vehicle diagnostic monitor 103; encrypt the vehicle data using the current encryption key to produce encrypted vehicle data; and, transmit, using communication interface 124, the encrypted vehicle data to remote server 150. As depicted, device 101 is configured to transmit, using communication interface 124, the encrypted vehicle data to remote server 150 via mobile device 105; however in other implementations interface 124 can include radios and the like communicate with remote server 150 without an intervening device; in these implementations encrypted vehicle data can be communicated to remote server 150 via wireless link between device 101 and remote server 150.

[0039] While details of vehicle diagnostic monitor 103 are not depicted, vehicle diagnostic monitor 103 comprises components of vehicle 107 which track and/or measure parameters associated with operation of vehicle 107 including, but not limited to, speed, acceleration, braking, distance travelled, fuel consumption, deployment of airbags and the like. In other words, vehicle diagnostic monitor 103 comprises hardware configured to track and/or measure parameters of vehicle 107 which can be used to rate a driver for insurance and/or determine when a driver is speeding, how the driver accelerates, how often the driver brakes, where a driver travels, time of day or night a driver is on the road, where a driver leaves the vehicle for an extended period of time (such as parking) and the like.

[0040] Optional mobile device 105 comprises a processor 130, a memory 132, a communication interface 134, a display device 136, an input device 138, and optionally a speaker 139 and a microphone 140. While not depicted, mobile device 105 further comprises a power source, including but not limited to a battery and/or a power pack, or any other suitable power source, a housing and the like. Indeed, mobile device 105 can be any type of electronic device that can be used in a self-contained manner. Mobile

device 105 includes, but is not limited to, any suitable combination of electronic devices, communications devices, mobile devices, laptop computers, portable electronic devices, mobile computing devices, portable computing devices, tablet computing devices, laptop computing devices, PDAs (personal digital assistants), cellphones, smartphones, e-readers, and the like. Other suitable devices are within the scope of present implementations. In general, however, mobile device 105 is configured to communicate with both device 101 and a remote server 150, for example a server of an insurance company, and the like, via links 115, 151.

[0041] Furthermore, while only one optional mobile device 105 is depicted in system 100, system 100 can comprise a plurality of optional mobile devices similar to mobile device 105, each configured to communicate with device 101 and server 150, for example upon execution of a user-based insurance application and the like. Each of mobile devices, including mobile device 105, upon execution of the user-based insurance application, can be configured to act as a go-between and/or an intermediate device between device 101 and server 150. Hence, communication between device 101 and server 150 occurs without the use of a vehicle-based telematics system.

[0042] Server 150 generally comprises one or more servers configured to manage at least a portion of a user based insurance system, including, but not limited to, managing keys of a user-based insurance system and/or further configured to communicate with one or more mobile devices, including mobile device 105, via a network that includes link 151. Server 150 can be based on any well-known server environment including a module that houses one or more central processing units, volatile memory (e.g. random access memory), persistent memory (e.g. hard disk devices) and network interfaces to allow server 150 to communicate over link 151. However, it is to be emphasized that a vast array of other types of computing environments for server 150 are contemplated. For example, server 150 can comprise a computing device, including but not limited to one or more of a personal computer, a laptop computer, and a mobile computing device. Furthermore, while processor(s) and memory(s) of server 150 are not depicted, they are appreciated to be nonetheless present. Server 150 can further comprise an Internet of Things (IoT) platform; alternatively, system 100 can comprise an IoT platform configured to communicate with both device 101 and server 150.

[0043] Server 150 stores, in a memory, a plurality of driver-associated decryption keys 155-1, 155-2, 155-3...155-n which are interchangeably referred to hereafter,

collectively, as keys 155 and, generically, as a key 155. For example, each key 155 can correspond to a key 125 stored at device 101 and hence can be used to decrypt data encrypted with a corresponding key 125.

5 [0044] In general, each pair of keys 125, 155 can comprise, respectively, a public key and a corresponding private key. In some implementations, each key 125 can comprise an ECC (elliptical curve cryptography) public key, and each key 155 can comprise a corresponding ECC private key. However, other types of encryption/decryption keys are within the scope of present implementations including, but not limited to, asymmetric keys and symmetric keys.

10 [0045] While an integer number of “n” pairs of keys 125, 155 are depicted, a number of each of keys 125, 155 can correspond to a number of drivers of vehicle 107 and/or a number of drivers of vehicle 107 that are registered for user-based insurance.

[0046] It is also assumed that keys 125, 155 have been previously stored at each of device 101 and server 150 using one or more provisioning processes. For example, 15 keys 125, 155 can be stored at each of device 101 and server 150 at a factory and assigned to drivers of vehicle 107 by an insurance company, and the like, operating server 150; in these implementations, when a driver registers for user-based insurance, server 150, and the like, can transmit a key assignment command to device 101 via mobile device 105, and processor 120 can assign a given key 125 to a given driver, for 20 example by storing driver identification data received with the key assignment command in association with a given key 125 identified in the key assignment command.

[0047] Alternatively, when a new driver of vehicle 107 registers with the insurance company for user-based insurance, a new pair of keys 125, 155 can be generated, for 25 example by server 150, and new key 125 can be transmitted to device 101, by server 150 transmitting new key 125 to mobile device 105, which in turn transmits the new key 125 to device 101 when devices 101, 105 are next in communication; the new key 125 can also be stored with driver identification data received with the new key 125.

[0048] Alternatively, a new driver can log-in to system 100 at mobile device 105 30 and/or at infotainment unit 111 (e.g. using display device 112 and/or an input device) using driver identification data (e.g. credentials) previously provided to the new driver from an insurance company, for example using email, messages, posted mail, and the like; the driver identification data are then uniquely associated with a private key 125,

which can be used to encrypt to vehicle data for the driver. The private key 125 can be provisioned at device 101 as described above.

[0049] Furthermore, keys 125 can be stored in a secure data base at memory 122 and received at device 101 using a key exchange mechanism (including, but not limited to, ECC based Diffie Hellman exchange) between device 101 and server 150.

[0050] In other words, while not depicted, each key pair 125, 155 can be stored, at device 101 and server 150 respectively, in conjunction with an associated driver identifier, including, but not limited to, an insurance policy number, an alphanumeric identifier, a log-in identifier and the like.

[0051] Furthermore, provisioning of device 101 can include provisioning device 101 with a certificate (e.g. a certificate associated with remote server 150 and/or a remote server certificate). Such provisioning can occur at a factory and/or by an entity provisioning and shipping device 101 for installation at vehicle 107, such as an insurance company. When device 101 is first installed and/or received at port 116, and communications are established with remote server 150 and/or an IoT platform, device 101 can register itself with remote server 150 (and/or the IoT platform). Device 101 and remote server 150 (and/or the IoT platform) can authenticate each other in such a registration process using a suitable protocol which can include, but is not limited to, TLS (transport layer security), and the like. Upon authentication with remote server 150 (and/or IoT platform), device 101 can be officially activated, in that server 150 will recognize communications from device 101 as being from an authenticated device.

[0052] The registration process and/or authentication process can include, but is not limited to, device 101 communicating a VIN (“vehicle identification number”) of vehicle 107 to remote server 150; the VIN can be provisioned at device 101 using input device 128 and/or an input device at infotainment unit and/or at the factory and/or by the entity shipping device 101, which can be the same entity insuring vehicle 107. Alternatively, device 101 can be configured to automatically retrieve the VIN from a memory (not depicted) of vehicle 107 that stores associated vehicle data. In this manner, device 101 can be associated with vehicle 107 as uniquely identified by the VIN. Furthermore, when a user registers with system 100, and has a key 125 assigned to the user, remote server 150 (and/or the IoT platform) can recognize that a

user is associated with vehicle 107, as well as that device 101 is being used with vehicle 107, and further recognize when the user is driving vehicle 107.

[0053] However, device 101 can be reused with a new vehicle by erasing keys 125, the VIN and other vehicle-associated data, and repeating the provisioning using data associated with the new vehicle. However, in this case one would need to reinstall a new set of keys 125 in the device. That is, when the device is installed it may authenticate with the server and the server may authenticate with the device to establish that both know each other and are valid/authorized entities and then proceed to communicate. The server may then exchange the public key with the device while it stores the corresponding private key.

[0054] Link 115 generally comprises any suitable link that enables device 101 and mobile device 105 to communicate. Link 115 can hence include any suitable combination of wired and/or wireless links, wired and/or wireless devices and/or wired and/or wireless networks, including but not limited to any suitable combination of USB (universal serial bus) cables, serial cables, wireless links, cell-phone links, cellular network links (including but not limited to 2G, 2.5G, 3G, 4G+, and the like) wireless data, Bluetooth™ links, Zigbee™ links, NFC (near field communication) links, WiFi links, WiMax links, packet based links, the Internet, analog networks, the PSTN (public switched telephone network), access points, and the like, and/or a combination. However, in particular non-limiting implementations, link 115 comprises a local link, for example a BTLE (Bluetooth™ low energy link) and the like.

[0055] Similarly, link 151 generally comprises any suitable link that enables mobile device 105 and server 150 to communicate. Link 151 can hence include any suitable combination of wired and/or wireless links, wired and/or wireless devices and/or wired and/or wireless networks, including but not limited to any suitable combination of wireless links, cell-phone links, cellular network links (including but not limited to 2G, 2.5G, 3G, 4G+, and the like), WiFi links, WiMax links, packet based links, the Internet, analog networks, the PSTN (public switched telephone network), access points, and the like, and/or a combination. However, in particular non-limiting implementations, link 151 comprises a cellular data link, and the like, such that mobile device 105 and server 150 can communicate while vehicle 107 is moving.

[0056] Links 115, 151 can optionally be replaced with a link between device 101 and server 150, such a link being similar to link 151.

[0057] Communication bus 113 comprises any suitable communication bus used in a vehicle, including, but not limited to, communication buses using one or more of the following protocols: Byteflight, CAN (Controller Area Network), D2B (Domestic Digital Bus), FlexRay, DC-BUS, IDB-1394, IEBus, I²C, ISO 9141-1, ISO9141-2, J1708, J1587, J1850, J1939, ISO 11783, J1939, ISO 11783, Keyword Protocol 2000 (KWP2000), LIN (Local Interconnect Network), MOST (Media Oriented Systems Transport), Multifunction Vehicle Bus, SMARTwireX, SPI (Serial Peripheral Interface), Ethernet, Ethernet AVB and the like. In some implementations, communication bus 113 can include an OBD-II port and/or an OBD port and/or a USB port and the like.

[0058] It should be emphasized, however, that the structure of devices 101, 105 and server 150 are purely examples and other implementations of each are within the scope of present implementations.

[0059] For example, in Fig. 1, device 101 is depicted as a dongle configured to removably connect to communication bus 113 of vehicle 107, to connect communication interface 124 to vehicle diagnostic monitor 103. Hence, vehicle 107 can be retrofitted for user-based insurance by plugging the dongle into port 116, which can include, but is not limited to, an OBD-II port connected to communication bus 113.

[0060] While not depicted, infotainment system 111 comprises components that can provide entertainment and/or information to a driver of vehicle 107, including, but not limited to, AM/FM radios, satellite radios, CD players, GPS/navigation devices, MP3 players, and the like, with display 112 and/or an input device generally configured to receive input data and communicate with device 101. For example, display 112 and/or an associated input device, such as a touchscreen, a key pad and the like, can be used to receive input data that can be communicated to device 101.

[0061] However, in other implementations, device 101 can be implemented as component of vehicle 107 and/or infotainment system 111, in communication with vehicle diagnostic monitor 103 via communication bus 113.

[0062] In general, data from vehicle diagnostic monitor 103 can be received at processor 120 (which can be implemented as a plurality of processors, including but

not limited to one or more central processors (CPUs)). Processor 120 can further comprise one or more hardware processors and/or an ASIC (application-specific integrated circuit) processor. Processor 120 is configured to communicate with a memory 122 which can comprise a non-volatile storage unit (e.g. Erasable Electronic Programmable Read Only Memory (“EEPROM”), Static RAM, Flash Memory, Atomic RAM, Resistive RAM, Phase Change Memory) and/or a volatile storage unit (e.g. dynamic random access memory (“RAM”)). In particular non-limiting implementations, memory 122 comprises a special storage configured for storing leys 125 that can include, but is not limited to fuses, a one-time programmable (“OTP”) or fuses and the like. In particular, encryption keys described herein are stored in a non-volatile portion of memory 122; indeed, encryption keys described herein are generally not stored in a volatile memory. Further, memory described herein used to hold keys may be chosen as to be secure and tamper-proof.

[0063] Programming instructions that implement the functional teachings of device 101 as described herein can be maintained, persistently, in memory 122 and used by processor 120, which makes appropriate utilization of volatile storage during the execution of such programming instructions. Those skilled in the art will now recognize that memory 122 is an example of a computer-readable medium, and in particular a non-transitory computer-readable medium, storing a computer program, wherein execution of the computer program is for configuring the processor 120 as described herein. Furthermore, memory 122 is also an example of a memory unit and/or memory module.

[0064] In general, when processor 120 processes such instructions stored at memory 122, processor 120 is configured to: determine a current driver of vehicle 107; select a current encryption key from plurality of the driver-associated encryption keys 125 based on the current driver; collect, using communication interface 124, vehicle data from vehicle diagnostic monitor 103; encrypt the vehicle data using the current encryption key to produce encrypted vehicle data; and, transmit, using communication interface 124, the encrypted vehicle data to server 150.

[0065] Interface 124, is implemented as one or more radios and/or connectors and/or network adaptors, configured to wirelessly communicate with mobile device 105 and/or remote server, and vehicle diagnostic monitor 103, for example via link 115 and communication bus 113. It will be appreciated that, in these implementations, interface 124 can be configured to correspond with network architecture that is used to implement

one or more communication links to the one or more communication networks and/or devices, including but not limited to any suitable combination of USB (universal serial bus) cables, serial cables, wireless links, Bluetooth links, NFC (near field communication) links, packet based links, analog networks, access points, and the like, and/or a combination. When device 101 is configured to communicate with remote server 150, and/or an IoT platform, without the use of mobile device 105, 124 can be configured to correspond with network architecture that is used to implement one or more communication links to remote server 150, and/or an IoT platform, including but not limited to any suitable combination of any suitable combination of wired and/or wireless links, wired and/or wireless devices and/or wired and/or wireless networks, including but not limited to any suitable combination of USB (universal serial bus) cables, serial cables, wireless links, Bluetooth™ links, Zigbee™ links, NFC (near field communication) links, WiFi links, other packet based links, and the like.

[0066] As depicted, interface 124 is generally enabled to communicate with device 105 via link 115, and with vehicle diagnostic monitor 103 via communication bus 113. Hence, interface 124 can comprises one or more of: an OBD-II (on-board diagnostics) connector, an OBD (on-board diagnostics) connector, a USB (universal serial bus) connector, or other connector configured to communicate with vehicle diagnostic monitor 103 via communication bus 113.

[0067] Furthermore, in some implementations, interface 124 can be configured to communicate with infotainment unit 111, for example via communication bus 113; such communication can be used for enrolment of users, assignment of a key 125 to a user, logging into device 101, and the like.

[0068] Optional input device 128 can generally be enabled to receive input data, and can comprise any suitable combination of input devices, including but not limited to a keyboard, a keypad, a pointing device, a mouse, a track wheel, a trackball, a touchpad, a touch screen and the like. Other input devices are within the scope of present implementations.

[0069] While not depicted, device 101 can further comprise a power source, including but not limited to a battery and/or a power pack, and/or a connection to a power supply of vehicle 107, or any other suitable power source, as well as a housing and the like.

[0070] In any event, it should be understood that a wide variety of configurations for device 101 are contemplated.

[0071] Attention is now directed to Figure 3 which depicts a block diagram of a flowchart of a method 300 for collecting user-based insurance data in vehicles, according to non-limiting implementations. In order to assist in the explanation of method 300, it will be assumed that method 300 is performed using device 101, and specifically by processor 120 and when processor 120 processes instructions stored at memory 122. Indeed, method 300 is one way in which device 101 can be configured. Furthermore, the following discussion of method 300 will lead to a further understanding of device 101, system 100, and its various components. However, it is to be understood that device 101 and/or method 300 can be varied, and need not work exactly as discussed herein in conjunction with each other, and that such variations are within the scope of present implementations.

[0072] Regardless, it is to be emphasized, that method 300 need not be performed in the exact sequence as shown, unless otherwise indicated; and likewise various blocks may be performed in parallel rather than in sequence; hence the elements of method 300 are referred to herein as “blocks” rather than “steps”. It is also to be understood, however, that method 300 can be implemented on variations of device 101 as well.

[0073] At block 301, processor 120 determines a current driver of vehicle 107.

[0074] At block 303, processor 120 selects a current encryption key from a plurality of the driver-associated encryption keys 125 based on the current driver.

[0075] At block 305, processor 120 collects, using communication interface 124, vehicle data from vehicle diagnostic monitor 103.

[0076] At block 307, processor 120 encrypts the vehicle data using the current encryption key to produce encrypted vehicle data.

[0077] At block 309, processor 120 transmits, using communication interface 124, the encrypted vehicle data to remote server 150.

[0078] Method 300 will now be discussed with reference to Figs. 4 to 9, each of which are substantially similar to Fig. 2, with like elements having like numbers.

[0079] Attention is next directed to Fig. 4 which depicts a non-limiting implementation of block 301, in which processor 120 is further configured to determine the current driver of the vehicle by receiving log-in data 401 from input device of device 101. For example, as depicted, a log-in identifier 403 is stored in association with key 125-1 and identifies a driver associated with key 125-1; while only one log-in identifier 403 is depicted in Fig. 4, it is assumed that each key 125 is stored in association with a

respective log-in identifier. Log-in identifier 403 can be provisioned at device 101, as described above in conjunction with provisioning of keys 125. A current driver can be determined at processor 120 by receiving log-in data 401 and comparing log-in data 401 with the log-in identifiers stored at memory 122, including log-in identifier 403. A
5 current encryption key 125 can then be selected by processor 120 at block 303 based on a log-in identifier 403 that matches log-in data 401. As depicted, assuming that log-in identifier 403 matches log-in data 401, processor 120 selects key 125-1 as the current encryption key at block 303.

[0080] Alternatively, an input device of vehicle 107 located, for example, at dashboard
10 110 and/or at infotainment system 111 and/or at display 112 (e.g. a touchscreen), can be used to receive log-in data 401, which can be relayed to device 101 via communication bus 113, and a current encryption key 125 can then be selected by processor 120 at block 303 based on a log-in identifier 403 that matches log-in data 401 received at the input device of vehicle 107.

[0081] Furthermore, to address privacy issues, the driver can be prompted, e.g., at
15 mobile device 105 and/or at infotainment unit 111, whether or not they want their data to be tracked. When a “Yes” option is selected, then data is tracked. When a “No” option is selected, then data is not tracked, however this can result in the driver not receiving insurance deductions, for example when insufficient data is tracked they.

[0082] Thresholds for determining when insurance deductions are received can be set by an
20 insurance company in at remote server 150 and/or at an IoT platform. Moreover, in certain circumstances, the selection of “Yes” or “No” can itself be a data point that is tracked, as can the insertion and/or removal of the device 101.

[0082] To further address privacy issues, in some implementations, data at device 101
25 can be associated with fine-grained permissions, in that different types of data collected by device 101 can be tagged with different permission levels in memory 122. Such permission levels can be set, for example, by the owner of the vehicle, the owner of the insurance policy, the insurance company, and/or the owner of the data. In some implementations, a user, such as a driver, via an application at mobile device 105, can
30 select who can access what data. For example, the driver can elect to have their parents access the data and the insurance company access the data, or only the insurance company. Additionally, a parent can elect to access a child’s data, but opt not to share the child’s information with the insurance company. When a permission

level is received, a tag is stored to a record of data that is transmitted. Remote server 150 (and/or the IoT platform) can then associate the tag with who can access the data.

[0083] In any event, in these implementations, when a driver enters the vehicle, the driver can log-in to device 101 via input device 128 and/or an input device of vehicle 107, and device 101 can select a key 125 accordingly. It is assumed that log-in identifier 403 is unique for each driver of vehicle 107 and/or unique to each associated key 125.

[0084] However, other processes for determining a current driver at block 301 are within the scope of present implementations. For example, attention is next directed to Fig. 5 which depicts device 101 receiving driver identification data 501, which can be similar to or different from log-in data 401, from mobile device 105. For example, as depicted in Fig. 5, in these implementations, memory 132 at mobile device 105 can store driver identification data 501 and transmit driver identification data 501 to device 101 when mobile device 105 is in communication with device 101. Driver identification data 501 can be provisioned at mobile device 105 when a user-insurance application is installed at mobile device 105, for example using data that identifies a user of mobile device 105, whom is assumed to also be the driver and/or in conjunction with provisioning keys 125 at device 101 using mobile device 105, as described above. Similar driver identification data 503 is stored in association with key 125-1 and identifies a driver associated with key 125-1; while only one set of driver identification data 503 is depicted in Fig. 5, it is assumed that each key 125 is stored in association with respective driver identification data. Driver identification data 503 can be provisioned at device 101 in conjunction with provisioning keys 125 at device 101 using mobile device 105, as described above.

[0085] Hence, when a driver enters a vehicle with mobile device 105, mobile device 105 can automatically transmit driver identification data 501 to device 101. A current driver can be determined at processor 120 by receiving driver identification data 501 and comparing driver identification data 501 with driver identification data stored at memory 122, including driver identification data 503. A current encryption key 125 can then be selected by processor 120 at block 303 based on a driver identification data 503 that matches driver identification data 501. As depicted, assuming that driver identification data 503 matches driver identification data 501, and processor 120 selects key 125-1 as the current encryption key at block 303.

[0086] However, in some situations, two registered drivers of vehicle 107 can be present in vehicle 107, for example, one as a current driver and the other as a passenger; in these situations, each of the drivers can have a mobile device, each of which can transmit respective driver identification data to device 101. Hence, to determine which is the
5 current driver, log-in data 401 can also be received at processor 120 as described above. Alternatively, processor 120 can cause display 112 of vehicle 107 and/or display 136 of mobile device 105 (and/or of the second mobile device), using communication bus 113 and/or link 115 and the like, to render a request confirmation of a current driver. Respective input can be received at vehicle 107 and/or at mobile device 105 (and/or at
10 the second mobile device) confirming which of the drivers is the current driver. In yet further implementations, device 101 can comprise a display, and such a request for confirmation of a current driver can be rendered at the display of device 101. At this stage, permission to track data for the current driver can also be requested.

[0087] In yet further implementations, as depicted in Fig. 6, processor 120 can be further
15 configured to determine the current driver of vehicle 107 by comparing vehicle data 601 received from vehicle diagnostic monitor 103 with stored vehicle data 603 associated with the current driver and/or a given key 125. For example, a driver's habits in operating a vehicle can act as a type of unique signature, for example similar to hand writing, speech patterns and the like; such patterns can be collected and/or determined
20 and stored at memory 122 as stored vehicle data 603. When a current driver operates vehicle 107, vehicle data 601 can be collected and compared to stored vehicle data 603 to determine a current driver. Stored vehicle data 603 can comprise processed vehicle data comprising patterns and/or raw vehicle data.

[0088] For example, as depicted, stored vehicle data 603 is stored in association with
25 key 125-1 and identifies a driver associated with key 125-1; while only one set of stored vehicle data 603 is depicted in Fig. 6, it is assumed that each key 125 is stored in association with stored vehicle data. A current encryption key 125 can then be selected by processor 120 at block 303 based on stored vehicle data 603 matching vehicle data 601. As depicted, assuming that stored vehicle data 603 matches vehicle data 601,
30 processor 120 selects key 125-1 as the current encryption key at block 303. Such matching can comprise matching patterns in each of stored vehicle data 603 and vehicle data 601; such pattern matching need not be exact but can be within percentages of threshold values.

[0089] In some implementations processes for determining a current driver as described with reference to Figs. 4, 5 and 6 can be combined. For example, log-in data 401 and/or driver identification data 501 can be used to determine a current driver, vehicle data can be collected and stored as stored vehicle data 603 in association with a key 125 that is in turn stored in association with log-in data 401 and/or driver identification data 501; a next time the same driver operates vehicle 107, stored vehicle data 603 can be used to identify the driver and select a current encryption key.

[0090] Attention is next directed to Figs. 7 and 8, which depict an implementation of blocks 305, 307, 309. With reference to Fig. 7, at block 305, processor 120 collects vehicle data 701 from vehicle diagnostic monitor 103, and encrypts vehicle data 701, at block 307, using the key selected at block 303, for example key 125-1. As depicted in Fig. 8 encryption of vehicle data 701 produces encrypted vehicle data 801, which is transmitted to remote server 150, for example via mobile device 105 (e.g. via interface 124 and link 115), at block 309. In particular, vehicle data 701 can include, but is not limited to, when the vehicle was started, when the vehicle was stopped and/or turned off, speed of the vehicle, acceleration of the vehicle, braking of the vehicle, distance travelled by the vehicle, fuel consumption of the vehicle, idle time of the vehicle, deployment of airbags at the vehicle, location of the vehicle, and the like. In other words, vehicle diagnostic monitor 103 tracks and/or measures parameters of vehicle 107 which can be used to rate a driver for insurance and/or determine when a driver is speeding, how the driver accelerates, how often the driver brakes, and the like, and transmit such data to device 101 as vehicle data 701. In some of these implementations, vehicle data 701 can be time-stamped and/or each event recorded in vehicle data 701 can be time-stamped.

[0091] Mobile device 105 then transmits encrypted vehicle data 801 to server 150 using link 151.

[0092] Alternatively, at block 309, device 101 can transmit encrypted vehicle data 801 to server 150 using a link there between without using mobile device 105.

[0093] Regardless, server 150 can receive encrypted vehicle data 801 and use keys 155 to attempt to decrypt encrypted vehicle data 801; when successful decryption occurs producing vehicle data 701, for example using a given key 155-1, server 150 can store and/or process vehicle data 701 to produce a user-based insurance rating for the associated driver.

[0094] In some implementations vehicle data 701 can be encrypted at block 307 with an identifier of a current driver, for example, log-in identifier 403 and/or driver identification data 503, which can also be stored at server 150. Hence, when server 150 decrypts vehicle data 701, an identifier of a current driver can be determined. Similarly, encrypted vehicle data 801 can be transmitted with an unencrypted identifier of a current driver and the unencrypted identifier of a current driver can be used by server 150 to determine which key 155 to use to decrypt encrypted vehicle data 801. Indeed, in some implementations, encrypted vehicle data 801 can include the encrypted identifier of a current driver and can also be transmitted with the unencrypted identifier of a current driver such that when encrypted vehicle data 801 is decrypted, the two identifiers can be compared as a verification and/or as an integrity check. In yet a more complicated embodiment the driver identifier and vehicle data can be hashed and signed by the key 125 and the signed hash together with the unsigned data can be sent to the server 150. The server decrypts the signed hash using the corresponding private key 155, then hashes the unsigned data using a similar hash algorithm and compares the two hashes. If they correspond there is an integrity check.

[0095] Furthermore, vehicle data 701 can be encrypted to produce encrypted vehicle data 801 periodically and/or when vehicle 107 is shut down after block 301 occurs. In other words, blocks 305, 307 and 309 can be repeated periodically or can occur one time per each use of vehicle 107, a use of vehicle 107 comprising execution of blocks 301 to block 303, which can occur when vehicle 107 is turned on and/or started, to when vehicle 107 is turned off and/or shut down. Alternatively, blocks 305 to 307 can occur periodically and/or be repeated throughout a use of vehicle 107, and again at the end of a use of vehicle 107. In some implementations, vehicle 107 can include a system for detecting catastrophic occurrences at vehicle 107, for example deployment of airbags, crashes, and the like, and blocks 305 to 307 can also occur when such a catastrophic occurrence is detected; in these implementations, vehicle data 701 and encrypted vehicle data 801 can include an indication of such catastrophic occurrence such that an insurance company, and the like, can be informed of such immediately, and alternatively inform emergency services of such. In some implementations vehicle diagnostic monitor 103 can comprise a system for detecting catastrophic occurrences at vehicle 107.

[0096] In yet further implementations, mobile device 105 and/or device 101 can be configured to monitor whether mobile device 105 has been used during operation of the

vehicle, for example to make cellular telephone calls and/or to access the internet and/or whether a keyboard at mobile device 105 has been accessed during operation of the vehicle and/or to whether an input device (e.g. input device 138) has been accessed during operation of the vehicle. Such data can be incorporated into encrypted data 801 and /or transmitted to server 150 with encrypted vehicle data 801. In some of these implementations, device 101 can be configured to collect usage data from mobile device 105 and combine such usage data with vehicle data 701 prior to encryption, such that encrypted vehicle data 801 further comprises mobile device user data. Hence, in these implementations, processor 120 is further configured to combine vehicle data 701 with mobile device user data received from device 105 prior to encrypting vehicle data 701 at block 307 of method 300, such that encrypted vehicle data 801 includes encrypted mobile usage data.

[0097] Alternatively, mobile device 105 can be configured to: receive encrypted vehicle data 801 from device 101; and transmit encrypted vehicle data 801 to server 150 with mobile device user data. The mobile device user data can be time-stamped, as can vehicle data 701 (which can include start and stop times of usage of the vehicle), so that the two can be coordinated by server 150.

[0098] Persons skilled in the art will appreciate that there are yet more alternative implementations and modifications possible. For example, in some implementations, device 101 can be configured to be in a read-only mode with respect to data being requested by mobile device 105, server 150, and the like. For example, in these implementations while requests for data can be received on link 115, and data can be transmitted on link 115, but data cannot be received on link 115 and stored at memory 122. Hence, in such implementations, device 101 is prevented from being an attack vector for attempted hacking attempts on the vehicle. In particular, in some implementations, processor 120 can be further configured to place device 101 in a read-only mode when communication interface 124 is connected to vehicle diagnostic monitor 103.

[0099] Furthermore, device 101 can have at least two modes of communicating. For example, device 101 can communicate with remote server 150 (and/or IoT platform) directly when device 101 includes a cellphone modem, and device 101 can communicate with mobile device 105 when device 101 includes a USB and/or Bluetooth link (or other data connection) to mobile device 105. Other data connections to remote server 150 are

also within the scope of present implementations. For example, device 101 can be configured to communicate with an in-vehicle telematics connection (including, but not limited to an OnStar™ or E-Call system and the like). In some implementations, an insurance company can pay the data usage bill associated with collecting the vehicle data. In other implementations, systems can be used that track personal data usage vs. other types of data usage, including, but not limited to systems developed by Movirtu™. Such systems can separate data traffic between personal usage and that used for the insurance company (e.g. professional use). For example, mobile device 105 can be configured with such an application such that when device 101 transmits data via mobile device 150, this data can be recognized by mobile device 150, using a tag, a token, a parameter and the like, and then transmitted to a server in a network that allows tracking the data for personal and professional use. This can enable an insurance company to reimburse the driver for the data used to communicate the encrypted vehicle data, and other data for operating system 100.

[00100] Furthermore, device 101 can be further configured to reduce the risk of hacking. For example, a concern with insurance devices, such as device 101, is that they can be hacked: for example, a hacker could access to device 101 via mobile device 105 by hacking into the mobile device 105, and then gain control of vehicle 107 as when device 101 is connected to an OBD-II port, and hence a CAN bus, for example. To reduce such risk, in some implementations, when device 101 and remote server 150 (and/or IoT platform) authenticate each other they can establish a second key pair. This second key pair can comprise: a private key that can be used/stored by remote server 150; and an associated public key stored at device 101. Every incoming command from remote server 150 can be encrypted with the private key, by remote server 150, and device 101 can decrypt the commands using the public key. As it is unlikely that a hacker can use the same private key as remote server 150, such a scheme can prevent random commands from infecting device 101 and hence compromising vehicle 107. These keys can be regularly updated on a random schedule to ensure there is less chance to compromise them.

[00101] A further protection scheme could be implemented as follows:

[00102] 1. At remote server 150, encrypt a command (and/or message and the like) with the server private key.

[00103] 2. At remote server 150, generate a hash of the command and sign it with the device public key.

[00104] 3. At remote server 150, transmit both the encrypted command and the hash to device 101.

5 [00105] 4. At device 101, decrypt the encrypted command with a corresponding server public key.

[00106] 5. At device 101, unlocks the hash with a device private key.

[00107] 6. At device 101, process the decrypted command through a hash algorithm (i.e. the same algorithm used to generate the hash at remote server 150) and
10 compare the resulting hash with the unlocked hash to verify the command.

[00108] For a hacker to gain access to the system, the hacker would have to know the private keys of remote server 150 and device 101 and all the algorithms used, which reduced the chances of a hacker breaking in to system 100. Furthermore, as device 101 can be shipped with a remote server certificate, it can be difficult for a
15 hacker to replicate the remote server certificate.

[00109] Indeed, attention is now directed to Figure 9 which depicts a block diagram of a flowchart of a method 900 for securely remotely controlling devices in vehicles, according to non-limiting implementations. In order to assist in the explanation of method 900, it will be assumed that method 900 is performed using
20 system 100 and specifically device 101, and server 150. Indeed, method 900 is one way in which system 100 can be configured. Furthermore, the following discussion of method 900 will lead to a further understanding of system 100, device 101, and server 150. However, it is to be understood that system 100, device 101, and server 150 and/or method 900 can be varied, and need not work exactly as discussed herein in conjunction
25 with each other, and that such variations are within the scope of present implementations.

[00110] Regardless, it is to be emphasized, that method 900 need not be performed in the exact sequence as shown, unless otherwise indicated; and likewise various blocks may be performed in parallel rather than in sequence; hence the elements
30 of method 900 are referred to herein as “blocks” rather than “steps”. It is also to be understood, however, that method 900 can be implemented on variations of device 101 as well.

[00111] It is further appreciated that a portion of method 900 occurs at server 150 and a portion of method 900 occurs at device 101, with portions separated by a stippled line.

[00112] Furthermore, it is assumed in method 300 that server 150 and device 101 have exchanged their respective public keys and/or their respective public keys have been issued to each for example by a key issuing authority (which can also be server 150); hence, server 150 has received and/or stored (and/or generated) a device public key associated with device 101, and device 101 has received and/or stored a server public key associated with server 150. Furthermore, it is assumed that server 150 has received and/or stored (and/or generated) a server private key complementary to the server public key, and device 101 has received and/or stored a device private key complementary to the device public key. It is further assumed that each of device 101 and server 150 are configured to produce hashes using a same hash algorithm which has been previously provisioned at each of device 101 and server 150,

[00113] At block 901, server 150 encrypts a command (and/or message and the like) with the server private key.

[00114] At block 903, server 150 generates a hash of the command using the hash algorithm and signs it with the device public key.

[00115] At block 905, server 150 transmits both the encrypted command and the hash signed with the device public key to device 101.

[00116] At block 907, device 101 receives both the encrypted command and the hash signed with the device public key.

[00117] At block 909, device 101 decrypts the encrypted command with the corresponding server public key.

[00118] At block 911, device 101 unlocks the hash with a device private key.

[00119] At block 913, device 101 generates a hash of the decrypted command using the hash algorithm (i.e. the same algorithm used to generate the hash at remote server 150 at block 903).

[00120] At block 915, device 101 compares the hash of the decrypted command with the hash received by server 150 to determine if they are the same.

[00121] When the hashes are the same (a “Yes” decision at block 915”), at block 917 device 101 implements the decrypted command (e.g. the decrypted command is verified).

[00122] When the hashes are not the same (a “No” decision at block 915”), at block 919 device 101 discards the decrypted command (e.g. the decrypted command is not verified). Alternatively, device 101 can take remedial action at block 919, provide a warning at an output device, such as display 126, that an external device is attempting to hack device 101, and/or transmit a record of the transaction with server 150 to a trusted security authority (whose address has been provisioned at device 101, for example at memory 132).

[00123] Those skilled in the art will appreciate that in some implementations, the functionality of device 101, mobile device 105, and server 150 can be implemented using pre-programmed hardware or firmware elements (e.g., application specific integrated circuits (ASICs), electrically erasable programmable read-only memories (EEPROMs), etc.), or other related components. In other implementations, the functionality of device 101, mobile device 105, and server 150 can be achieved using a computing apparatus that has access to a code memory (not depicted) which stores computer-readable program code for operation of the computing apparatus. The computer-readable program code could be stored on a computer readable storage medium which is fixed, tangible and readable directly by these components, (e.g., removable diskette, CD-ROM, ROM, fixed disk, USB drive, flash memory, and the like). Furthermore, the computer-readable program can be stored as a computer program product comprising a computer usable medium. Further, a persistent storage device can comprise the computer readable program code. The computer-readable program code and/or computer usable medium can comprise a non-transitory computer-readable program code and/or non-transitory computer usable medium. Alternatively, the computer-readable program code could be stored remotely but transmittable to these components via a modem, network interface card, or other interface device connected to a network (including, without limitation, the Internet) over a transmission medium. The transmission medium can be either a non-mobile medium (e.g., optical and/or digital and/or analog communications lines) or a mobile medium (e.g., microwave, infrared, free-space optical or other transmission schemes) or a combination thereof.

[00124] A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by any one of the patent document or patent disclosure, as it

appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyrights whatsoever.

[00125] Persons skilled in the art will appreciate that there are yet more alternative implementations and modifications possible, and that the above examples are
5 only illustrations of one or more implementations. The scope, therefore, is only to be limited by the claims appended hereto.

What is claimed is:

1. A device comprising:
 - a processor, a memory storing a plurality of driver-associated encryption keys and a communication interface configured to communicate with a vehicle
 - 5 diagnostic monitor and a remote server, the processor configured to:
 - determine a current driver of the vehicle;
 - select a current encryption key from the plurality of the driver-associated encryption keys based on the current driver;
 - collect, using the communication interface, vehicle data from the
 - 10 vehicle diagnostic monitor;
 - encrypt the vehicle data using the current encryption key to produce encrypted vehicle data; and,
 - transmit, using the communication interface, the encrypted vehicle data to the remote server.
- 15 2. The device of claim 1, further comprising a removable dongle configured to removably connect to a communication bus.
3. The device of claim 1, wherein the communication interface comprises one or more of: an OBD (on-board diagnostics) connector, an OBD-II connector, a USB (universal serial bus) connector, an Ethernet bus connector, and a CAN (controller area
- 20 network) Bus connector.
4. The device of claim 1, wherein each of the driver-associated encryption keys comprises a respective private encryption key.
5. The device of claim 1, wherein each of the driver-associated encryption keys comprises an ECC (elliptical curve cryptography) key.
- 25 6. The device of claim 1, wherein the processor is further configured to determine the current driver of the vehicle by receiving log-in data from an input device of one or more of the vehicle, a mobile device, and the device.
7. The device of claim 1, wherein the processor is further configured to determine the current driver of the vehicle by receiving driver identification data from an input
- 30 device of one or more of the vehicle, a mobile device, and the device.

8. The device of claim 1, wherein the processor is further configured to combine the vehicle data with user data prior to encrypting the vehicle data.
9. The device of claim 1, wherein the processor is further configured to place the device in a read-only mode when the communication interface is connected to the vehicle diagnostic monitor.
10. A method comprising:
- at a device comprising: a processor, a memory storing a plurality of driver-associated encryption keys and a communication interface configured to communicate with a vehicle diagnostic monitor and a remote server:
- determining, at the processor, a current driver of the vehicle;
- selecting, at the processor, a current encryption key from the plurality of the driver-associated encryption keys based on the current driver;
- collecting, at the processor, using the communication interface, vehicle data from the vehicle diagnostic monitor;
- encrypting, at the processor, the vehicle data using the current encryption key to produce encrypted vehicle data; and,
- transmitting, at the processor, using the communication interface, the encrypted vehicle data to the second device.
11. The method of claim 10, wherein the communication interface comprises one or more of: an OBD (on-board diagnostics) connector, an OBD-II (on-board diagnostics) connector, a USB (universal serial bus) connector, an Ethernet bus connector, and a CAN (controller area network) Bus connector.
12. The method of claim 10, wherein each of the driver-associated encryption keys comprises a respective public encryption key.
13. The method of claim 10, wherein each of the driver-associated encryption keys comprises an ECC (elliptical curve cryptography) key.
14. The method of claim 10, further comprising determining the current driver of the vehicle by receiving log-in data from an input device of one or more of the vehicle, a mobile device, and the device.

15. The method of claim 10, further comprising determining the current driver of the vehicle by comparing the vehicle data with stored vehicle data associated with the current driver.

16. The method of claim 10, further comprising determining the current driver of the vehicle by receiving driver identification data from an input device of one or more of
5 the vehicle, a mobile device, and the device.

17. The method of claim 10, further comprising combining the vehicle data with user data received from a mobile device prior to encrypting the vehicle data.

18. The method of claim 10, further comprising placing the device in a read-only
10 mode when the communication interface is connected to the vehicle diagnostic monitor.

19. A non-volatile computer-readable medium storing a computer program,
wherein execution of the computer program is for:

at a device comprising: a processor, a memory storing a plurality of driver-associated encryption keys and a communication interface configured to communicate with a
15 vehicle diagnostic monitor and a remote server:

determining, at the processor, a current driver of the vehicle;

selecting, at the processor, a current encryption key from the plurality of the driver-associated encryption keys based on the current driver;

collecting, at the processor, using the communication interface, vehicle data
20 from the vehicle diagnostic monitor;

encrypting, at the processor, the vehicle data using the current encryption key to produce encrypted vehicle data; and,

transmitting, at the processor, using the communication interface, the encrypted vehicle data to the second device.

25

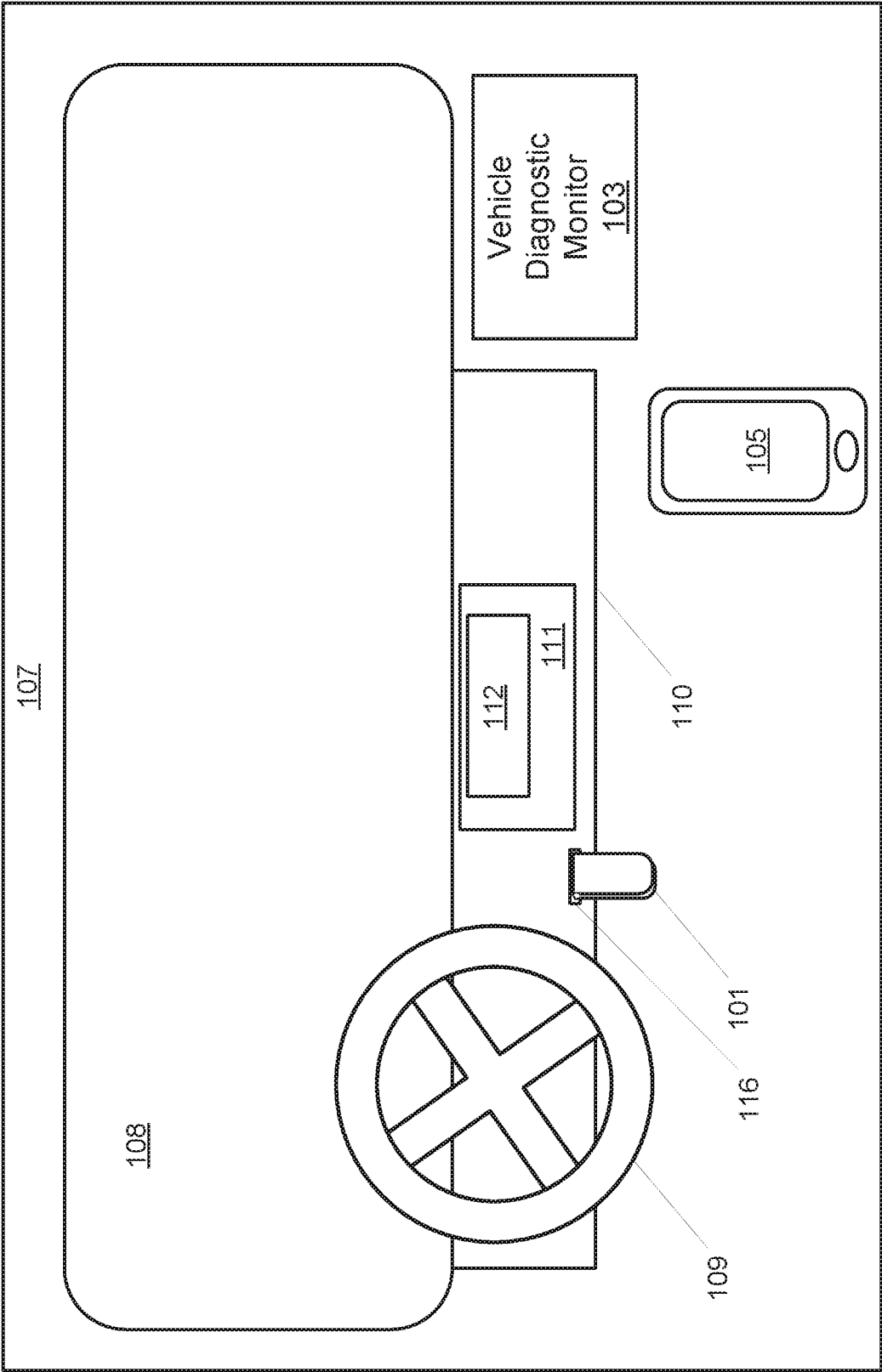


Fig. 1

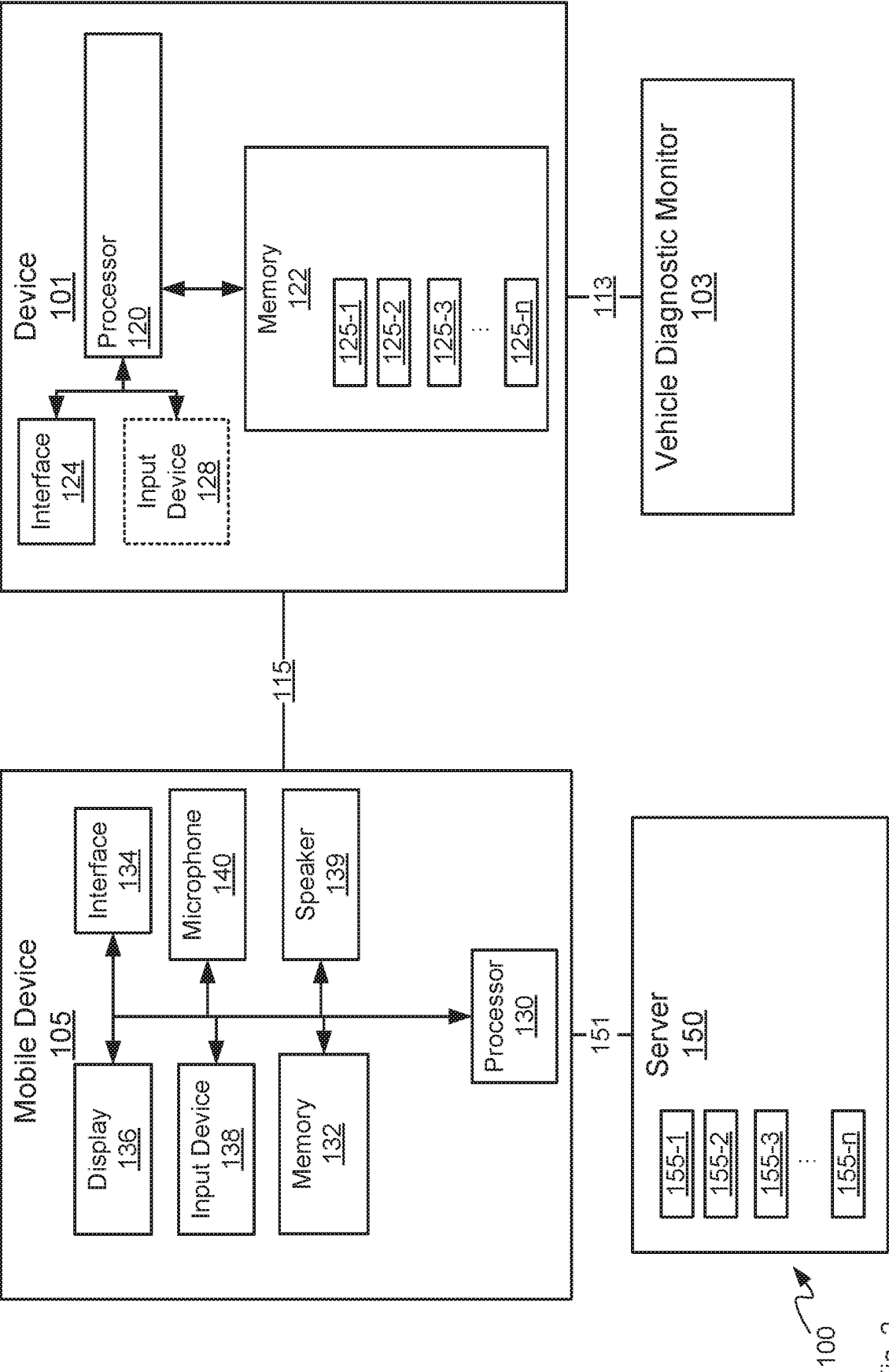
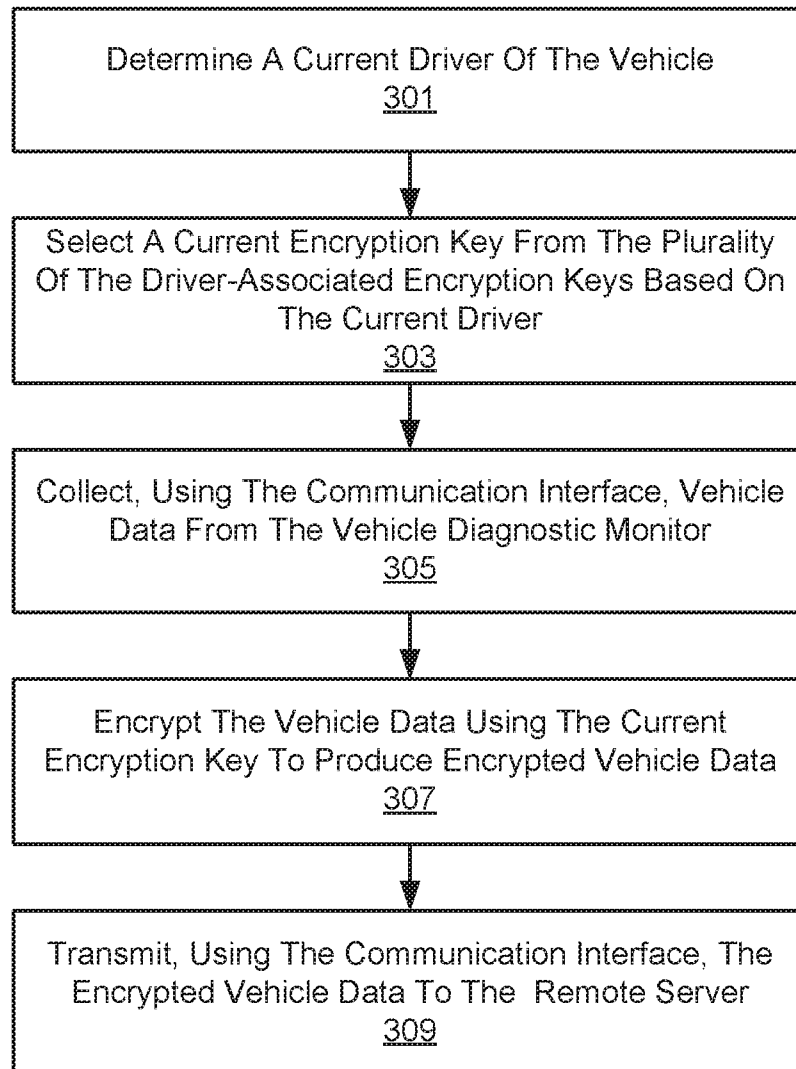


Fig. 2



300 ↗

Fig. 3

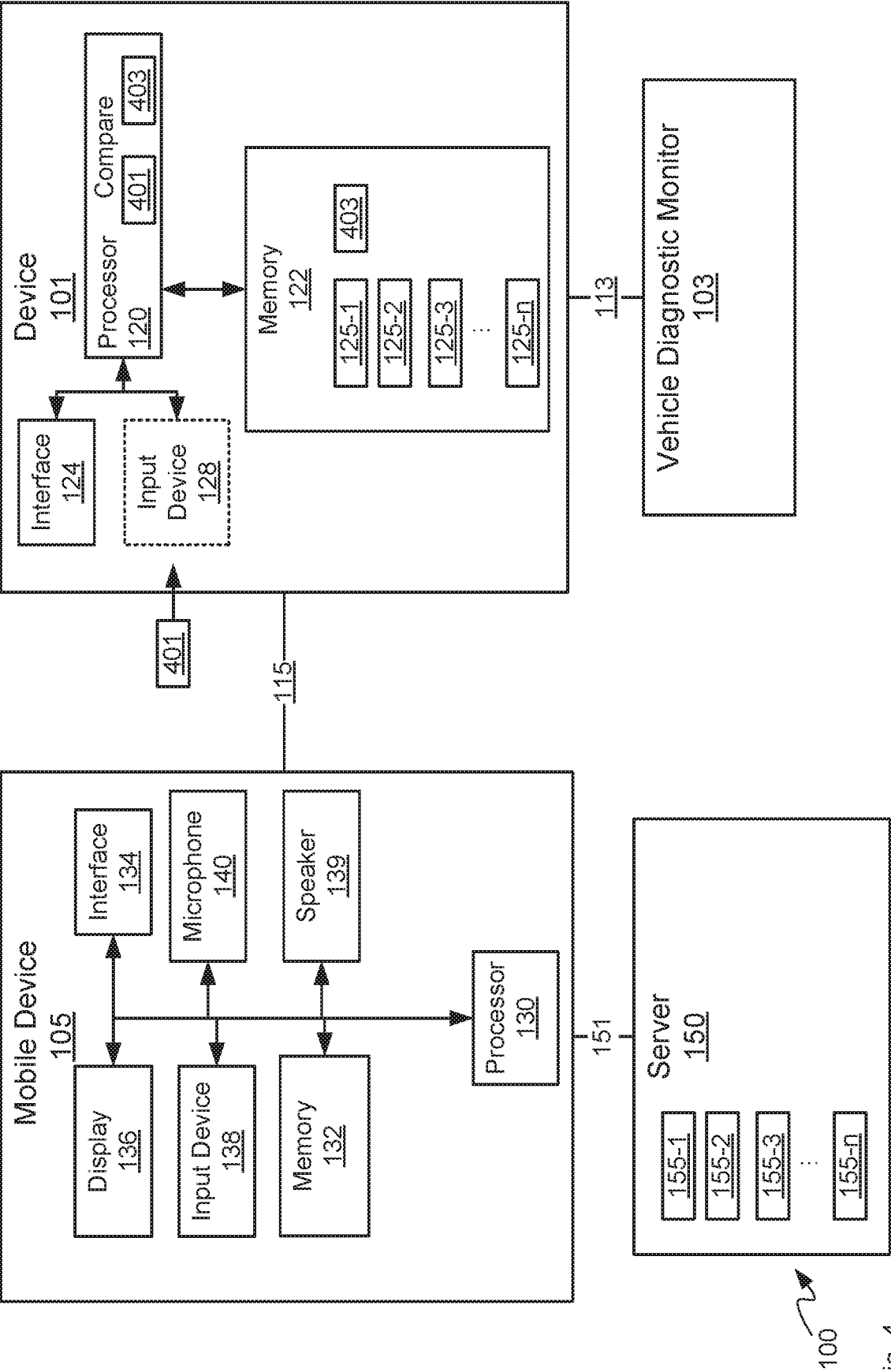


Fig. 4

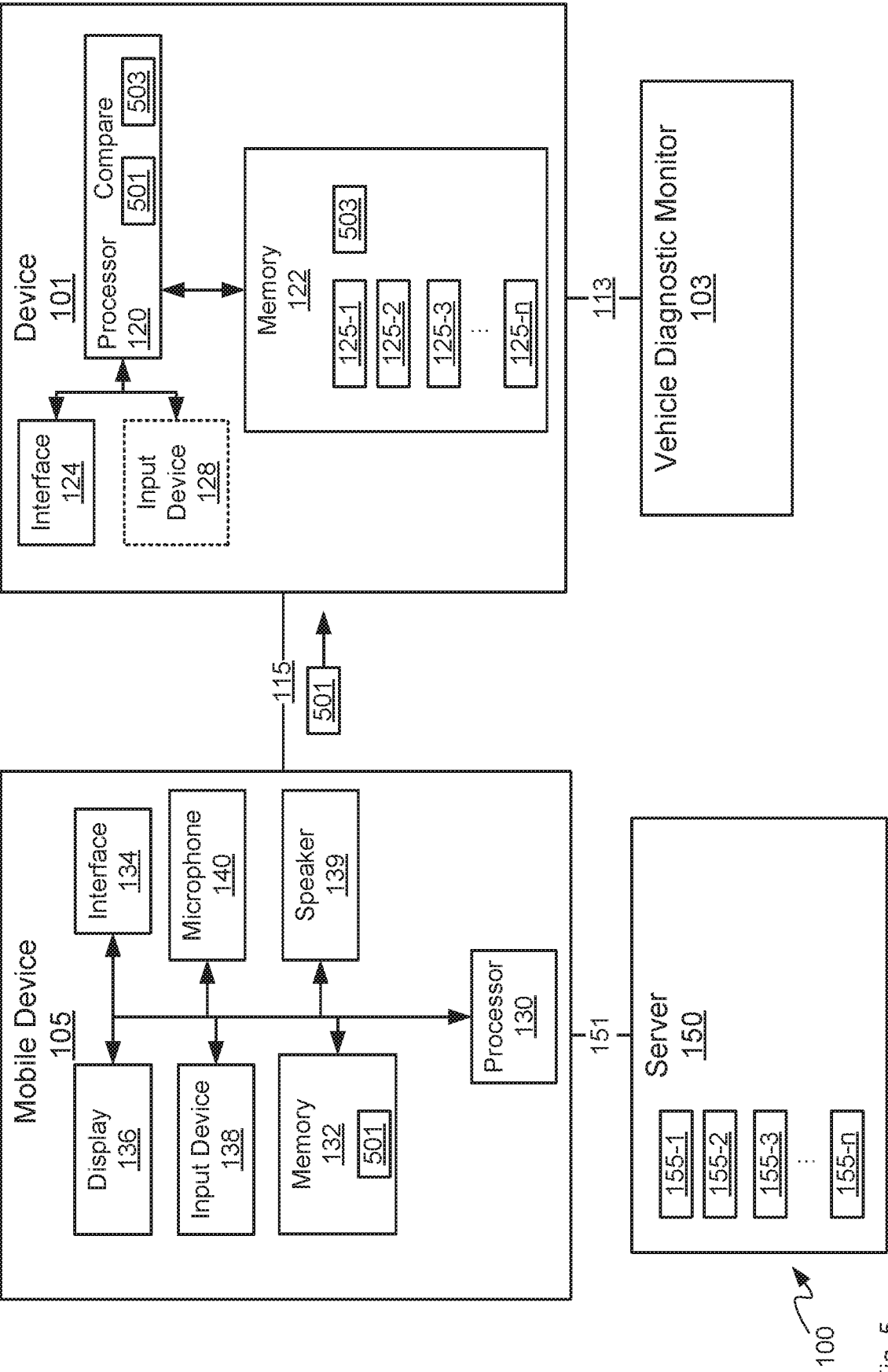


Fig. 5

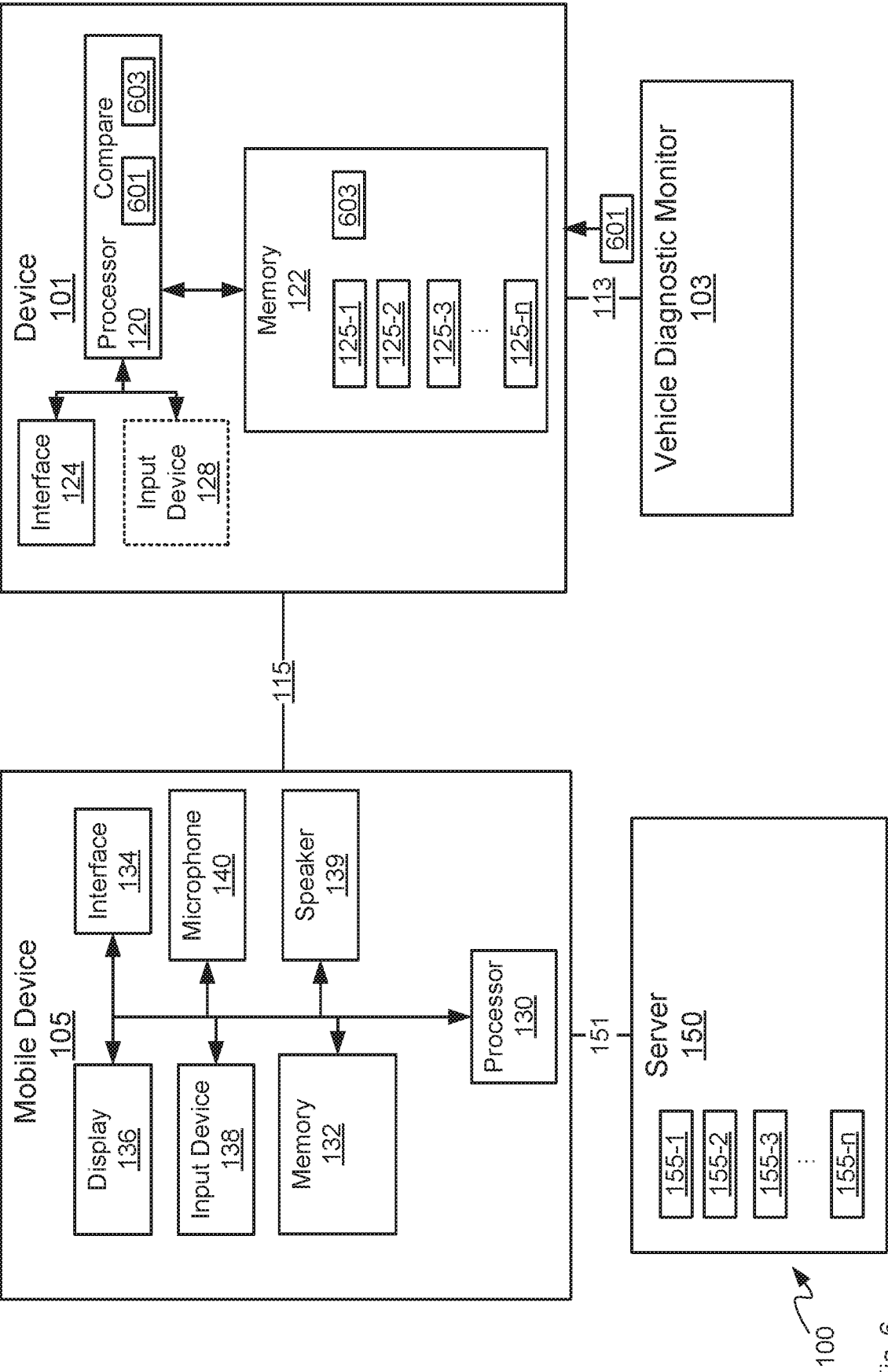


Fig. 6

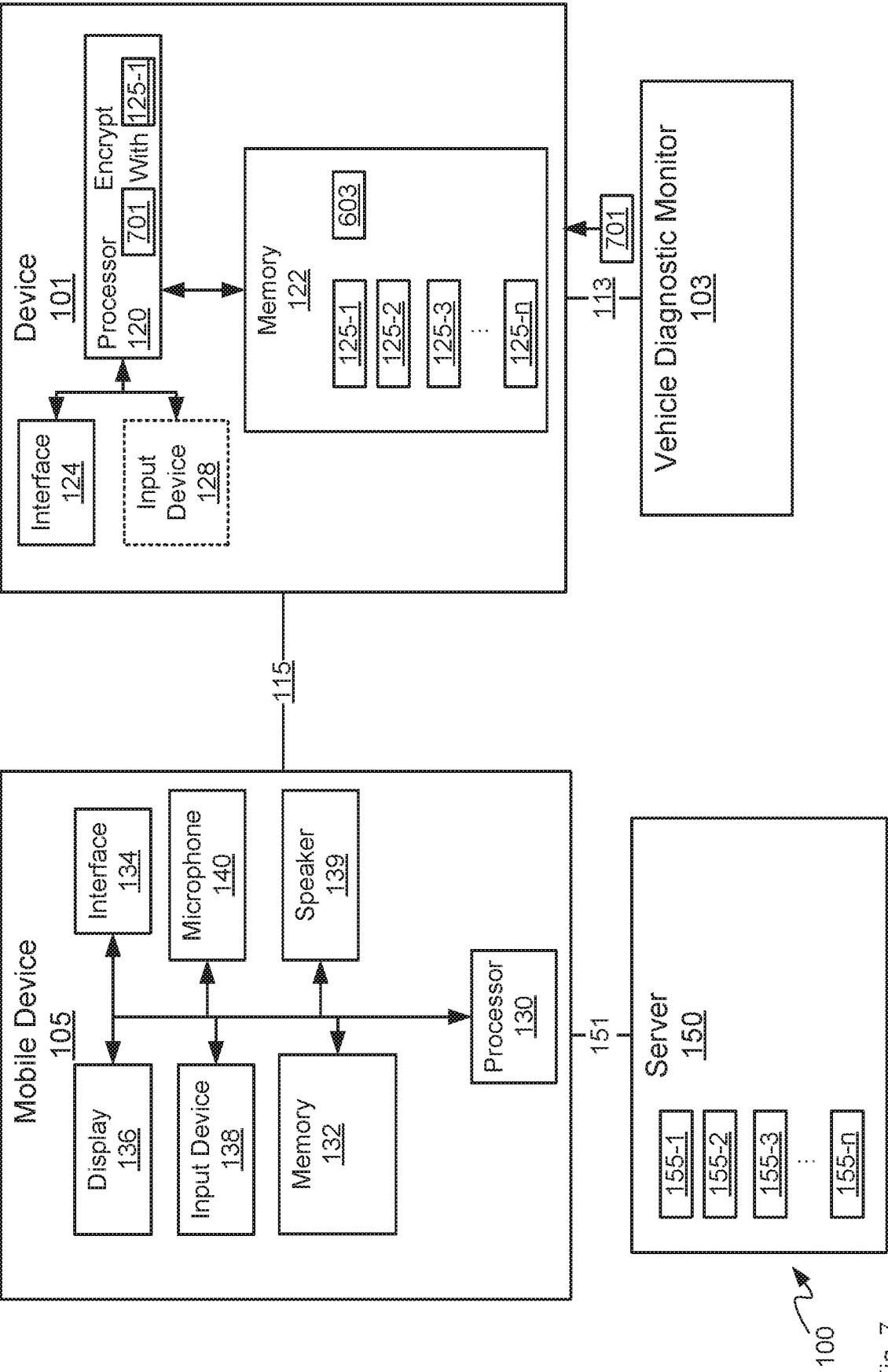


Fig. 7

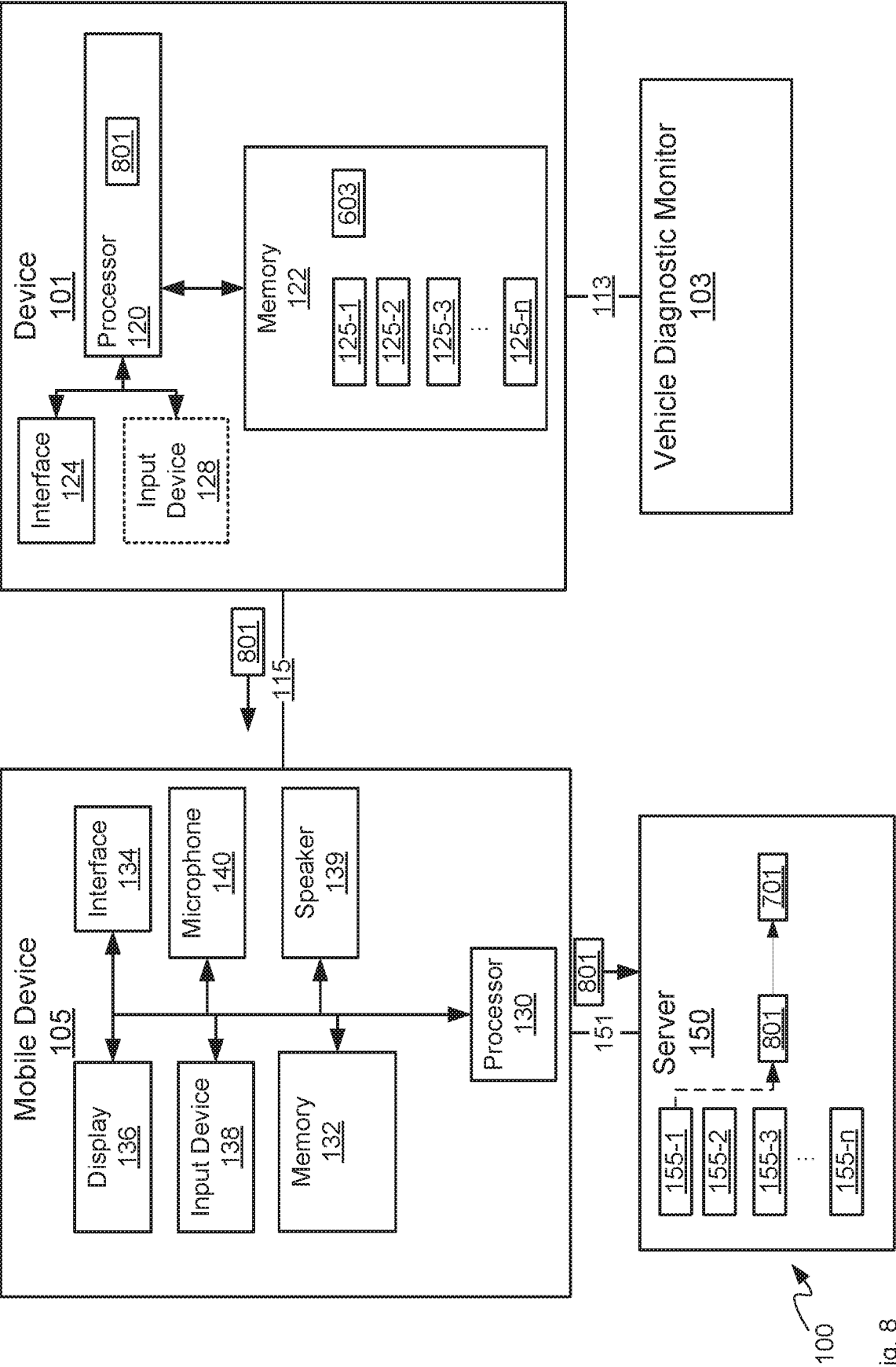


Fig. 8

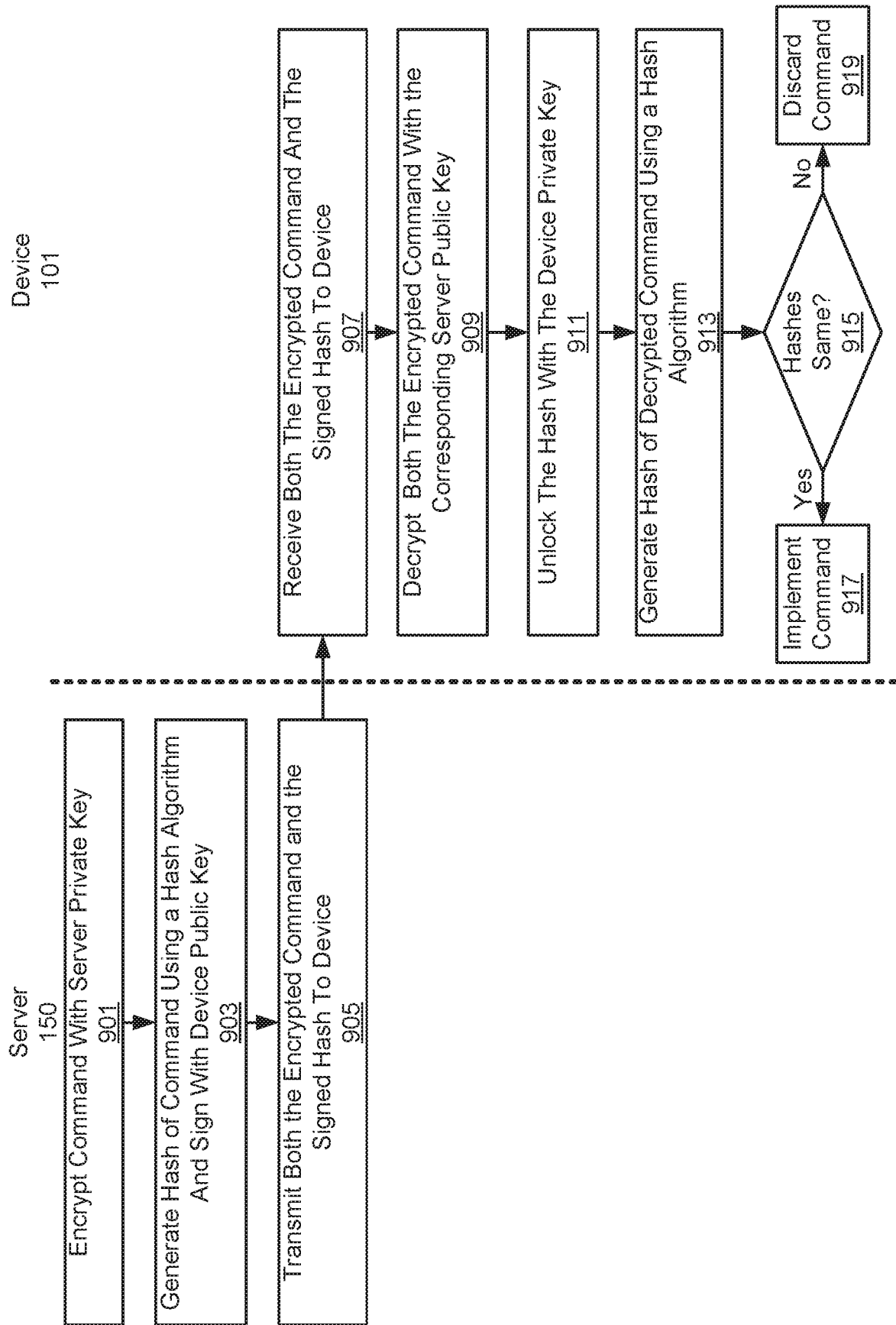


Fig. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/013002

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C5/00 G07C5/08
ADD. B60W40/09

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C B60W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 2 495 703 A1 (DATA TEC CO LTD [JP]) 5 September 2012 (2012-09-05) abstract paragraph [0001] paragraph [0018] - paragraph [0019] paragraph [0027] - paragraph [0046] paragraph [0063] - paragraph [0066] paragraph [0081] - paragraph [0090] paragraph [0106] figures 1,2,7B,8-10,13,14 paragraph [0118] - paragraph [0121] ----- -/-	1-14, 16-19 15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

5 April 2017

Date of mailing of the international search report

25/04/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Post, Katharina

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/013002

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014/195100 A1 (LUNDGAARD SOREN K [US] ET AL) 10 July 2014 (2014-07-10) abstract paragraph [0008] - paragraph [0012] paragraph [0041] paragraph [0050] - paragraph [0052] paragraph [0063] paragraph [0094] figures 1,5 -----	1-4, 10-12,19
A	US 2012/197486 A1 (ELLIOTT BRYANT [US]) 2 August 2012 (2012-08-02) abstract paragraph [0005] paragraph [0033] - paragraph [0043] figures 1,4,5 -----	1-3,10, 11
Y	US 2012/283893 A1 (LEE JIN-WOO [KR] ET AL) 8 November 2012 (2012-11-08) abstract paragraph [0019] paragraph [0026] figures 2,4 -----	15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2017/013002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2495703	A1	05-09-2012	EP 2495703 A1 05-09-2012
			JP 4729137 B1 20-07-2011
			JP 2012185537 A 27-09-2012
			US 2012224827 A1 06-09-2012

US 2014195100	A1	10-07-2014	NONE

US 2012197486	A1	02-08-2012	NONE

US 2012283893	A1	08-11-2012	CN 102774382 A 14-11-2012
			DE 102012207458 A1 08-11-2012
			US 2012283893 A1 08-11-2012
