



- (51) **International Patent Classification:**
H04L 9/08 (2006.01)
- (21) **International Application Number:**
PCT/US2015/037614
- (22) **International Filing Date:**
25 June 2015 (25.06.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
14/467,252 25 August 2014 (25.08.2014) US
- (71) **Applicant:** INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95054 (US).
- (72) **Inventors:** ANDIAPPAN, Rajasekaran; Arkkitechdinkatu 38 C 31, 33720 Tampere (FI). SENGUPTA, Uttam, K.; 14192 NW Meadowridge Drive, Portland, OR 97229 (US). KUPERMANN, Eli, Elik; HaShaham 38/3, 98577 Maale Adumim (IL). JOSHI, Mandar; 19950 Bonnie Ridge Way, Saratoga, CA 95070 (US).
- (74) **Agent:** SHICHRUR, Naim, Avraham; Shichrur & CO., c/o CPA Global, P.O. Box 52050, Minneapolis, MN 55402 (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, 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, KN, KP, KR, 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.

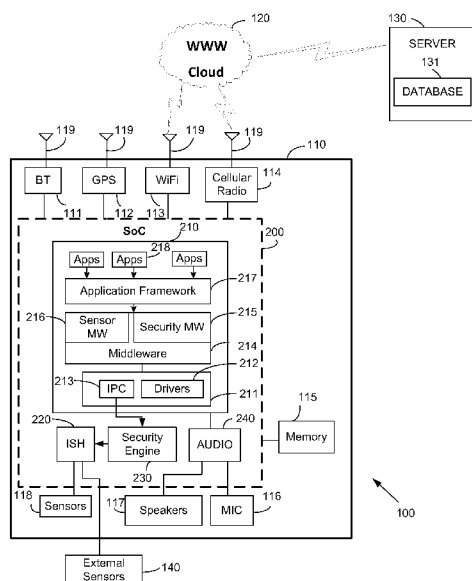
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, 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).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

(54) **Title:** HANDLING SENSOR DATA**FIG. 1**

(57) **Abstract:** An apparatus, a system and a method for securing sensor data by a security engine circuitry of a system on chip (SoC). For example, the security engine may receive from a processor circuitry of the SoC an inter processor communication (IPC) request to secure sensor data, and may send to an integrated sensor hub (ISH) of the SoC an IPC request to receive sensor data. The ISH may collect sensor data from one or more internal and/or external sensors, and may send the collected sensor data to the security engine. The security engine may receive the collected sensor data from the ISH, may secure the collected sensor data, and may send secured sensor data to the processor circuitry.

HANDLING SENSOR DATA

TECHNICAL FIELD

[0001] Some embodiments described herein generally relate to handling sensor data.

5

BACKGROUND

[0002] Today, handheld devices, such as Smartphones and tablets, rely on sensor data (accelerometer, gyro, magnetometer, pressure, ambient light, temperature, etc.) to enhance the user experience (UX) for a whole range of applications (e.g., phone settings, games) and offer new features (e.g., always-on sensing, motion-based gestures, user activity state, pedometer, etc.) to enable new categories of applications. Besides motion sensors and other ambient sensors, applications on mobile devices also use sensor data from other sensors, such as, audio (e.g., for voice authentication), camera (e.g., for face recognition, augmented reality), always-on location (using GPS, WiFi, 3G/LTE, dead-reckoning), and the like.

10

15

[0003] The sensor data may include user sensitive, personal and private information, such as user health related information, audio information, camera pictures and video, and/or user location. This user information is not protected and/or secured, while provided to backend services, and may be downloaded and viewed by unwanted entities and/or persons. Thus, there is a need to protect and secure the user information.

20

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] For simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity of presentation. Furthermore, reference
5 numerals may be repeated among the figures to indicate corresponding or analogous elements. The figures are listed below.

[0005] FIG. 1 is a schematic block diagram illustration of a system including a mobile device, a cloud, and a server, in accordance with some demonstrative embodiments.

[0006] FIG. 2 is a schematic flow-chart illustration of a method of securing a sensor data at
10 system on chip (SoC), in accordance with some demonstrative embodiments.

[0007] FIG. 3 is a schematic block diagram illustration of a mobile device, in accordance with some demonstrative embodiments.

[0008] FIG. 4 is a schematic illustration of a product of manufacture, in accordance with some demonstrative embodiments.

15 [0009] Reference will now be made to the exemplary embodiments illustrated, and specific language will be used herein to describe the same. It will nevertheless be understood that no limitation of the scope of the disclosure is thereby intended.

DETAILED DESCRIPTION

[0010] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of some embodiments. However, it will be understood by persons of ordinary skill in the art that some embodiments may be practiced without these specific details. In other instances, well-known methods, procedures, components, units and/or circuits have not been described in detail so as not to obscure the discussion.

[0011] Discussions herein utilizing terms such as, for example, “processing”, “computing”, “calculating”, “determining”, “establishing”, “analyzing”, “checking”, or the like, may refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing device, that manipulate and/or transform data represented as physical (e.g., electronic) quantities within the computer’s registers and/or memories into other data similarly represented as physical quantities within the computer’s registers and/or memories or other information storage medium that may store instructions to perform operations and/or processes.

[0012] The terms “plurality” and “a plurality”, as used herein, include, for example, “multiple” or “two or more”. For example, “a plurality of items” includes two or more items.

[0013] References to “one embodiment,” “an embodiment,” “demonstrative embodiment,” “various embodiments,” etc., indicate that the embodiment(s) so described may include a particular feature, structure, or characteristic, but not every embodiment necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrase “in one embodiment” does not necessarily refer to the same embodiment, although it may.

[0014] As used herein, unless otherwise specified the use of the ordinal adjectives “first,” “second,” “third,” etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

[0015] Some embodiments may be used in conjunction with various devices and systems, for example, a Personal Computer (PC), a User Equipment (UE), a Mobile Device (MD), an Internet of Things (IoT) device, a desktop computer, a mobile computer, a laptop computer, a notebook computer, a tablet computer, an UltrabookTM computer, a Smartphone device, a server computer, a handheld computer, a handheld device, a Personal Digital Assistant (PDA) device, a handheld PDA device, an on-board device, an off-board device, a hybrid device, a vehicular device, a non-vehicular device, a mobile or portable device, a consumer device, a non-mobile or non-portable device, a wireless communication station, a wireless communication device, a wireless Access

Point (AP), a wired or wireless router, a wired or wireless modem, a video device, an audio device, an audio-video (A/V) device, a wired or wireless network, a cellular network, a cellular node, a handheld device, e.g., a Smartphone, a Wireless Application Protocol (WAP) device, vending machines, sell terminals, and the like.

5 [0016] The phrases “wireless device” and/or “mobile device”, as used herein, includes, for example, a device capable of wireless communication, a communication device capable of wireless communication, a communication station capable of wireless communication, a portable or non-portable device capable of wireless communication, or the like. In some demonstrative embodiments, a wireless device may be or may include a peripheral that is integrated with a
10 computer, or a peripheral that is attached to a computer. In some demonstrative embodiments, the phrase “wireless device” and/or “mobile device” may optionally include a wireless service.

[0017] The term “communicating” as used herein with respect to a wire and/or wireless and/or internal communication signal includes transmitting the communication signal and/or receiving the communication signal. For example, a communication unit, which is capable of
15 communicating a communication signal, may include a transmitter to transmit the communication signal to at least one other communication unit, and/or a communication receiver to receive the communication signal from at least one other communication unit.

[0018] Reference is made to FIG. 1, which schematically illustrates a system 100 including a mobile device 110, a World Wide Web (WWW) cloud 120, and a server 130, in accordance with
20 some demonstrative embodiments. One or more external sensors 140 may be operably coupled to mobile device 110, if desired.

[0019] According to some exemplary embodiments, system 100 may include a wireless local area network (WLAN), a cellular network, a local area network (LAN), a wide area network (WAN), a wireless WAN, or the like.

25 [0020] According to some non-limiting embodiments, for example, mobile device 110 may include a wireless mobile device such as, for example, a cellphone, a Smartphone, a wearable device, a tablet, a laptop computer, an Internet of things (IoT) device, and the like.

[0021] According to a non-limiting exemplary embodiment, mobile device 110 may include a system on chip (SoC) circuitry and/or logic 200, a Bluetooth (BT) circuitry 111, a global
30 positioning system (GPS) receiver 112, a wireless local area network (WLAN) radio 113, e.g., a Wireless-Fidelity (WiFi) radio, a memory 115, a microphone (MIC) 116, one or more speakers 117, one or more sensors 118, and one or more antennas 119, e.g., a plurality of antennas 119.

[0022] According to some non-limiting embodiments, SoC circuitry 200 may include a

processor circuitry 210, an integrated sensor hub (ISH) 220, a security engine circuitry 230, and/or an audio circuitry 240, if desired.

[0023] For example, processor circuitry 210 may include, but not limited to, a kernel layer 211 which may include, for example, one or more drivers 212 and an inter-processor communication (IPC) logic 213; a middleware (MW) layer 214, which may include, for example, a security MW logic 215, and a sensor MW logic 216; an application framework layer 217; and one or more applications 218, e.g., operably coupled to application framework layer 217, if desired.

[0024] In some demonstrative embodiments, ISH 220 may include a sensor data acquisition (DAQ) and sensor fusion. ISH 220 may perform sensor processing, e.g., all sensor processing, required for an OS in processor circuitry 210, and may also perform continuous sensing usages, e.g., when a platform of device 110 is in a low power state, e.g., a lowest power state.

[0025] In some demonstrative embodiments, sensors 118 may be connected to ISH 220 by a wired or a wireless I/O bus. For example, ISH 220 may include a processor core, which may, for example, operate at a speed of 100 Megahertz (MHz) or any other speed, and ISH 220 may handle more complex workloads in a responsive fashion, if desired.

[0026] In another demonstrative embodiment, ISH 220 may include a paging architecture for code-provider flexibility in handling larger code sizes, if desired. For example, ISH 220 may include a direct IPC channel to processor circuitry 210, security engine 230, Audio DSP 240, an image processor (not shown), and the like.

[0027] According to some demonstrative embodiments, ISH 220 may collect data and/or communicate with one or more external sensors 140, which, for example, may be connected with a low power radio protocol. According to another example external sensors 140 may be connected to ISH 220 via a wireless link. Thus, exemplary embodiments of ISH 220 may become the communication Hub for collecting data from external sensor pods.

[0028] ISH Firmware of ISH 220 may be secure. For example, the ISH firmware may be configured to perform sensor DAQ and processing, may be integrity checked and loaded from a signed firmware image, e.g., from external memory 115.

[0029] The above embodiments may apply to other IP blocks that are used to offload for example, audio processing (Audio DSP), camera image processing (Imaging Signal Processor), location (GNSS/GPS, WiFi, 3G/LTE), and the like.

[0030] In some demonstrative embodiments, a user of mobile device 110 may use one or more applications 218 operated on mobile device 110, for example, to transfer user data. The user data

may be collected by one or more sensors 118 and or one or more external sensors 140, and provided, e.g., through WWW cloud 120 or via any other medium, to server 130, for example, a backend server or any other server. For example, the user data may include medical data such as, for example, blood pressure data, sugar level data, heartbeat data, stress data, and the like.

5 Additionally or alternatively, the user data may include user location data, image data, video data, audio data, private data such as, for example, contacts list data, blog data, password data, bank account information, and/or any other private information, sensitive information, and/or information and/or data to be protected or secured.

[0031] According to some exemplary embodiments, application 218 may receive user data, may
10 validate a certificate, and may locally logs the user data. According to another example, the user data may be sent to WWW cloud 120, where the certificate is verified and further heuristics may be performed to match data patterns with historical data from the same user. Thus, preventing false information or outliers in the data getting logged. The user may change the privacy setting of the secure sensing, e.g., ordering ISH 220 not to forward data from some health sensors to the
15 host. Security engine 230 may encrypt data so that only the remote web service can open it, if desired.

[0032] According to some demonstrative embodiments, mobile device 110 may include an enhanced privacy identifier (EPID) provisions and software (not shown), and server 130 may include EPID software and an access to a corresponding public key, for example, from an issuer
20 of the EPID keys.

[0033] According to some demonstrative embodiments, mobile device 110 may be configured to transfer the user data in a secure manner to server 130 e.g., the backend server. For example, application 218 may create a verified device message and may send the verified device message to security engine 230. Security engine 230 may sign the verified device message by using for
25 example, the EPID protocol, and/or digital signature standard (DSS). The Signed message may be transferred from security engine 230 to a host side application (not shown). The host side application may send the signed message to the server 130.

[0034] In some demonstrative embodiments, server side SW (not shown) may use an Issuer's public key to attest that the signature belongs to mobile device 110 in good standing. Once the
30 connection between mobile device 130 and server 130 is established, the EPID Sigma protocol may be used to exchange session keys, for example, session key (SK) encrypt messages, master keys (MK), integrity protects messages, or the like. The SK may be transferred to the security engine 230, if desired.

[0035] According to some demonstrative embodiments, the sensor data from sensors 118 and/or 140, for example, user health related data, audio data, camera data, location data, or other Personally Identifiable Information (PII) data, may be transferred to server 130, e.g., in a secure manner. For example, application 218 may request certified sensor data related to user health.

5 ISH 220 may gather the sensor data from sensors 118 and/or 140, and may transfer the sensor data to security engine 230. Security engine 230 may encrypt the sensor data, e.g., with the SK and the MK, for example, to sign the sensor data, and thus, apply an integrity protection to the sensor data.

10 [0036] In some demonstrative embodiments, security engine 230 may pass the encrypted sensor data to application 218, which operates on processor circuitry 210. The encrypted sensor data may be sent on a secure channel to server 130. Server 130, e.g., the backend server, may use a copy of the SK, e.g., to decrypt the encrypted sensor data. Server 130 may verify that the integrity of the sensor data has not been compromised.

15 [0037] In some demonstrative embodiments, server 130 may process the sensor data, e.g., to complete checking the sensor data, to consume the data, and/or to complete any necessary analysis, and may, optionally, securely send an output of processing the sensor data back to application 218 on mobile device 110.

20 [0038] Advantageously, a device, e.g., mobile device 110, equipped with EPID may be recognized by a backend server, e.g., server 130 as a device associated with a certain level of trust/security capabilities. For example, the device may use a Sigma protocol to setup a session oriented secure channel from the device to the backend server. In alternative embodiments, the device may implement a public key infrastructure (PKI), e.g., directly in security engine 230, to generate a key pair and establish a secure channel between mobile device 110 and server 130 for user authentication and transfer of sensor data.

25 [0039] According to some demonstrative embodiments, for example, SoC 200 may be configured to secure sensor data, e.g., from sensors 118 and/or 140. Processor circuitry 210 may be configured to collect and update sensor data to a service. ISH 220 may be configured to collect and process the one or more sensors data.

30 [0040] In some demonstrative embodiments, security engine 230 may be configured to receive the sensor data from the ISH 220. Security engine 230 may certify the sensor data, and may send certified sensor data to middleware framework 214. Security engine 230 may be configured to receive from IPC 213 of processor circuitry 210 an IPC request to provide the secure sensor data. Security engine 230 may be configured to send to ISH 220 the IPC request, to add a certificate to

the requested sensor data, and to send the certified requested sensor data to processor circuitry 210.

[0041] According to some demonstrative embodiments, security engine 230 may be configured to generate at least one encryption key to encrypt the sensor, data and to add a certificate to the sensor data. For example, the certified requested sensor data may be delivered to middleware (MW) framework 214 of the processor circuitry 210.

[0042] For example, the certified requested sensor data may be configured to be used by a service in mobile device 110 and/or in cloud 120. The certified requested sensor data may be configured to be certified against user credentials, and to be logged to a database 131 in server 130.

[0043] Reference is made to FIG. 2, which schematically illustrates a method of securing a sensor data at a system on chip (SoC) 200, in accordance with some demonstrative embodiments. For example, a secure and/or hardware certified data 250 (FIG. 2) may flow from processor circuitry 210 to security engine 230, from security engine 230 to ISH 220 and back to security engine 230, and to application 218 (Fig. 1), which may be running on an operating system (OS) of processor circuitry 210. For example, the OS may be an Android™ OS, an Apple® iOS®, a Windows® OS, or the like.

[0044] According to some alternative embodiments, ISH 220 may include one or more IP blocks such as, for example, audio, sensor, imaging, and the like. For example, ISH 220 may collect data from one or more sensors, a microphone, a camera and the like, e.g., as described above, although it should be understood that other alternative embodiments with different IP blocks may be used.

[0045] As indicated at block 300, according to some demonstrative embodiments, for example, the method of Fig. 2 may be initiated by an application e.g., application 218 (Fig. 1), operated over the operating system (OS) of processor circuitry 210. Application 218 (Fig. 1) may request certified data from, for example, one or more sensors, e.g., sensors 118 and/or 140 (Fig. 1). At processor circuitry 210, middleware (MW) 214 (Fig. 1) and/or an OS framework component may translate the request to a system call (text box 305). MW 214 (Fig. 1) and/or the OS framework component may redirect the system call to a security engine device driver (text box 310). The security engine device driver may send an IPC 213 (Fig. 1) to security engine 230 (text box 315).

[0046] As indicated at block 320, security engine 230 may check the validity of the request and that the ISH FW is in operation. Security engine 230 may send IPC 213 (Fig. 1) to ISH 220, e.g.,

to request ISH 220 to gather sensor data and return processed data (text box 325). While ISH 220 gathers the sensor data, security engine 230 may go to a lower power state mode and/or may execute other tasks (text box 327).

[0047] According to some exemplary embodiments, ISH 220 may receive IPC 213 (Fig. 1) and may start an execution thread (text box 330). ISH 220 may collect sensor data (text box 335), may process the sensor data, and may store the processed sensors data in a memory e.g., memory 115 (Fig. 1), if desired (text box 340). ISH 220 may send the processed data to security engine (text box 345).

[0048] According to some exemplary embodiments, security engine 22 may receive the processed data from ISH 220, may use a session key to encrypt the processed data and may use one or more unique keys to add a certificate to the processed data (text box 350). For example, security engine 230 may negotiate the session key with WWW cloud 120 (Fig. 1), if desired. Security engine 230 may send the processed certified data to processor circuitry 210 (text box 355).

[0049] As indicated at block 360, a security engine device driver (not shown) of processor circuitry 210 may receive the certified sensor data and may pass it to sensor MW 216 (Fig. 1). Application 218 (Fig. 1) may receive the certified sensor data, and may pass certified sensor data 250 to a service in WWW cloud 120 (Fig. 1) (text box 365). The certified sensor data may be decrypted. The certificate may be verified against user credentials, and logged to a database e.g. database 131 (Fig. 1) at server 130 (Fig. 1), if desired (text box 370).

[0050] Reference is made to FIG. 3, which schematically illustrates a mobile device, in accordance with some demonstrative embodiments. The mobile device may include, for example, a user equipment (UE), a mobile station (MS), a mobile wireless device, a cell phone, a Smartphone, a mobile communication device, a tablet, a handset, or other type of mobile wireless device. The mobile device may include one or more antennas configured to communicate with a transmission station, such as a base station (BS), an evolved Node B (eNB), a base band unit (BBU), a remote radio head (RRH), a remote radio equipment (RRE), a relay station (RS), a radio equipment (RE), or other type of wireless wide area network (WWAN) access point. The mobile device may be configured to communicate using at least one wireless communication standard including 3GPP LTE, 3GPP UMTS, GSM, WiMAX, High Speed Packet Access (HSPA), Bluetooth, and WiFi. The mobile device may communicate using separate antennas for each wireless communication standard or shared antennas for multiple wireless communication standards. The mobile device may communicate in a WLAN, a wireless personal area network (WPAN), and/or a WWAN.

[0051] FIG. 3 also provides an illustration of a microphone and one or more speakers that may be used for audio input and output from the mobile device. The display screen may be a liquid crystal display (LCD) screen, or other type of display screen such as an organic light emitting diode (OLED) display. The display screen can be configured as a touch screen. The touch screen
5 may use capacitive, resistive, or another type of touch screen technology. A SoC 200 (FIG. 1), which may include processor circuitry 210 (FIG. 1) and one or more IP blocks, may be coupled to internal memory to provide processing and display capabilities. A non-volatile memory port may also be used to provide data input/output options to a user. The non-volatile memory port may also be used to expand the memory capabilities of the mobile device. A keyboard may be
10 integrated with the mobile device or wirelessly connected to the mobile device to provide additional user input. A virtual keyboard may also be provided using the touch screen.

[0052] Various techniques, or certain aspects or portions thereof, may take the form of program code (i.e., instructions) embodied in tangible media, such as, for example CD-ROMs, hard drives, Solid-State Drives (SSD), non-transitory computer readable storage medium, or any other
15 machine-readable storage medium wherein, when the program code is loaded into and executed by a machine, such as a computer, the machine becomes an apparatus for practicing the various techniques. In the case of program code execution on programmable computers, the computing device may include a processor circuitry, a storage medium readable by the processor circuitry (including volatile and non-volatile memory and/or storage elements), at least one input device,
20 and at least one output device. The volatile and non-volatile memory and/or storage elements may be a RAM, EPROM, flash drive, optical drive, magnetic hard drive, or other medium for storing electronic data. One or more programs that may implement or utilize the various techniques described herein may use an application programming interface (API), reusable controls, and the like. Such programs may be implemented in a high level procedural or object
25 oriented programming language to communicate with a computer system. However, the program(s) may be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language, and combined with hardware implementations.

[0053] Reference is made to FIG. 4, which schematically illustrates a product of manufacture
30 400, in accordance with some demonstrative embodiments. Product 400 may include a non-transitory machine-readable storage medium 402 to store logic 404, which may be used, for example, to perform at least part of the functionality of one or more elements of system 100 (FIG. 1), one or more elements of SoC 200 (FIG. 1) and/or to perform one or more operations of the method of FIG. 2. The phrase “non-transitory machine-readable medium” is directed to

include all computer-readable media, with the sole exception being a transitory propagating signal.

[0054] In some demonstrative embodiments, product 400 and/or machine-readable storage medium 402 may include one or more types of computer-readable storage media capable of storing data, including volatile memory, non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and the like. For example, machine-readable storage medium 402 may include, RAM, DRAM, Double-Data-Rate DRAM (DDR-DRAM), SDRAM, static RAM (SRAM), ROM, programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), Compact Disk ROM (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewritable (CD-RW), flash memory (e.g., NOR or NAND flash memory), content addressable memory (CAM), polymer memory, phase-change memory, ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, a disk, a floppy disk, a hard drive, an optical disk, a magnetic disk, a card, a magnetic card, an optical card, a tape, a cassette, and the like. The computer-readable storage media may include any suitable media involved with downloading or transferring a computer program from a remote computer to a requesting computer carried by data signals embodied in a carrier wave or other propagation medium through a communication link, e.g., a modem, radio or network connection.

[0055] In some demonstrative embodiments, logic 404 may include instructions, data, and/or code, which, if executed by a machine, may cause the machine to perform a method, process and/or operations as described herein. The machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware, software, firmware, and the like.

EXAMPLES

[0056] The following examples pertain to further embodiments.

[0057] Example 1 includes a method for securing sensor data by a security engine circuitry of a system on chip (SoC), the method comprising receiving from a processor circuitry of the SoC an inter processor communication (IPC) request to receive the sensor data; sending to an integrated sensor hub (ISH) of the SoC an IPC request for receiving the sensor data; receiving the sensor data from the ISH; generating certified encrypted sensor data based on the sensor data; and sending the certified encrypted sensor data to the processor circuitry.

[0058] Example 2 includes the subject matter of Example 1, and optionally, wherein generating

the certified encrypted sensor data comprises adding a certificate to the sensor data to provide certified sensor data; and encrypting the certified sensor data with one or more keys.

[0059] Example 3 includes the subject matter of Example 1 or 2, and optionally, comprising delivering the certified encrypted sensor data to a middleware (MW) framework of the processor circuitry.

[0060] Example 4 includes the subject matter of any one of Examples 1-3, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a device including the SoC.

[0061] Example 5 includes the subject matter of any one of Examples 1-4, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a cloud.

[0062] Example 6 includes the subject matter of any one of Examples 1-5, and optionally, wherein the certified encrypted sensor data is configured to be certified against user credentials and logged to a database.

[0063] Example 7 includes a system on chip (SoC) configured to secure sensor data, the SoC comprising processor circuitry; an integrated sensor hub (ISH) configured to collect and process the sensor data; and a security engine configured to receive the sensor data from the ISH, certify and encrypt the sensor data, and send certified encrypted sensor data to a middleware framework of the processor circuitry, the processor circuitry being configured to provide the certified encrypted sensor data to a service.

[0064] Example 8 includes the subject matter of Example 7, and optionally, wherein the security engine is configured to receive from the processor circuitry an inter processor communication (IPC) request to provide the secure sensor data.

[0065] Example 9 includes the subject matter of Example 7 or 8, and optionally, wherein the security engine is configured to send to the ISH an IPC request to receive the sensor data, to add a certificate to the sensor data, and to send the certified sensor data to the processor circuitry.

[0066] Example 10 includes the subject matter of any one of Examples 7-9, and optionally, wherein the security engine is configured to generate at least one encryption key to encrypt the sensor data and to add a certificate to the sensor data.

[0067] Example 11 includes the subject matter of any one of Examples 7-10, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a device including the SoC.

[0068] Example 12 includes the subject matter of any one of Examples 7-11, and optionally,

wherein the certified encrypted sensor data is configured to be used by a service in a cloud.

[0069] Example 13 includes the subject matter of any one of Examples 7-12, and optionally, wherein the certified encrypted sensor data is configured to be certified against user credentials and to be logged to a database.

- 5 [0070] Example 14 includes a computer program product comprising a non-transitory computer readable storage medium having a computer readable program code embodied therein, the computer readable program code adapted to be executed by a mobile device to implement a method for securing sensor data by security engine circuitry of a system on chip (SoC), the method comprising receiving from a processor circuitry of the SoC an inter processor
10 communication (IPC) request to receive the sensor data; sending to an integrated sensor hub (ISH) of the SoC an IPC request for receiving the sensor data; receiving the sensor data from the ISH; generating certified encrypted sensor data based on the sensor data; and sending the certified encrypted sensor data to the processor circuitry.

- [0071] Example 15 includes the subject matter of Example 14, and optionally, wherein sending
15 the certified requested sensor data comprises adding a certificate to the sensor data to provide certified sensor data; and encrypting the certified sensor data with one or more keys.

[0072] Example 16 includes the subject matter of Example 14 or 15, and optionally, wherein the method comprises delivering the certified encrypted sensor data to a middleware (MW) framework of the processor circuitry.

- 20 [0073] Example 17 includes the subject matter of any one of Examples 14-16, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a device including the SoC.

[0074] Example 18 includes the subject matter of any one of Examples 14-17, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a cloud.

- 25 [0075] Example 19 includes the subject matter of any one of Examples 14-18, and optionally, wherein the certified encrypted sensor data is configured to be certified against a user credentials and logged to a database.

- [0076] Example 20 includes a mobile device configured to secure sensor data, the mobile device comprising a wireless local area radio operably coupled to a system on chip (SoC), wherein the
30 SoC comprises processor circuitry; an integrated sensor hub (ISH) configured to collect and process the sensor data; and a security engine configured to receive the sensor data from the ISH, certify and encrypt the sensor data, and send certified encrypted sensor data to a middleware

framework of the processor circuitry, the processor circuitry being configured to provide the certified encrypted sensor data to a service.

[0077] Example 21 includes the subject matter of Example 20, and optionally, wherein the security engine is configured to receive from the processor circuitry an inter processor communication (IPC) request to provide the secure sensor data.

[0078] Example 22 includes the subject matter of Example 20 or 21, and optionally, wherein the security engine is configured to send to the ISH an IPC request to receive the sensor data, to add a certificate to the sensor data, and to send the certified sensor data to the processor circuitry.

[0079] Example 23 includes the subject matter of any one of Examples 20-22, and optionally, wherein the security engine is configured to generate at least one encryption key to encrypt the sensor data, and to add a certificate to the sensor data.

[0080] Example 24 includes the subject matter of any one of Examples 20-23, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a cloud.

[0081] Example 25 includes the subject matter of any one of Examples 20-24, and optionally, wherein the certified encrypted sensor data is configured to be certified against user credentials and to be logged to a database.

[0082] Example 26 includes a mobile device configured to secure sensor data, the mobile device comprising a system on chip (SoC) operably coupled to one or more sensors, wherein the SoC comprises processor circuitry; an integrated sensor hub (ISH) configured to collect and process the sensor data; and a security engine configured to receive the sensor data from the ISH, certify and encrypt the sensor data, and send certified encrypted sensor data to a middleware framework of the processor circuitry, the processor circuitry being configured to provide the certified encrypted sensor data to a service.

[0083] Example 27 includes the subject matter of Example 26, and optionally, wherein the security engine is configured to receive from the processor circuitry an inter processor communication (IPC) request to provide the secure sensor data.

[0084] Example 28 includes the subject matter of Example 26 or 27, and optionally, wherein the security engine is configured to send to the ISH an IPC request to receive the sensor data, to add a certificate to the sensor data, and to send the certified sensor data to the processor circuitry.

[0085] Example 29 includes the subject matter of any one of Examples 26-28, and optionally, wherein the security engine is configured to generate at least one encryption key to encrypt the sensor data, and to add a certificate to the sensor data.

[0086] Example 30 includes the subject matter of any one of Examples 26-29, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a cloud.

[0087] Example 31 includes the subject matter of any one of Examples 26-30, and optionally, wherein the certified encrypted sensor data is configured to be certified against user credentials

5 and to be logged to a database.

[0088] Example 32 includes the subject matter of any one of Examples 26-31, and optionally, wherein the one or more sensors are external to the mobile device.

[0089] Example 33 includes a system on chip (SoC) configured to secure sensor data, the SoC comprising means to perform the method of any one of Examples 1-6.

10 [0090] Example 34 includes a computer program product comprising a non-transitory computer readable storage medium having a computer readable program code embodied therein, the computer readable program code adapted to be executed by a mobile device to implement the method of any one of Examples 1-6.

[0091] Example 35 includes a mobile device configured to secure sensor data comprising a
15 wireless local area radio operably coupled to a system on chip (SoC), wherein the SoC comprises means to perform the method of any one of Examples 1-6.

[0092] Example 36 includes a system on chip (SoC) configured to secure sensor data, the SoC comprising processor circuitry; an integrated sensor hub (ISH) means configured to collect and process the sensor data; and a security engine means configured to receive the sensor data from
20 the ISH, certify and encrypt the sensor data, and send certified encrypted sensor data to a middleware framework of the processor circuitry, the processor circuitry being configured to provide the certified encrypted sensor data to a service.

[0093] Example 37 includes the subject matter of Example 36, and optionally, wherein the security engine means is configured to receive from the processor circuitry SoC an inter
25 processor communication (IPC) request to provide the secure sensor data.

[0094] Example 38 includes the subject matter of Example 36 or 37, and optionally, wherein the security engine means is configured to send to the ISH means an IPC request to receive the sensor data, to add a certificate to the sensor data, and to send the certified sensor data to the processor circuitry.

30 [0095] Example 39 includes the subject matter of any one of Examples 36-38, and optionally, wherein the security engine means is configured to generate at least one encryption key to encrypt the sensor data, and to add a certificate to the sensor data.

[0096] Example 40 includes the subject matter of any one of Examples 36-39, and optionally, wherein the certified encrypted sensor data is to be delivered to a middleware (MW) framework of the processor circuitry.

5 [0097] Example 41 includes the subject matter of any one of Examples 36-40, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a device including the SoC.

[0098] Example 42 includes the subject matter of any one of Examples 36-41, and optionally, wherein the certified encrypted sensor data is configured to be used by a service in a cloud.

10 [0099] Example 43 includes the subject matter of any one of Examples 36-42, and optionally, wherein the certified encrypted sensor data is configured to be certified against user credentials and to be logged to a database.

[00100] It should be understood that many of the functional units described in this specification have been labeled as modules, in order to more particularly emphasize their implementation independence. For example, a module may be implemented as a hardware circuit comprising
15 custom VLSI circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic, programmable logic devices or the like.

[00101] Modules may also be implemented in software for execution by various types of
20 processors. An identified module of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions, which may, for instance, be organized as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located together, but may comprise disparate instructions stored in different locations which, when joined logically together, comprise the module and achieve the stated purpose for
25 the module.

[00102] Indeed, a module of executable code may be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several memory devices. Similarly, operational data may be identified and illustrated herein within modules, and may be embodied in any suitable form and organized within any
30 suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different storage devices, and may exist, at least partially, merely as electronic signals on a system or network. The modules may be passive or active, including agents operable to perform desired functions.

[00103] As used herein, a plurality of items, structural elements, compositional elements, and/or materials may be presented in a common list for convenience. However, these lists should be construed as though each member of the list is individually identified as a separate and unique member. Thus, no individual member of such list should be construed as a de facto equivalent of any other member of the same list solely based on their presentation in a common group without indications to the contrary. In addition, various embodiments and examples may be referred to herein along with alternatives for the various components thereof. It is understood that such embodiments, examples, and alternatives are not to be construed as de facto equivalents of one another, but are to be considered as separate and autonomous representations.

[00104] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

[00105] In the foregoing description, numerous specific details are provided, such as examples of layouts, distances, network examples, etc., to provide a thorough understanding of some demonstrative embodiments. One skilled in the relevant art will recognize, however, that some embodiments can be practiced without one or more of the specific details, or with other methods, components, layouts, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the disclosure.

[00106] While the foregoing examples are illustrative of the principles of some embodiments in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation can be made without the exercise of inventive faculty, and without departing from the principles and concepts of the disclosure. Accordingly, it is not intended that the disclosure be limited, except as by the claims set forth below.

CLAIMS

What is claimed is:

1. A method for securing sensor data by a security engine circuitry of a system on chip (SoC), the method comprising:
 - 5 receiving from a processor circuitry of the SoC an inter processor communication (IPC) request to receive the sensor data;
sending to an integrated sensor hub (ISH) of the SoC an IPC request for receiving the sensor data;
receiving the sensor data from the ISH;
 - 10 generating certified encrypted sensor data based on the sensor data; and
sending the certified encrypted sensor data to the processor circuitry.
2. The method of claim 1, wherein generating the certified encrypted sensor data comprises:
 - adding a certificate to the sensor data to provide certified sensor data; and
encrypting the certified sensor data with one or more keys.
- 15 3. The method of claim 1 comprising delivering the certified encrypted sensor data to a middleware (MW) framework of the processor circuitry.
4. The method of any one of claims 1-3, wherein the certified encrypted sensor data is configured to be used by a service in a device including said SoC.
5. The method of any one of claims 1-3, wherein the certified encrypted sensor data is
20 configured to be used by a service in a cloud.
6. The method of any one of claims 1-3, wherein the certified encrypted sensor data is configured to be certified against user credentials and logged to a database.
7. A system on chip (SoC) configured to secure sensor data, the SoC comprising:
 - processor circuitry;
 - 25 an integrated sensor hub (ISH) configured to collect and process the sensor data; and
a security engine configured to receive the sensor data from the ISH, to certify and encrypt the sensor data, and to send certified encrypted sensor data to a middleware framework of the processor circuitry, the processor circuitry being configured to provide the certified encrypted sensor data to a service.

8. The SoC of claim 7, wherein the security engine is configured to receive from the processor circuitry an inter processor communication (IPC) request to provide the secure sensor data.
9. The SoC of claim 7, wherein the security engine is configured to send to the ISH an IPC request to receive the sensor data, to add a certificate to the sensor data, and to send the certified sensor data to the processor circuitry.
10. The SoC of claim 7, wherein the security engine is configured to generate at least one encryption key to encrypt the sensor data, and to add a certificate to the sensor data.
11. The SoC of any one of claims 7-10, wherein the certified encrypted sensor data is configured to be used by a service in a device including said SoC.
12. The SoC of any one of claims 7-10, wherein the certified encrypted sensor data is configured to be used by a service in a cloud.
13. The SoC of any one of claims 7-10, wherein the certified encrypted sensor data is configured to be certified against user credentials and to be logged to a database.
14. A computer program product comprising a non-transitory computer readable storage medium having a computer readable program code embodied therein, the computer readable program code adapted to be executed by a mobile device to implement a method for securing sensor data by a security engine circuitry of a system on chip (SoC), the method comprising:
 - receiving from a processor circuitry of the SoC an inter processor communication (IPC) request to receive the sensor data;
 - sending to an integrated sensor hub (ISH) of the SoC an IPC request for receiving the sensor data;
 - receiving the sensor data from the ISH;
 - generating certified encrypted sensor data based on the sensor data; and
 - sending the certified encrypted sensor data to the processor circuitry.
15. The computer program product of claim 14, wherein sending the certified requested sensor data comprises:
 - adding a certificate to the sensor data to provide certified sensor data; and

encrypting the certified sensor data with one or more keys.

16. The computer program product of claim 14, wherein the method comprises:

delivering the certified encrypted sensor data to a middleware (MW) framework of the processor circuitry.

5 17. The computer program product of any one of claims 14-16, wherein the certified encrypted sensor data is configured to be used by a service in a device including said SoC.

18. The computer program product of any one of claims 14-16, wherein the certified encrypted sensor data is configured to be used by a service in a cloud.

10 19. The computer program product of any one of claims 14-16, wherein the certified encrypted sensor data is configured to be certified against a user credentials and logged to a database.

20. A mobile device configured to secure sensor data, the mobile device comprising:

a wireless local area radio operably coupled to a system on chip (SoC), wherein the SoC comprises:

15 processor circuitry;

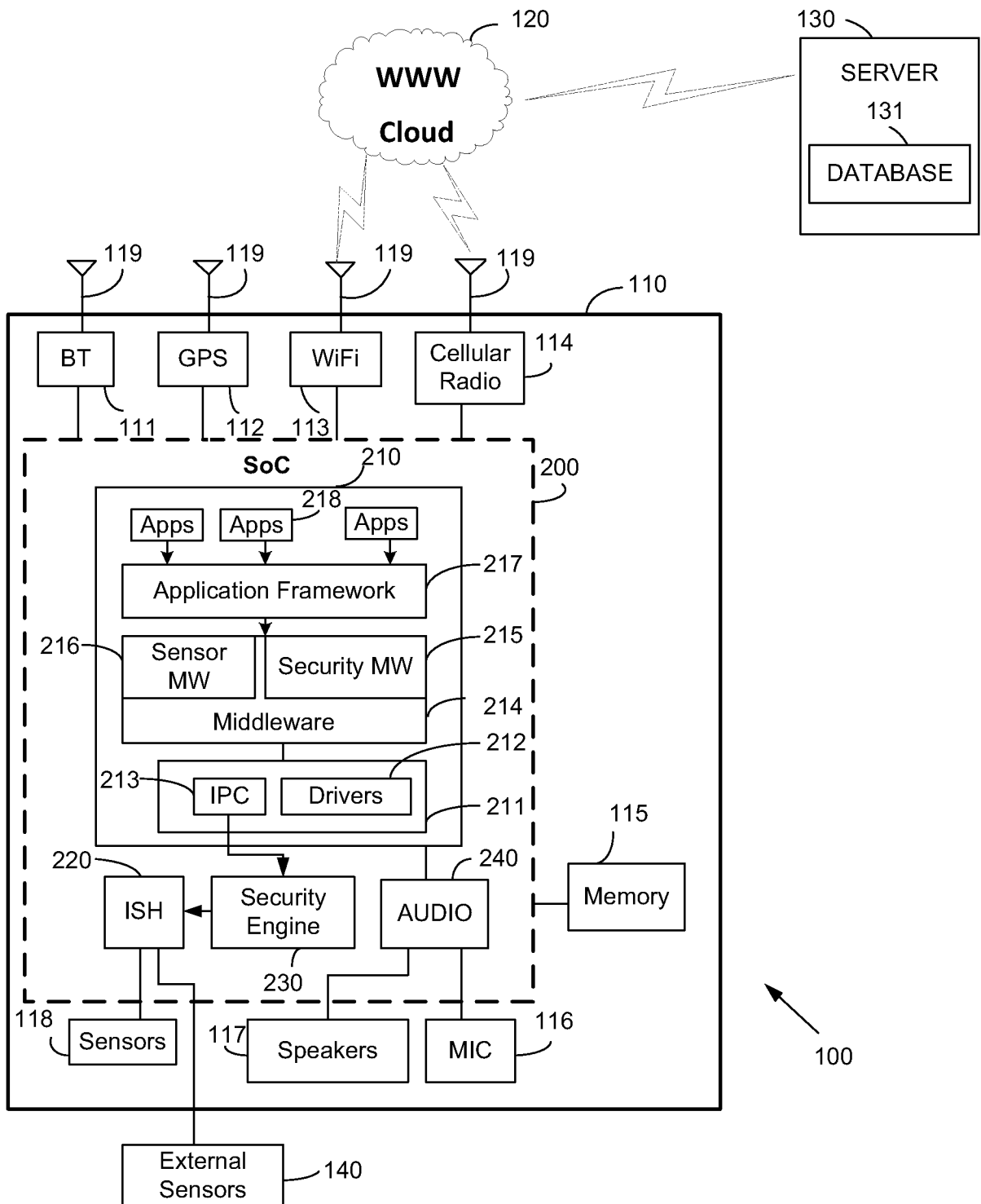
an integrated sensor hub (ISH) configured to collect and process the sensor data; and

a security engine configured to receive the sensor data from the ISH, to certify and encrypt the sensor data, and to send certified encrypted sensor data to a middleware framework of the processor circuitry, the processor circuitry being configured to provide
20 the certified encrypted sensor data to a service.

21. The mobile device of claim 20, wherein the security engine is configured to receive from the processor circuitry an inter processor communication (IPC) request to provide the sensor data.

22. The mobile device of claim 20, wherein the security engine is configured to send to the
25 ISH an IPC request to receive the sensor data, to add a certificate to the sensor data, and to send the certified encrypted sensor data to the processor circuitry.

23. The mobile device of any one of claims 20-22, wherein the security engine is configured to generate at least one encryption key to encrypt the sensor data and to add a certificate to the sensor data.

**FIG. 1**

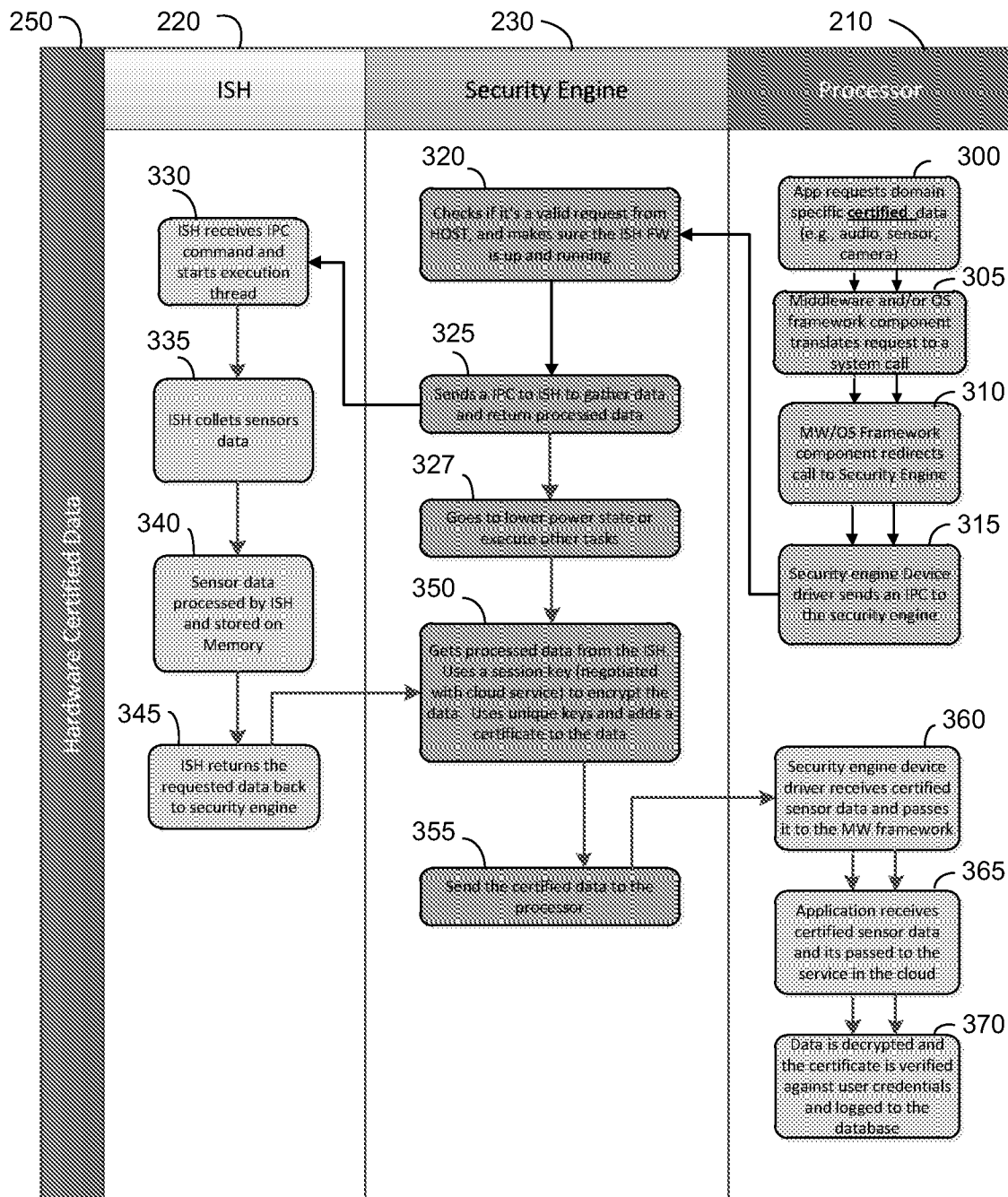
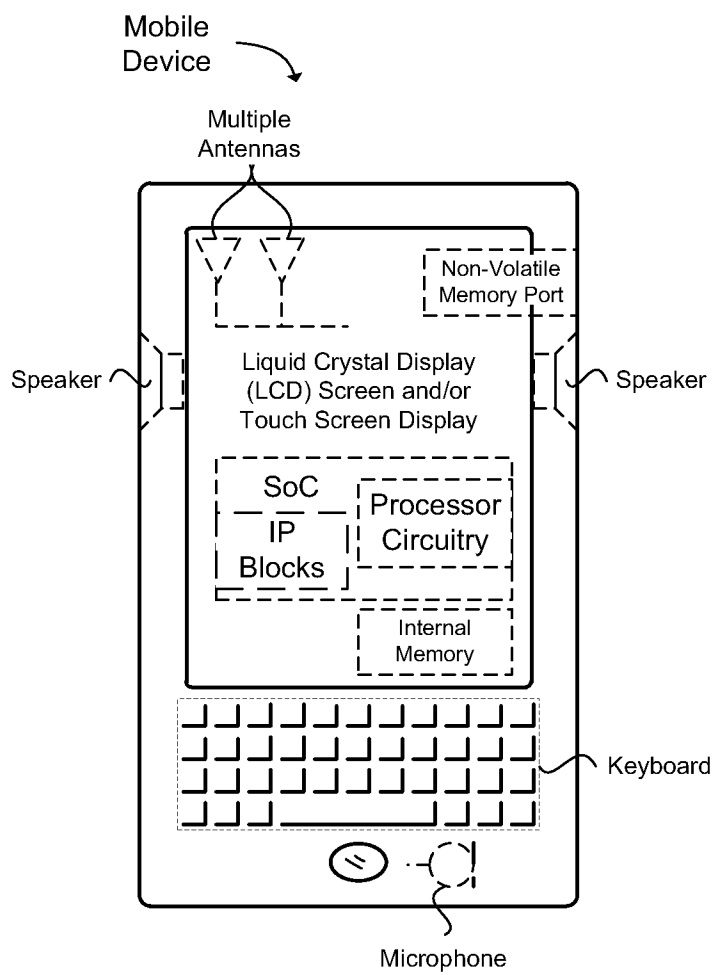
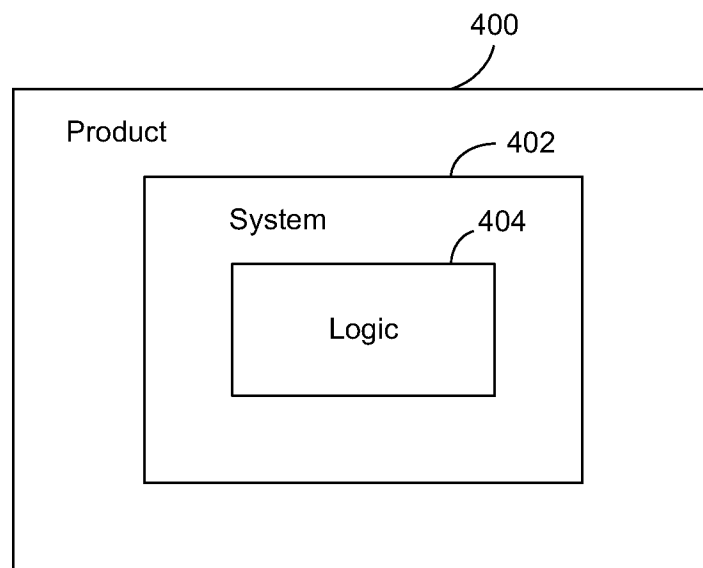


FIG. 2

**FIG. 3**

***FIG. 4***

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/037614**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/08(2006.01)i**

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)

H04L 9/08; G06F 3/00; H04L 29/06; H04L 9/00; G06F 21/60

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & keywords: system on chip, inter processor communication, integrated sensor hub, encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009-0164797 A1 (ALAN KRAMER) 25 June 2009 See paragraphs [0015]-[0054]; and figures 1-5.	1-23
Y	WO 2014-089749 A1 (INTEL CORPORATION) 19 June 2014 See paragraphs [0017]-[0048]; and figures 1-3.	1-23
A	US 2014-0068779 A1 (BOX, INC.) 06 March 2014 See paragraphs [0053]-[0096]; and figures 5-8.	1-23
A	US 2014-0205099 A1 (QUALCOMM INCORPORATED) 24 July 2014 See paragraphs [0063]-[0116]; and figures 2A-3C.	1-23
A	US 2014-0150100 A1 (QUALCOMM INCORPORATED) 29 May 2014 See paragraphs [0071]-[0115]; and figure 2.	1-23



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

07 October 2015 (07.10.2015)

Date of mailing of the international search report

07 October 2015 (07.10.2015)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 35208,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

KIM, Do Weon

Telephone No. +82-42-481-5560



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/037614

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009-0164797 A1	25/06/2009	EP 2075730 A1 JP 2009-151788 A	01/07/2009 09/07/2009
WO 2014-089749 A1	19/06/2014	CN 104011627 A DE 112012005643 T5 GB 201410976 D0 JP 2015-506047 A KR 10-2014-0102715 A KR 10-2015-0084849 A	27/08/2014 09/10/2014 06/08/2014 26/02/2015 22/08/2014 22/07/2015
US 2014-0068779 A1	06/03/2014	None	
US 2014-0205099 A1	24/07/2014	None	
US 2014-0150100 A1	29/05/2014	TW 201441811 A US 2014-0053260 A1 WO 2014-116977 A2 WO 2014-116977 A3	01/11/2014 20/02/2014 31/07/2014 31/07/2014