(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2014 (03.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/004590 A2

(51) International Patent Classification:
H04L 9/00 (2006.01) *A61B 5/021* (2006.01)
G06F 21/00 (2013.01) *A61B 5/01* (2006.01)
G06Q 50/24 (2012.01) *A61B 5/1455* (2006.01)
G06Q 50/22 (2012.01) *A61B 5/02* (2006.01)
A61B 5/145 (2006.01) *A61B 5/024* (2006.01)

(21) International Application Number:
PCT/US2013/047729

(22) International Filing Date:
25 June 2013 (25.06.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/532,588 25 June 2012 (25.06.2012) US

(71) Applicant: **SPRINT COMMUNICATIONS COMPANY L.P.** [US/US]; 6450 Sprint Parkway, MailStop KSOPH-N0312-3A371, Overland Park, Kansas 66251-2100 (US).

(72) Inventors: **MCROBERTS, Leo Michael**; 12505 King Street, Overland Park, Kansas 66213 (US). **PACZKOWSKI, Lyle W.**; 2402 West 70th Terrace, Mission Hills, Kansas 66208 (US). **RONDEAU, David E.**; 15725 W. Locust Street, Olathe, Kansas 66062 (US).

(74) Agents: **CONLEY ROSE, P.C.** et al.; 5601 Granite Parkway, Ste. 500, Plano, Texas 75024 (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, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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,

[Continued on next page]

(54) Title: END-TO-END TRUSTED COMMUNICATIONS INFRASTRUCTURE

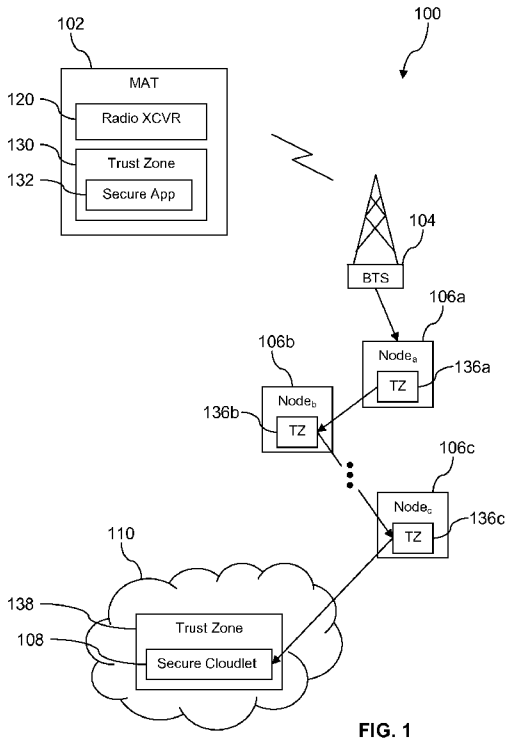

FIG. 1

(57) Abstract: A method of delivery of medical data via a trusted end-to-end communication link. The method comprises obtaining a measurement of a parameter of a human being by a first sensor, obtaining a biometric from the human being by a second sensor, receiving input from the first and second sensors by a secure application executing in a trusted security zone of a processor, whereby access to the input from the first and second sensors by applications executing in a normal partition of the processor is blocked, wherein the input from the first and second sensors comprises the measurement of the parameter and the biometric, and transmitting a message based on the input from the first and second sensors via a trusted end-to-end communication link to a medical data server, wherein an application that receives the message executes in a trusted security zone of the server.

WO 2014/004590 A2

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:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

End-to-end Trusted Communications Infrastructure

BACKGROUND

[0001] Electronic communications may carry a wide variety of content, for example electronic mail, medical records, financial transactions, and other confidential information. The electronic communications may travel for some of the communication end-to-end path over unsecured communication links where the content may be subject to tampering or intrusion. A variety of security measures have been applied to provide increased security and to raise the level of difficulty for nefarious actors attempting to access the confidential information.

SUMMARY

[0002] In an embodiment, a method of delivery of medical data via a trusted end-to-end communication link is disclosed. The method comprises obtaining a measurement of a parameter of a human being by a first sensor, obtaining a biometric from the human being by a second sensor, receiving input from the first and second sensors by a secure application executing in a trusted security zone of a processor, whereby access to the input from the first and second sensors by applications executing in a normal partition of the processor is blocked, wherein the input from the first and second sensors comprises the measurement of the parameter and the biometric, and transmitting a message based on the input from the first and second sensors via a trusted end-to-end communication link to a medical data server, wherein an application that receives the message executes in a trusted security zone of the server.

[0003] In an embodiment, a method establishing a trusted end-to-end communication link is disclosed. The method comprises executing a communication application in a trusted security zone of a mobile access terminal, sending a message from the mobile access terminal to a trusted communication application executing in a trusted security zone of a trusted enterprise edge node, and sending the message from the trusted enterprise edge node to a trusted cloudlet executing on in a trusted security zone of a cloud based server.

[0004] In an embodiment, a method of accessing medical diagnostic information is disclosed. The method comprises obtaining a measurement of a parameter of a human being from a first sensor and a biometric from the human being from a second sensor, transmitting the measurement of the parameter and the biometric from the first and second sensors, and receiving the measurement of the parameter and the biometric from the first and second sensors by a processor executing in a trusted security zone of

a mobile access terminal, whereby access to the measurement of the parameter and the biometric from the first and second sensors by applications executing in a normal execution mode is blocked. The method further comprises transmitting a first message based on the measurement of the parameter and the biometric by the mobile access terminal via a trusted end-to-end communication link to a medical data server, wherein the trusted end-to-end communication link comprises a wireless communication link, and receiving the first message by an application that executes in a trusted security zone of the medical data server. The method further comprises transmitting a second message based on the measurement of the parameter and the biometric by the medical data server via a trusted end-to-end communication link to a computer associated with a medical doctor and determining a medical care instruction for the human being based on the second message.

[0005] These and other features will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] For a more complete understanding of the present disclosure, reference is now made to the following brief description, taken in connection with the accompanying drawings and detailed description, wherein like reference numerals represent like parts.

[0007] FIG. 1 is an illustration of a communication system according to an embodiment of the disclosure.

[0008] FIG. 2 is an illustration of a message flowing through a trusted end-to-end communication link according to an embodiment of the disclosure.

[0009] FIG. 3A is an illustration of a human body monitor according to an embodiment of the disclosure.

[0010] FIG. 3B is an illustration of a system for delivery of medical information according to an embodiment of the disclosure.

[0011] FIG. 4 is a flow chart of a method according to an embodiment of the disclosure.

[0012] FIG. 5 is a flow chart of another method according to an embodiment of the disclosure.

[0013] FIG. 6 is a flow chart of another method according to an embodiment of the disclosure.

[0014] FIG. 7 is an illustration of a mobile access terminal according to an embodiment of the disclosure.

[0015] FIG. 8 is a block diagram of a mobile access terminal according to an embodiment of the disclosure.

[0016] FIG. 9A is an illustration of a software architecture according to an embodiment of the disclosure.

[0017] FIG. 9B is an illustration of another software architecture according to an embodiment of the disclosure.

[0018] FIG. 10 is a block diagram of a computer system according to an embodiment of the disclosure.

DETAILED DESCRIPTION

[0019] It should be understood at the outset that although illustrative implementations of one or more embodiments are illustrated below, the disclosed systems and methods may be implemented using any number of techniques, whether currently known or not yet in existence. The disclosure should in no way be limited to the illustrative implementations, drawings, and techniques illustrated below, but may be modified within the scope of the appended claims along with their full scope of equivalents.

[0020] In an embodiment, a system and methods of providing a trusted end-to-end communication link are described. Trusted communication can be established between two devices each of which are executing their communication processing in a trusted security zone. As described further below, trusted security zones reduce the ability of nefarious applications that may have infiltrated an electronic processing device to read from or write to memory, to read from or write to input/output devices, or to read from or write to communication ports while the subject processor and/or electronic processing device is executing in the trusted security zone. A communication application executing in a trusted security zone can have a high level of confidence that an untrusted application is not executing on the electronic processing device, for example a mobile telephone, at the same time and hence is prevented from interfering with or monitoring the activities of the communication application.

[0021] A trusted end-to-end communication link may be established by assuring that all communication applications in the end-to-end communication link that execute at the network layer and/or higher layers execute in trusted security zones of the subject electronic processing devices, for example a mobile phone, a base transceiver station, a media access gateway, Internet routers, switches, server computers, and the like. Prior to a first node transmitting a message over a trusted end-to-end communication

link to a second node, the first node may handshake with or otherwise communicate with the second node to pre-arrange for the second node to handle the forthcoming message from the first node in the trusted security zone of the second node. This handshaking may comprise the first node validating the trusted status of the second node. Said in other words, the handshaking may promote the first node evaluating whether the second node is configured to support the trusted end-to-end communication link.

[0022] As an electronic message is passed from one network node to the next, each successive node in the trusted end-to-end communication link may validate the continuity of trust by examining and validating trust tokens that are accumulated by the message as it transits the trusted end-to-end communication link. The trust tokens are built and provided by the previous node and/or previous nodes in the trusted end-to-end communication link. The trust tokens comprise indications or information about how the subject message was handled, e.g., processed in a trusted security zone, and may be viewed as a kind of birth certificate or pedigree of the message. Some or all of the trust token may be encrypted to avoid monitoring or tampering by untrusted nodes. Trust tokens may be created by a secure application, such as the communication application that is executing in the trusted security zone to conduct communication over the trusted end-to-end communication link, or by a base layer of functionality and/or utilities provided by the trusted security zone itself.

[0023] For example, a secure application executing in the trusted security zone of a mobile phone may send a message to a first trusted network node. The message may comprise content and a first trust token that encrypts information about the mobile phone that establishes that the message was generated by the trusted security zone of the mobile phone. The message may be verified to be trusted by the first trusted network node by examining the first trust token. The first trusted network node may then build a second trust token, extend the message by the addition of the second trust token, and transmit the extended message to a second trusted network node. The message may be verified to be trusted by the second trusted network node by examining the second trust token alone or by examining both the first and the second trust tokens. Through the remainder of the trusted end-to-end communication link, every network node that handles the message at the network layer or higher layer handles the message in a trusted security zone of that node, verifies the continuity of trust by examining one or more trust tokens, builds an additional trust token, extends

the message with the additional trust token, and sends the message on to the next trusted network node. At the endpoint of the trusted end-to-end communication link, the message may be consumed by a secure application executing in a trusted security zone of the endpoint device after the continuity of trust of the message is verified. In an alternative embodiment, rather than the message being accompanied by a plurality of trust tokens, the message may be accompanied by a single trust token that may be extended and/or appended to by each successive trusted network node.

[0024] In an embodiment, the trusted end-to-end communication link may extend from a mobile access terminal to a base transceiver station (BTS) to an enterprise network via a virtual private network (VPN) connection. The continuity of trust of the connection between the mobile access terminal and the base transceiver station may not be explicitly verified because the air interface of the base transceiver station may be considered to be invulnerable to a hacking attack. The continuity of trust of the virtual private network connection into the enterprise network may not be explicitly verified because it likewise may be considered to be invulnerable to a hacking attack. If the trusted end-to-end communication link then extends out of the enterprise network through a firewall or through a multi-protocol label switching (MPLS) port into the Internet and on to an endpoint device, such as a secure cloudlet executing on a trusted security zone of a server computer operated in a cloud computing service, trust may be provided as described above, with the subject message being handled at the network layer or above layers only by applications executing in trusted security zones on the subject network nodes, each trusted security zone verifying the continuity of trust of the received message and adding an additional trust token or extending the trust token when transmitting the message on to the next node. At the server computer in the cloud, the secure cloudlet executes in a trusted security zone of the server computer and verifies the continuity of trust of the received message and/or the trusted end-to-end communication link.

[0025] In an embodiment, a monitor device may comprise a sensor and a biometric scanner or sensor. The sensor may measure or sample a bodily parameter of a human being such as a blood sugar level, a blood thickness, a blood pressure, a bodily temperature, a pulse rate, a heart rhythm, or another parameter. At the same time that the bodily parameter is being sampled, the biometric scanner may capture a biometric signature of the human being whose bodily parameter is being measured. In an embodiment, the monitor device is configured such that taking the sample of the bodily

parameter of the human being is inseparably linked to capturing the biometric signature of the same human being. The biometric signature may be used to establish and/or to corroborate the identity of the human being. The biometric signature may be a finger print, a retinal scan, a face scan, a DNA signature, or other. A secure application executing in a trusted security zone of a mobile access terminal or a computer reads the bodily parameter sample and the biometric signature from the monitor device.

[0026] The secure application may then package the bodily parameter sample and the biometric signature into a medical record content, build a trusted token, and send a message comprising the medical record content and the trusted token through a trusted end-to-end communication link to a corresponding trusted application executing in a trusted security zone of a medical data server. Alternatively, the trusted token may be built by a base layer of functionality and/or utilities provided by the trusted security zone itself. Sending the message over the trusted end-to-end communication link may assure that the medical record content is maintained in confidence, for example in compliance with FDA and/or HIPAA privacy regulations. In an embodiment, medical records maintained by the medical data server may be accessed over a trusted end-to-end communication link to analyze the medical records for a variety of purposes, for example to conduct treatment efficacy studies and/or to diagnose and determine a treatment regime for a patient, while assuring compliance with FDA and/or HIPAA privacy regulations.

[0027] A trusted security zone provides chipsets with a hardware root of trust, a secure execution environment for applications, and secure access to peripherals. A hardware root of trust means the chipset should only execute programs intended by the device manufacturer or vendor and resists software and physical attacks, and therefore remains trusted to provide the intended level of security. The chipset architecture is designed to promote a programmable environment that allows the confidentiality and integrity of assets to be protected from specific attacks. Trusted security zone capabilities are becoming features in both wireless and fixed hardware architecture designs. Providing the trusted security zone in the main mobile device chipset and protecting the hardware root of trust removes the need for separate secure hardware to authenticate the device or user. To ensure the integrity of the applications requiring trusted data, such as a mobile financial services application, the trusted security zone also provides the secure execution environment where only trusted applications can operate, safe from attacks. Security is further promoted by

restricting access of non-trusted applications to peripherals, such as data inputs and data outputs, while a trusted application is running in the secure execution environment. In an embodiment, the trusted security zone may be conceptualized as hardware assisted security.

[0028] A complete Trusted Execution Environment (TEE) may be implemented through the use of the trusted security zone hardware and software architecture. The Trusted Execution Environment is an execution environment that is parallel to the execution environment of the main mobile device operating system. The Trusted Execution Environment and/or the trusted security zone may provide a base layer of functionality and/or utilities for use of applications that may execute in the trusted security zone. For example, in an embodiment, trust tokens may be generated by the base layer of functionality and/or utilities of the Trusted Execution Environment and/or trusted security zone for use in trusted end-to-end communication links to document a continuity of trust of the communications. Through standardization of application programming interfaces (APIs), the Trusted Execution Environment becomes a place to which scalable deployment of secure services can be targeted. A device which has a chipset that has a Trusted Execution Environment on it may exist in a trusted services environment, where devices in the trusted services environment are trusted and protected against attacks. The Trusted Execution Environment can be implemented on mobile phones and tablets as well as extending to other trusted devices such as personal computers, servers, sensors, medical devices, point-of-sale terminals, industrial automation, handheld terminals, automotive, etc.

[0029] The trusted security zone is implemented by partitioning all of the hardware and software resources of the mobile device into two partitions: a secure partition and a normal partition. The secure partition may be implemented by a first physical processor, and the normal partition may be implemented by a second physical processor. Alternatively, the secure partition may be implemented by a first virtual processor, and the normal partition may be implemented by a second virtual processor. Placing sensitive resources in the secure partition can protect against possible attacks on those resources. For example, resources such as trusted software applications may run in the secure partition and have access to hardware peripherals such as a touchscreen or a secure location in memory. Less secure peripherals such as wireless radios may be disabled completely while the secure partition is being accessed, while other peripherals may only be accessed from the

secure partition. While the secure partition is being accessed through the Trusted Execution Environment, the main mobile operating system in the normal partition is suspended, and applications in the normal partition are prevented from accessing the secure peripherals and data. This prevents corrupted applications or malware applications from breaking the trust of the device.

[0030] The trusted security zone is implemented by partitioning the hardware and software resources to exist in a secure subsystem which is not accessible to components outside the secure subsystem. The trusted security zone is built into the processor architecture at the time of manufacture through hardware logic present in the trusted security zone which enables a perimeter boundary between the secure partition and the normal partition. The trusted security zone may only be manipulated by those with the proper credential and, in an embodiment, may not be added to the chip after it is manufactured. Software architecture to support the secure partition may be provided through a dedicated secure kernel running trusted applications. Trusted applications are independent secure applications which can be accessed by normal applications through an application programming interface in the Trusted Execution Environment on a chipset that utilizes the trusted security zone.

[0031] In an embodiment, the normal partition applications run on a first virtual processor, and the secure partition applications run on a second virtual processor. Both virtual processors may run on a single physical processor, executing in a time-sliced fashion, removing the need for a dedicated physical security processor. Time-sliced execution comprises switching contexts between the two virtual processors to share processor resources based on tightly controlled mechanisms such as secure software instructions or hardware exceptions. The context of the currently running virtual processor is saved, the context of the virtual processor being switched to is restored, and processing is restarted in the restored virtual processor. Time-sliced execution protects the trusted security zone by stopping the execution of the normal partition while the secure partition is executing.

[0032] The two virtual processors context switch via a processor mode called monitor mode when changing the currently running virtual processor. The mechanisms by which the processor can enter monitor mode from the normal partition are tightly controlled. The entry to monitor mode can be triggered by software executing a dedicated instruction, the Secure Monitor Call (SMC) instruction, or by a subset of the hardware exception mechanisms such as hardware interrupts, which can be configured

to cause the processor to switch into monitor mode. The software that executes within monitor mode then saves the context of the running virtual processor and switches to the secure virtual processor.

[0033] The trusted security zone runs a separate operating system that is not accessible to the device users. For security purposes, the trusted security zone is not open to users for installing applications, which means users do not have access to install applications in the trusted security zone. This prevents corrupted applications or malware applications from executing powerful instructions reserved to the trusted security zone and thus preserves the trust of the device. The security of the system is achieved at least in part by partitioning the hardware and software resources of the mobile phone so they exist in one of two partitions, the secure partition for the security subsystem and the normal partition for everything else. Placing the trusted security zone in the secure partition and restricting access from the normal partition protects against software and basic hardware attacks. Hardware logic ensures that no secure partition resources can be accessed by the normal partition components or applications. A dedicated secure partition operating system runs in a virtual processor separate from the normal partition operating system that likewise executes in its own virtual processor. Users may install applications on the mobile device which may execute in the normal partition operating system described above. The trusted security zone runs a separate operating system for the secure partition that is installed by the mobile device manufacturer or vendor, and users are not able to install new applications in or alter the contents of the trusted security zone.

[0034] Turning now to FIG. 1, a first system 100 for providing trusted end-to-end communication links is described. In an embodiment, the system 100 comprises a mobile access terminal (MAT) 102, a base transceiver station (BTS) 104, a plurality of network nodes 106, and a secure cloudlet 108 executing in a trusted security zone 138 of a server computer located in a cloud computing facility 110. The MAT 102 may be any of a mobile phone, a personal digital assistant (PDA), a media player, a laptop computer, a tablet computer, a notepad computer, or other portable communication device. The network nodes 106 may comprise a first network node 106a, a second network node 106b, and a third network node 106c. It is understood that the system 100 may comprise any number of network nodes 106. The network nodes 106 may be any of network routers, network switches, media access gateways (MAGs), and other data communication networking equipment. The network nodes 106 may be abstracted

as a network cloud or as a communication infrastructure. While the description below refers to the MAT 102, it is understood that at least some of the teachings may be implemented by a desktop computer or other substantially stationary computer that is coupled to the network nodes 106 by a wired connection instead of by a wireless connection.

[0035] The base transceiver station 104 may provide a wireless communication link to the MAT 102, providing edge access from the MAT 102 to the network nodes 106, for example to the first network node 106a. The base transceiver station 104 may provide a wireless communication link according to one or more of a code division multiple access (CDMA), a global system for mobile communications (GSM), a long evolution (LTE), a worldwide interoperability for microwave access (WiMAX), or other wireless communication protocol.

[0036] In an embodiment, the MAT 102 comprises a radio transceiver 120, a trusted security zone 130, and a secure application 132. For example, the radio transceiver 120 may comprise a cellular communication transceiver that is operable to provide a wireless communication link according to one or more of a code division multiple access (CDMA), a global system for mobile communications (GSM), a long term evolution (LTE), a worldwide interoperability for microwave access (WiMAX), or other wireless communication protocol. The MAT 102 may comprise other radio transceivers in addition to the radio transceiver 120, for example a near field communication (NFC) radio transceiver, a Bluetooth® radio transceiver, a WiFi radio transceiver, or other short range radio transceiver.

[0037] As described above, the trusted security zone 130 may be provided by a physically separate processor or by a virtual processor. The secure application 132 may be any of a variety of applications that process and/or transmit confidential information. The confidential information may comprise sensitive business documents such as electronic mail, marketing literature, business plans, client lists, addresses, employee data, intellectual property documents, and the like. The confidential information may comprise personal medical records or medical data that are subject to privacy requirements enforced by government regulatory bodies or commercial standards. The confidential information may comprise financial information such as account numbers, authentication identities, account balance information, and the like.

[0038] When processing and/or transmitting the confidential information, the secure application 132 executes at least partially in the trusted security zone 130. It is a

characteristic or feature of the trusted security zone 130, as described more fully above, that when the secure application 132 executes in the trusted security zone 130, untrusted applications are prevented from executing and/or accessing trusted memory partitions and/or accessing the display or input devices of the MAT 102, thereby reducing the opportunity for malware that may have infiltrated the MAT 102 to corrupt or to monitor the confidential information. When the confidential information is transmitted by the secure application 132 via a trusted end-to-end communication link to the secure cloudlet 108, the trusted security zone 130 builds a message that comprises the confidential information, which may be referred to as a content portion or a content of the message, and a first trust token. In some contexts, the message may be said to incorporate or to encapsulate the content portion and the first trust token. The first trust token comprises information that may be used by another trusted security zone to verify a trust level of the message. The first trust token may comprise indications or information about how the message was handled, e.g., processed in the trusted security zone 130, and may be viewed as a kind of birth certificate or pedigree of the message. Some or all of the trust token may be encrypted to avoid monitoring or tampering by untrusted nodes. In some contexts, the verification of the trust level of the message by analyzing the trust token or a plurality of trust tokens incorporated in, encapsulated in, or adjoined to a message may be referred to as verifying a continuity of trust of the message and/or verifying a continuity of trust of at least a portion of the trusted end-to-end communication link.

[0039] Each of the network nodes 106 comprises a trusted security zone 136. In some contexts, the network nodes 106 may be referred to as trusted network nodes or trusted nodes. The first network node 106a comprises a first trusted security zone 136a, the second network node 106b comprises a second trusted security zone 136b, and the third network node 106c comprises a third trusted security zone 136c. In an embodiment, the network nodes 106 may be dedicated solely to providing trusted end-to-end communication links and may carry no untrusted message traffic. Alternatively, the network nodes 106 may carry both trusted and untrusted message traffic, suspending handling of all untrusted message traffic when handling a trusted message. In an embodiment, communication devices that do not process the message at the network layer of the open system interconnect (OSI) model or above are assumed to be trusted and are not burdened with verifying the continuity of trust of the message before forwarding the message on along the trusted end-to-end communication link.

[0040] The Internet protocol is an example of a network layer process, and the transfer control protocol (TCP) is an example of a process that processes messages at a layer above the network layer. Data communication hubs and the base transceiver station 104 are examples of communication devices or nodes that do not process messages at the network layer or above. In another embodiment, however, lower layer communication devices perform some verification of the continuity of trust of the message.

[0041] In an embodiment, the processing of a message at one network node 106 at each of a plurality of communication layers at or above the network layer is performed by one or more applications executing at least in part in the trusted security zone 136 of the subject network node 106. For example, if the first network node 106a processes the message at both the IP layer and at the UDP layer, the processing at the IP layer is conducted by an application executing at least in part in the trusted security zone 136a, and the processing of the message at the UDP layer is conducted by an application executing at least in part in the trusted security zone 136a. In an embodiment, a trusted token may be generated and associated with the message by an application processing the message at a first communication layer, and a second trusted token may be generated and associated with the message by an application processing the message at a second communication layer. For example, a first application processing the message at the IP communication layer and executing at least in part in the trusted security zone 136a may generate a first trust token and associate it with the message, and a second application processing the message at the UDP communication layer and executing at least in part in the trusted security zone 136a may generate a second trust token and associate it with the message. In an embodiment, the first and second trust tokens may be generated by a base layer of functionality and/or utilities of the trusted security zone 136a that is invoked by the first and second applications.

[0042] When the message is received by the network node 106, the message is identified as a message to be processed by the trusted security zone 136, for example the message may be identified as a trusted message by a field of the message or by the presence of a trust token in the message. The message is analyzed by the trusted security zone 136 to determine the trust level of the message, for example by examining one or more trust tokens that may be encapsulated in the message or associated with the message. If the trust level of the message is sufficient, the network node 106 processes the message, builds a new trust token, encapsulates the new trust

token into the message, and sends the message on to the next network node 106 for handling. The message processing, trust token creation, and message transmitting are performed in the trusted security zone 136 of the network node 106. The new trust token comprises information that may be used by another trusted security zone to verify the trust level of the message, for example to verity that the subject network node processed the message in such a manner as to maintain trust continuity of the message.

[0043] When the message has transited the trusted end-to-end communication link and is received by the trusted security zone 138 of the server located in the cloud computing facility 110, the trust level of the message is analyzed to determine that the continuity of trust of the message has been maintained and that the trust level of the message is sufficient. In an embodiment, the trust level may be a figure of merit that varies over a range of numerical values, for example from 0 to 1, from 0 to 10, from 1 to 10, from 0 to 100, from 1 to 100 or over some other numerical range. The numerical values may be integer values or decimal values. Alternatively, the trust level may be a binary value, either trusted or untrusted. In another embodiment, some other scale of trust level may be implemented. If the trust level of the message is sufficient, the message is provided to the secure cloudlet 108 executing in the trusted security zone 138, and the secure cloudlet 108 consumes the message. For example, the secure cloudlet 108 may process the message in any of a variety of ways including storing the content of the message in a data store, analyzing the content, aggregating the content with other previously received content, and/or other processing.

[0044] The communication infrastructure and processing method described above can be said to provide a trusted end-to-end communication link, because processing of the message at the network layer and above is performed by applications executing at least in part in a trusted security zone that first verifies the continuity of trust of the message before processing it. This infrastructure and processing method promotes a communication end point, for example the secure cloudlet 108, being able to have a high level of confidence that the content of the message has not been intercepted and copied and/or tampered with.

[0045] Turning now to FIG. 2, an example of message propagation through the trusted end-to-end communication link is described. The MAT 102 builds a first message 150 comprising a content 152 and a first trust token 154a. For example, the trusted security zone 130 and/or the secure application 132 executing in the trusted

security zone 130 creates the content 152, builds the first trust token 154a, and composes the first message 150 from the content 152 and the first trust token 154a. As described above, trust tokens may comprise information that may be used by another trusted security zone to verify the trust level of the message. Trust tokens may be analogized to a birth certificate and/or a pedigree. The trust token may comprise encrypted data and/or identity codes that can be decrypted by a trusted security zone to assure that the sending network element has maintained the continuity of trust of the message. The identity codes may identify a network node 136 or other communication device in the path of the trusted end-to-end communication link. The MAT 102 and/or the trusted security zone 130 transmits the first message 150 to the first node 106a.

[0046] The first node 106a processes the first message 150 in the first trusted security zone 136a by analyzing the first message 150 to verify the continuity of trust of the first message 150. For example, the first trusted security zone 136a, or a secure communication application executing in the first trusted security zone 136a, reads and validates the first trust token 154a, which may be referred to as verifying the continuity of trust of the first message 150. In an embodiment, the first trusted security zone 136a may determine a trust level of the first message 150. If the first message 150 has an acceptable trust level, the first trusted security zone 136a builds a second trust token 154b and composes a second message 156 from the content 152, the first trust token 154a, and the second trust token 154b. Alternatively, the second message 156 may not comprise the first trust token 154a, and the second trust token 154b may comprise information about the level of trust determined by the first trusted security zone 136a when verifying the continuity of trust of the first message 150. The first network node 106a and/or the first trusted security zone 136a transmits the second message 156 to the second network node 106b.

[0047] The second network node 106b processes the second message 156 in the second trusted security zone 136b by analyzing the second message 156 to verify the continuity of trust of the second message 156, builds a third trust token 154c, and builds a third message 158 comprising the first trust token 154a, the second trust token 154b, and the third trust token 154c. Alternatively, only the third trust token 154c is encapsulated in the third message 158, and information about the level of trust associated with the first message 150 determined by the first network node 106a and the level of trust associated with the second message 156 determined by the second network node 106b is included in the third trust token 154c. The second network node

106b and/or the second trusted security zone 136b transmits the third message 158 to the third network node 106c.

[0048] The third network node 106c processes the third message 158, builds a fourth message 160 including a fourth trust token 154d in a similar fashion, and transmits the fourth message 160 to the trusted security zone 138 and/or the secure cloudlet 108. While the propagation of the content 152 through the trusted end-to-end communication link has been described by speaking of a plurality of different but related messages – a first message 150, a second message 156, a third message 158, and a fourth message 160 – according to a different manner of speaking or a different abstraction it could be said that one message propagates through the trusted end-to-end communication link, where the one message is extended or progressively composed in its transit of the link. In an embodiment, rather than a trust token or trust tokens being encapsulated in the messages 150, 156, 158, 160, the trust token and/or trust tokens may be linked to the messages 150, 156, 158, 160, such as being linked by being contained within a single payload of an IP packet.

[0049] Each of the messages 150, 156, 158, and 160 may be encapsulated as a payload of a data packet, for example as a payload of an IP packet or an IP datagram. Depending on the size of the content 152 and the one or more trust tokens 154, the content 152 may be segmented into multiple segments and each segment sent separately in a message as described above. It is understood that the trusted end-to-end communication link may comprise any number of network nodes 106 and that any number of corresponding messages may be built in communicating the content 152 from the MAT 102 to the secure cloudlet 108.

[0050] Turning now to FIG. 3A and FIG. 3B, a monitor 172 and a second system 178 for providing trusted end-to-end communication links is described. In an embodiment, the monitor 172 comprises a biometric sensor 174 and a human body parameter sensor 176. The trusted network nodes 106a, 106b, 106c may be abstracted to be parts of a network 190. Network 190 may comprise additional nodes and/or communication devices and may comprise one or more public networks, private networks, or a combination thereof. The body parameter sensor 176 may measure or sample a bodily parameter of a human being 170 such as a blood sugar level, a blood thickness, a blood pressure, a bodily temperature, a blood oxygen saturation level, a pulse rate, a heart rhythm, or another bodily parameter. In some contexts the body parameter sensor 176 may be referred to as a transducer or as comprising a

transducer. The body parameter sensor 176 may capture only raw data values that may not be directly related to a standard measurement value, and the raw data values may be processed by another device, for example processed by the secure application 132 executing in the trusted security zone 130 of the MAT 102, to represent the value of the sensed parameter in standard or customary units. For example the secure application 132 may process blood thickness raw data received from the monitor 172 and/or the body parameter sensor 176 to determine an international normalized ratio (INR) value of blood thickness based on the raw data. Alternatively, the body parameter sensor 176 and/or the monitor 172 may process the raw data and output these bodily parameter values in standard units.

[0051] The biometric sensor 174 captures a biometric signature of the human being 170, for example a finger print, a retinal scan, a face scan, a DNA signature, or other biometric signature. In some contexts, the biometric sensor 174 may be referred to as a biometric scanner. In an embodiment, the biometric sensor 174 and the body parameter sensor 176 may capture a biometric signature and a body parameter value substantially concurrently. In an embodiment, the monitor 172 may be configured such that the process of sensing the body parameter value by the body parameter sensor 176 and of capturing the biometric signature by the biometric sensor 174 are inseparable processes. For example, in an embodiment, the body parameter sensor 176 and the biometric sensor 174 are integrated into a single package such as a pulse oximeter clamp that also captures a finger print biometric. As is known by those skilled in the art, a standard oximeter clamp may be clamped to a finger to read both a pulse rate and a blood oxygen saturation percentage. The biometric signature may be associated with the body parameter value to identify and/or corroborate the identity of the human being 170.

[0052] The monitor 172 may be communicatively coupled to the MAT 102, for example via a wired communication link or via a short range wireless communication link such as NFC, Bluetooth®, or WiFi wireless links. The monitor 172 transmits the body parameter value and the biometric signature to the secure application 132 executing in the trusted security zone 130 of the MAT 102. The communication from the monitor 172 to the MAT 102 is assumed to be trusted and/or substantially invulnerable to hacking. The secure application 132 may produce a medical record content that comprises the body parameter value and the biometric signature. The biometric signature may be encoded and/or compressed in one or more ways and may

be encapsulated in the medical record content in the form of a pleogram. In an embodiment, the medical record content may comprise additional supporting information such as a date and a time of day. The secure application 132 may create a message comprising the medical record content and a trust token and send the message over a trusted end-to-end communication link to a secure application 184 executing in a trusted security zone 182 of a medical data server 180. The propagation of the message over the trusted end-to-end communication link may be substantially similarly to the process described above.

[0053] The secure application 184 may provide for storing the medical record content in a data store 186 coupled to the medical data server 180. The secure application 184, or a different secure application executing in the trust zone 182 of the medical data server 180, may process a plurality of medical record contents of a single human being 170 to track a chronic condition of the human 170. Alternatively, the secure application 184 may process a plurality of medical record contents associated with a plurality of selected humans 170, for example to calculate an efficacy of a medical treatment or drug.

[0054] In an embodiment, a secure application 196 executing in a trusted security zone 194 of a medical data analyzer 192 requests medical record contents from the medical data server 180, and the medical data server 180 sends the requested medical record contents via a trusted end-to-end communication link as described above. The medical records may be said to be verifiably confidential medical records. In some circumstances, regulatory agencies, such as the FDA, may inspect the use and communication of medical records to confirm the compliance with medical record privacy regulations. The secure application 196 may analyze the medical record contents to diagnose a condition of the human 170 and/or to recommend a medical treatment program for the human. A medical doctor using the medical data analyzer 192, for example, may write a prescription for the human being 170 and send the prescription to a pharmacy that is customarily used by the human being 170. The secure application 196 may analyze medical records of a plurality of humans 170 to determine an efficacy of a medical treatment or drug.

[0055] Turning now to FIG. 4, a method 200 is described. At block 202, a measurement of a parameter of a human being is obtained by a first sensor and a biometric of the human being is obtained by a second sensor. For example, a parameter of a human being is obtained by the body parameter sensor 176 and a

biometric signature of the human being is obtained by the biometric sensor 174 as described above. At block 204, input from the sensors is received by a secure application executing in a trusted security zone of a processor, whereby access to the input from the sensors by applications executing in a normal partition of the processor is blocked, wherein the input from the sensors comprise the measurement of the parameter of the human being and the biometric of the human being. At block 206, a message based on the input from the sensors is transmitted via a trusted end-to-end communication link to a medical data server, wherein an application that receives the message executes in a trusted security zone of the server. The message may be substantially similar to the first message 150 described above and may comprise a content portion and one or more trust tokens.

[0056] Turning now to FIG. 5, a method 220 is described. At block 222, a communication application is executed in a trusted security zone of a mobile access terminal. For example, the secure application 132 executes in the trusted security zone 130 of the MAT 102 as described above. At block 224, a message is sent from the mobile access terminal to a trusted communication application executing in a trusted security zone of a trusted enterprise edge node. For example, the secure application 132 and/or the trusted security zone 130 builds the message 150 comprising the content 152 and the trust token 154 and sends the message 150 to the first network node 106a. In an embodiment, the message may be sent from the MAT 102 to an enterprise communication network via a virtual private network (VPN) session. The message may be directed to a device or service outside the enterprise communication network and may then propagate in the external Internet. The first network node 106a may be an enterprise firewall or a multi-protocol label switching port of a router. Thus, in this embodiment the enterprise network edge may have a trusted security zone to support a trusted end-to-end communication link from the enterprise network to external devices and/or external functionalities. At block 226, the message is sent from the trusted enterprise edge node to a trusted cloudlet executing on a trusted security zone of a cloud based server according to the processes for providing continuity of trust in the propagation of the message described above.

[0057] Turning now to FIG. 6, a method 240 is described. At block 242, a measurement of a parameter of a human being is obtained by a first sensor and a biometric from the human being is obtained by a second sensor. For example, the body parameter sensor 176 obtains a parameter value, and the biometric sensor 174 obtains

a biometric signature from the human 170. At block 244, the measurement of the parameter and the biometric signature is transmitted from the sensors, for example the parameter value and the biometric signature are transmitted by the monitor 172 to the MAT 102. At block 246, the measurement of the parameter and the biometric signature are received by a processor executing in a trusted security zone of a mobile access terminal from the sensors, whereby access to the measurement of the parameter and the biometric from the sensors by applications executing in a normal execution mode is blocked. For example, the parameter and the biometric signature are received by the secure application 132 executing in the trusted security zone 130 of the MAT 102.

[0058] At block 247, a first message is transmitted based on the measurement of the parameter and the biometric by the mobile access terminal via an trusted end-to-end communication link to a medical data server, wherein the trusted end-to-end communication link comprises a wireless communication link. For example, the first message is the first message 150 and the wireless communication link is established between the radio transceiver 120 and the base transceiver station 104.

[0059] At block 248, the first message is received by an application that executes in a trusted security zone of the medical data server. At block 250, a second message based on the measurement of the parameter and the biometric is transmitted by the medical data server via an end-to-end trusted communication link to a computer associated with a medical doctor. At block 252, a medical care instruction for the human being is determined based on the second message. For example, a medical doctor using the medical data analyzer 192 diagnoses a condition or status of the human 170 and prescribes a medication to treat the condition or status.

[0060] FIG. 7 shows a wireless communications system including a mobile device 400. FIG. 4 depicts the mobile device 400, which is operable for implementing aspects of the present disclosure, but the present disclosure should not be limited to these implementations. In an embodiment, the mobile access terminal 102 may be implemented as the mobile device 400. Though illustrated as a mobile phone, the mobile device 400 may take various forms including a wireless handset, a pager, a personal digital assistant (PDA), a gaming device, or a media player. The mobile device 400 includes a display 402 and a touch-sensitive surface and/or keys 404 for input by a user. The mobile device 400 may present options for the user to select, controls for the user to actuate, and/or cursors or other indicators for the user to direct. The mobile device 400 may further accept data entry from the user, including numbers

to dial or various parameter values for configuring the operation of the handset. The mobile device 400 may further execute one or more software or firmware applications in response to user commands. These applications may configure the mobile device 400 to perform various customized functions in response to user interaction. Additionally, the mobile device 400 may be programmed and/or configured over-the-air, for example from a wireless base station, a wireless access point, or a peer mobile device 400. The mobile device 400 may execute a web browser application which enables the display 402 to show a web page. The web page may be obtained via wireless communications with a base transceiver station, a wireless network access node, a peer mobile device 400 or any other wireless communication network or system.

[0061] FIG. 8 shows a block diagram of the mobile device 400. While a variety of known components of handsets are depicted, in an embodiment a subset of the listed components and/or additional components not listed may be included in the mobile device 400. The mobile device 400 includes a digital signal processor (DSP) 502 and a memory 504. As shown, the mobile device 400 may further include an antenna and front end unit 506, a radio frequency (RF) transceiver 508, a baseband processing unit 510, a microphone 512, an earpiece speaker 514, a headset port 516, an input/output interface 518, a removable memory card 520, a universal serial bus (USB) port 522, an infrared port 524, a vibrator 526, a keypad 528, a touch screen liquid crystal display (LCD) with a touch sensitive surface 530, a touch screen/LCD controller 532, a camera 534, a camera controller 536, and a global positioning system (GPS) receiver 538. In an embodiment, the mobile device 400 may include another kind of display that does not provide a touch sensitive screen. In an embodiment, the DSP 502 may communicate directly with the memory 504 without passing through the input/output interface 518. Additionally, in an embodiment, the mobile device 400 may comprise other peripheral devices that provide other functionality.

[0062] The DSP 502 or some other form of controller or central processing unit operates to control the various components of the mobile device 400 in accordance with embedded software or firmware stored in memory 504 or stored in memory contained within the DSP 502 itself. In addition to the embedded software or firmware, the DSP 502 may execute other applications stored in the memory 504 or made available via information carrier media such as portable data storage media like the removable memory card 520 or via wired or wireless network communications. The application software may comprise a compiled set of machine-readable instructions that configure

the DSP 502 to provide the desired functionality, or the application software may be high-level software instructions to be processed by an interpreter or compiler to indirectly configure the DSP 502.

[0063] The DSP 502 may communicate with a wireless network via the analog baseband processing unit 510. In some embodiments, the communication may provide Internet connectivity, enabling a user to gain access to content on the Internet and to send and receive e-mail or text messages. The input/output interface 518 interconnects the DSP 502 and various memories and interfaces. The memory 504 and the removable memory card 520 may provide software and data to configure the operation of the DSP 502. Among the interfaces may be the USB port 522 and the infrared port 524. The USB port 522 may enable the mobile device 400 to function as a peripheral device to exchange information with a personal computer or other computer system. The infrared port 524 and other optional ports such as a Bluetooth® interface or an IEEE 802.11 compliant wireless interface may enable the mobile device 400 to communicate wirelessly with other nearby handsets and/or wireless base stations.

[0064] The keypad 528 couples to the DSP 502 via the interface 518 to provide one mechanism for the user to make selections, enter information, and otherwise provide input to the mobile device 400. Another input mechanism may be the touch screen LCD 530, which may also display text and/or graphics to the user. The touch screen LCD controller 532 couples the DSP 502 to the touch screen LCD 530. The GPS receiver 538 is coupled to the DSP 502 to decode global positioning system signals, thereby enabling the mobile device 400 to determine its position.

[0065] FIG. 9A illustrates a software environment 602 that may be implemented by the DSP 502. The DSP 502 executes operating system software 604 that provides a platform from which the rest of the software operates. The operating system software 604 may provide a variety of drivers for the handset hardware with standardized interfaces that are accessible to application software. The operating system software 604 may be coupled to and interact with application management services (AMS) 606 that transfer control between applications running on the mobile device 400. Also shown in FIG. 9A are a web browser application 608, a media player application 610, and JAVA applets 612. The web browser application 608 may be executed by the mobile device 400 to browse content and/or the Internet, for example when the mobile device 400 is coupled to a network via a wireless link. The web browser application 608 may permit a user to enter information into forms and select links to retrieve and view

web pages. The media player application 610 may be executed by the mobile device 400 to play audio or audiovisual media. The JAVA applets 612 may be executed by the mobile device 400 to provide a variety of functionality including games, utilities, and other functionality.

[0066] FIG. 9B illustrates an alternative software environment 620 that may be implemented by the DSP 502. The DSP 502 executes operating system software 628 and an execution runtime 630. The DSP 502 executes applications 622 that may execute in the execution runtime 630 and may rely upon services provided by the application framework 624. Applications 622 and the application framework 624 may rely upon functionality provided via the libraries 626.

[0067] FIG. 10 illustrates a computer system 380 suitable for implementing one or more embodiments disclosed herein. The computer system 380 includes a processor 382 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 384, read only memory (ROM) 386, random access memory (RAM) 388, input/output (I/O) devices 390, and network connectivity devices 392. The processor 382 may be implemented as one or more CPU chips.

[0068] It is understood that by programming and/or loading executable instructions onto the computer system 380, at least one of the CPU 382, the RAM 388, and the ROM 386 are changed, transforming the computer system 380 in part into a particular machine or apparatus having the novel functionality taught by the present disclosure. It is fundamental to the electrical engineering and software engineering arts that functionality that can be implemented by loading executable software into a computer can be converted to a hardware implementation by well known design rules. Decisions between implementing a concept in software versus hardware typically hinge on considerations of stability of the design and numbers of units to be produced rather than any issues involved in translating from the software domain to the hardware domain. Generally, a design that is still subject to frequent change may be preferred to be implemented in software, because re-spinning a hardware implementation is more expensive than re-spinning a software design. Generally, a design that is stable that will be produced in large volume may be preferred to be implemented in hardware, for example in an application specific integrated circuit (ASIC), because for large production runs the hardware implementation may be less expensive than the software implementation. Often a design may be developed and tested in a software form and

later transformed, by well known design rules, to an equivalent hardware implementation in an application specific integrated circuit that hardwires the instructions of the software. In the same manner as a machine controlled by a new ASIC is a particular machine or apparatus, likewise a computer that has been programmed and/or loaded with executable instructions may be viewed as a particular machine or apparatus.

[0069] The secondary storage 384 is typically comprised of one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM 388 is not large enough to hold all working data. Secondary storage 384 may be used to store programs which are loaded into RAM 388 when such programs are selected for execution. The ROM 386 is used to store instructions and perhaps data which are read during program execution. ROM 386 is a non-volatile memory device which typically has a small memory capacity relative to the larger memory capacity of secondary storage 384. The RAM 388 is used to store volatile data and perhaps to store instructions. Access to both ROM 386 and RAM 388 is typically faster than to secondary storage 384. The secondary storage 384, the RAM 388, and/or the ROM 386 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

[0070] I/O devices 390 may include printers, video monitors, liquid crystal displays (LCDs), touch screen displays, keyboards, keypads, switches, dials, mice, track balls, voice recognizers, card readers, paper tape readers, or other well-known input devices.

[0071] The network connectivity devices 392 may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area network (WLAN) cards, radio transceiver cards such as code division multiple access (CDMA), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMAX), 4^{th} generation, 5^{th} generation, and/or other air interface protocol radio transceiver cards, and other well-known network devices. These network connectivity devices 392 may enable the processor 382 to communicate with the Internet or one or more intranets. With such a network connection, it is contemplated that the processor 382 might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Such information, which is often represented as a sequence of instructions to be executed using processor 382, may be received from

and outputted to the network, for example, in the form of a computer data signal embodied in a carrier wave.

[0072] Such information, which may include data or instructions to be executed using processor 382 for example, may be received from and outputted to the network, for example, in the form of a computer data baseband signal or signal embodied in a carrier wave. The baseband signal or signal embedded in the carrier wave, or other types of signals currently used or hereafter developed, may be generated according to several methods well known to one skilled in the art. The baseband signal and/or signal embedded in the carrier wave may be referred to in some contexts as a transitory signal.

[0073] The processor 382 executes instructions, codes, computer programs, scripts which it accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage 384), ROM 386, RAM 388, or the network connectivity devices 392. While only one processor 382 is shown, multiple processors may be present. Thus, while instructions may be discussed as executed by a processor, the instructions may be executed simultaneously, serially, or otherwise executed by one or multiple processors. Instructions, codes, computer programs, scripts, and/or data that may be accessed from the secondary storage 384, for example, hard drives, floppy disks, optical disks, and/or other device, the ROM 386, and/or the RAM 388 may be referred to in some contexts as non-transitory instructions and/or non-transitory information.

[0074] In an embodiment, the computer system 380 may comprise two or more computers in communication with each other that collaborate to perform a task. For example, but not by way of limitation, an application may be partitioned in such a way as to permit concurrent and/or parallel processing of the instructions of the application. Alternatively, the data processed by the application may be partitioned in such a way as to permit concurrent and/or parallel processing of different portions of a data set by the two or more computers. In an embodiment, virtualization software may be employed by the computer system 380 to provide the functionality of a number of servers that is not directly bound to the number of computers in the computer system 380. For example, virtualization software may provide twenty virtual servers on four physical computers. In an embodiment, the functionality disclosed above may be provided by executing the application and/or applications in a cloud computing environment. Cloud computing may comprise providing computing services via a network connection using dynamically

scalable computing resources. Cloud computing may be supported, at least in part, by virtualization software. A cloud computing environment may be established by an enterprise and/or may be hired on an as-needed basis from a third party provider. Some cloud computing environments may comprise cloud computing resources owned and operated by the enterprise as well as cloud computing resources hired and/or leased from a third party provider.

[0075] In an embodiment, some or all of the functionality disclosed above may be provided as a computer program product. The computer program product may comprise one or more computer readable storage medium having computer usable program code embodied therein to implement the functionality disclosed above. The computer program product may comprise data structures, executable instructions, and other computer usable program code. The computer program product may be embodied in removable computer storage media and/or non-removable computer storage media. The removable computer readable storage medium may comprise, without limitation, a paper tape, a magnetic tape, magnetic disk, an optical disk, a solid state memory chip, for example analog magnetic tape, compact disk read only memory (CD-ROM) disks, floppy disks, jump drives, digital cards, multimedia cards, and others. The computer program product may be suitable for loading, by the computer system 380, at least portions of the contents of the computer program product to the secondary storage 384, to the ROM 386, to the RAM 388, and/or to other non-volatile memory and volatile memory of the computer system 380. The processor 382 may process the executable instructions and/or data structures in part by directly accessing the computer program product, for example by reading from a CD-ROM disk inserted into a disk drive peripheral of the computer system 380. Alternatively, the processor 382 may process the executable instructions and/or data structures by remotely accessing the computer program product, for example by downloading the executable instructions and/or data structures from a remote server through the network connectivity devices 392. The computer program product may comprise instructions that promote the loading and/or copying of data, data structures, files, and/or executable instructions to the secondary storage 384, to the ROM 386, to the RAM 388, and/or to other non-volatile memory and volatile memory of the computer system 380.

[0076] In some contexts, the secondary storage 384, the ROM 386, and the RAM 388 may be referred to as a non-transitory computer readable medium or a computer readable storage media. A dynamic RAM embodiment of the RAM 388, likewise, may

be referred to as a non-transitory computer readable medium in that while the dynamic RAM receives electrical power and is operated in accordance with its design, for example during a period of time during which the computer 380 is turned on and operational, the dynamic RAM stores information that is written to it. Similarly, the processor 382 may comprise an internal RAM, an internal ROM, a cache memory, and/or other internal non-transitory storage blocks, sections, or components that may be referred to in some contexts as non-transitory computer readable media or computer readable storage media.

[0077] While several embodiments have been provided in the present disclosure, it should be understood that the disclosed systems and methods may be embodied in many other specific forms without departing from the spirit or scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details given herein. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted or not implemented.

[0078] Also, techniques, systems, subsystems, and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as directly coupled or communicating with each other may be indirectly coupled or communicating through some interface, device, or intermediate component, whether electrically, mechanically, or otherwise. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

CLAIMS

What is claimed is:

1. A method of delivery of medical data via a trusted end-to-end communication link, comprising:

obtaining a measurement of a parameter of a human being by a first sensor;

obtaining a biometric from the human being by a second sensor;

receiving input from the first and second sensors by a secure application executing in a trusted security zone of a processor, whereby access to the input from the first and second sensors by applications executing in a normal partition of the processor is blocked, wherein the input from the first and second sensor comprises the measurement of the parameter and the biometric; and

transmitting a message based on the input from the first and second sensor via a trusted end-to-end communication link to a medical data server, wherein an application that receives the message executes in a trusted security zone of the server.

2. The method of claim 1, wherein the trusted security zone is provided by the processor blocking access by the applications executing in the normal partition of the processor from accessing memory, reading inputs, and writing outputs while the secure application executes in the trusted security zone.

3. The method of claim 1, wherein the trusted security zone is provided by a first virtual processor and wherein the normal partition is provided by a second virtual processor.

4. The method of claim 1, wherein the trusted security zone is provided by a first physical processor and the normal partition is provided by a second physical processor.

5. The method of claim 1, wherein the parameter of the human being is a blood sugar level, a blood thickness, a blood pressure, a bodily temperature, a blood oxygen saturation level, a pulse rate, or a heart rhythm.

6. The method of claim 1, wherein the biometric is a fingerprint scan, a retinal scan, or a face scan.

7. The method of claim 1, wherein the medical data server comprises a plurality of medical records associated with a plurality of different human beings, wherein each medical record comprises a measurement of a parameter of a one of the human beings and a biometric of the one of the human beings, further comprising analyzing the plurality of medical records to perform an efficacy of a medical treatment regime.

8. A method establishing a trusted end-to-end communication link, comprising:

executing a communication application in a trusted security zone of a mobile access terminal;

sending a message from the mobile access terminal to a trusted communication application executing in a trusted security zone of a trusted enterprise edge node; and

sending the message from the trusted enterprise edge node to a trusted cloudlet executing on in a trusted security zone of a cloud based server.

9. The method of claim 8, wherein the trusted enterprise edge node is one of a firewall server or a multi-protocol label switching (MPLS) port on a router.

10. The method of claim 8, wherein the trusted security zone of the trusted enterprise edge node is provided by a processor of the trusted enterprise edge node blocking access by other applications executing in a normal partition of the processor from accessing memory, reading inputs, and writing outputs while the trusted communication application executes in the trusted security zone of the trusted enterprise edge node.

11. The method of claim 8, wherein the trusted security zone of the trusted enterprise edge node is provided by a first virtual processor and wherein a normal partition is provided by a second virtual processor, and while the first virtual processor is executing, the second virtual processor does not execute instructions.

12. The method of claim 8, wherein the mobile access terminal sends the message to the trusted communication application via a trusted end-to-end communication link.

13. The method of claim 12, wherein a portion of the trusted end-to-end communication link comprises a cellular wireless communication link.

14. The method of claim 13, wherein the cellular wireless communication link is provided based on at least one of a code division multiple access (CDMA), global system for mobile communication (GSM), a long-term evolution (LTE), or a worldwide interoperability for microwave access (WiMAX) communication protocol.

15. A method of accessing medical diagnostic information, comprising:

obtaining a measurement of a parameter of a human being from a first sensor and a biometric from the human being from a second sensor;

transmitting the measurement of the parameter and the biometric from the first and second sensors;

receiving the measurement of the parameter and the biometric from the first and second sensors by a processor executing in a trusted security zone of a

mobile access terminal, whereby access to the measurement of the parameter and the biometric from the first and second sensors by applications executing in a normal execution mode is blocked;

transmitting a first message based on the measurement of the parameter and the biometric by the mobile access terminal via a trusted end-to-end communication link to a medical data server, wherein the trusted end-to-end communication link comprises a wireless communication link;

receiving the first message by an application that executes in a trusted security zone of the medical data server;

transmitting a second message based on the measurement of the parameter and the biometric by the medical data server via a trusted end-to-end communication link to a computer associated with a medical doctor; and

determining a medical care instruction for the human being based on the second message.

16. The method of claim 15, wherein the parameter of the human being is a blood sugar level, a blood thickness, a blood pressure, a bodily temperature, a blood oxygen saturation level, a pulse rate, or a heart rhythm.

17. The method of claim 15, wherein the biometric is one of a fingerprint scan, a retinal scan, or a face scan.

18. The method of claim 15, wherein the second message provides verifiably confidential medical records.

19. The method of claim 15, wherein the medical data server maintains a data store of medical records associated with a plurality of different human beings, each medical record comprising a parameter of and a biometric from one of the human beings, further comprising analyzing a plurality of the medical records to determine an efficacy of a medical treatment regime.

20. The method of claim 15, further comprising receiving with the first message a plurality of trust tokens, each trust token associated with a trusted security zone of a network node in the trusted end-to-end communication link from the mobile access terminal to the medical data server and analyzing the plurality of trust tokens to validate the trust level of the trusted end-to-end communication link.

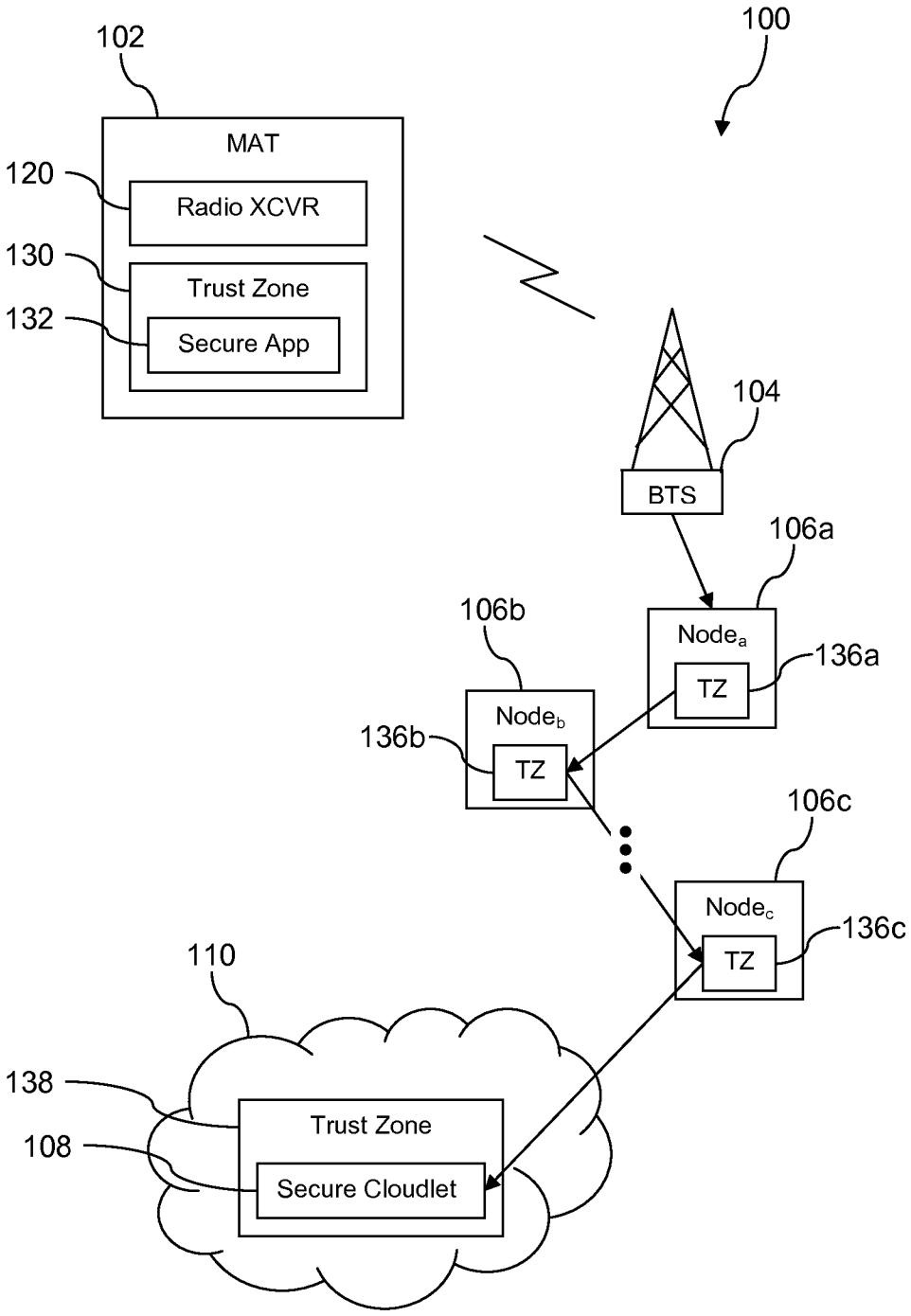
100
102
MAT
120
Radio XCVR
130
Trust Zone
132
Secure App
104
BTS
106a
Node$_a$
136a
TZ
106b
Node$_b$
136b
TZ
106c
Node$_c$
136c
TZ
110
138
Trust Zone
108
Secure Cloudlet

FIG. 1

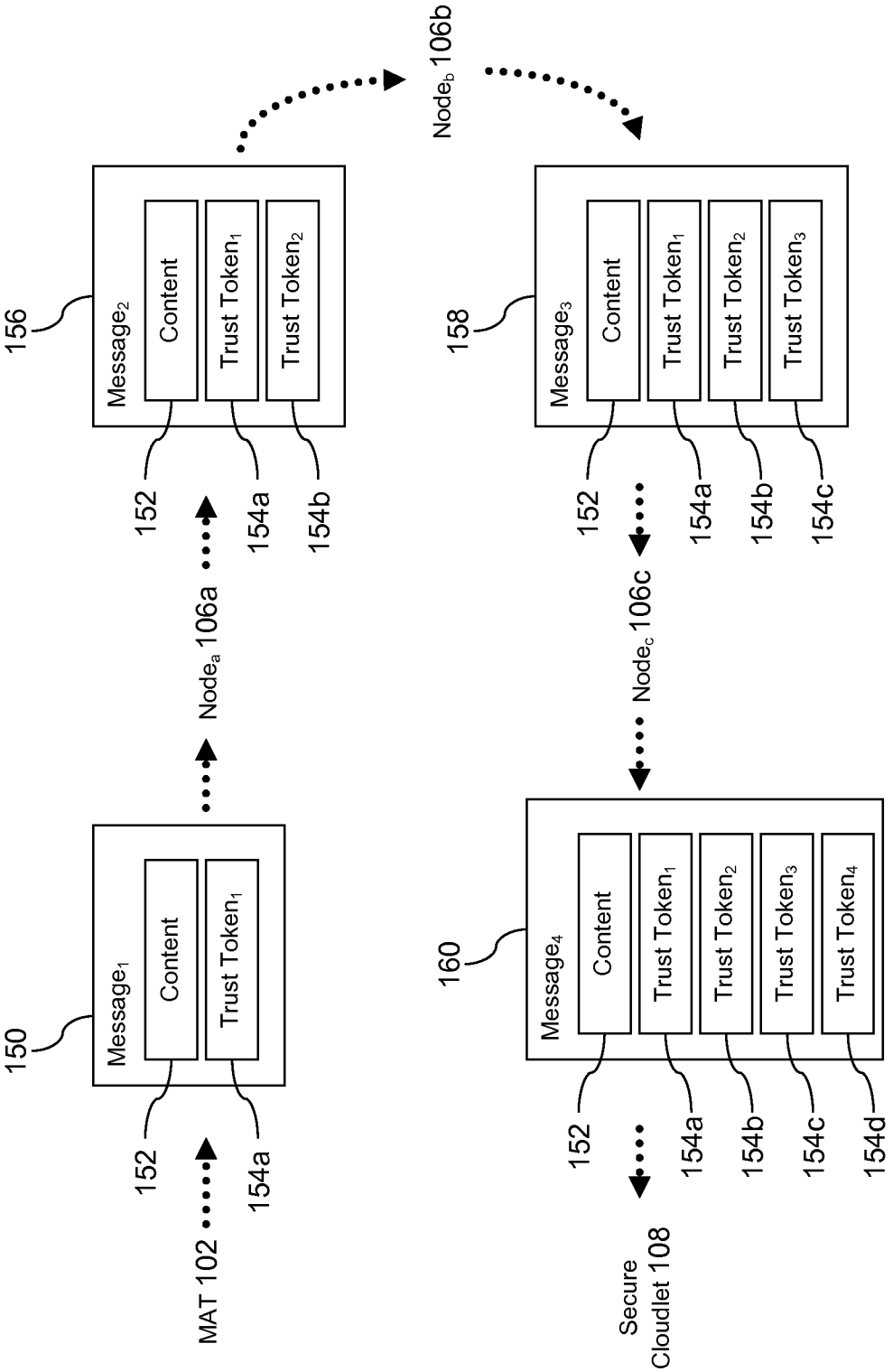
MAT 102
Node$_a$ 106a
Node$_b$ 106b
Node$_c$ 106c
Secure Cloudlet 108
150
Message$_1$
Content
Trust Token$_1$
152
154a
156
Message$_2$
Content
Trust Token$_1$
Trust Token$_2$
152
154a
154b
158
Message$_3$
Content
Trust Token$_1$
Trust Token$_2$
Trust Token$_3$
152
154a
154b
154c
160
Message$_4$
Content
Trust Token$_1$
Trust Token$_2$
Trust Token$_3$
Trust Token$_4$
152
154a
154b
154c
154d

FIG. 2

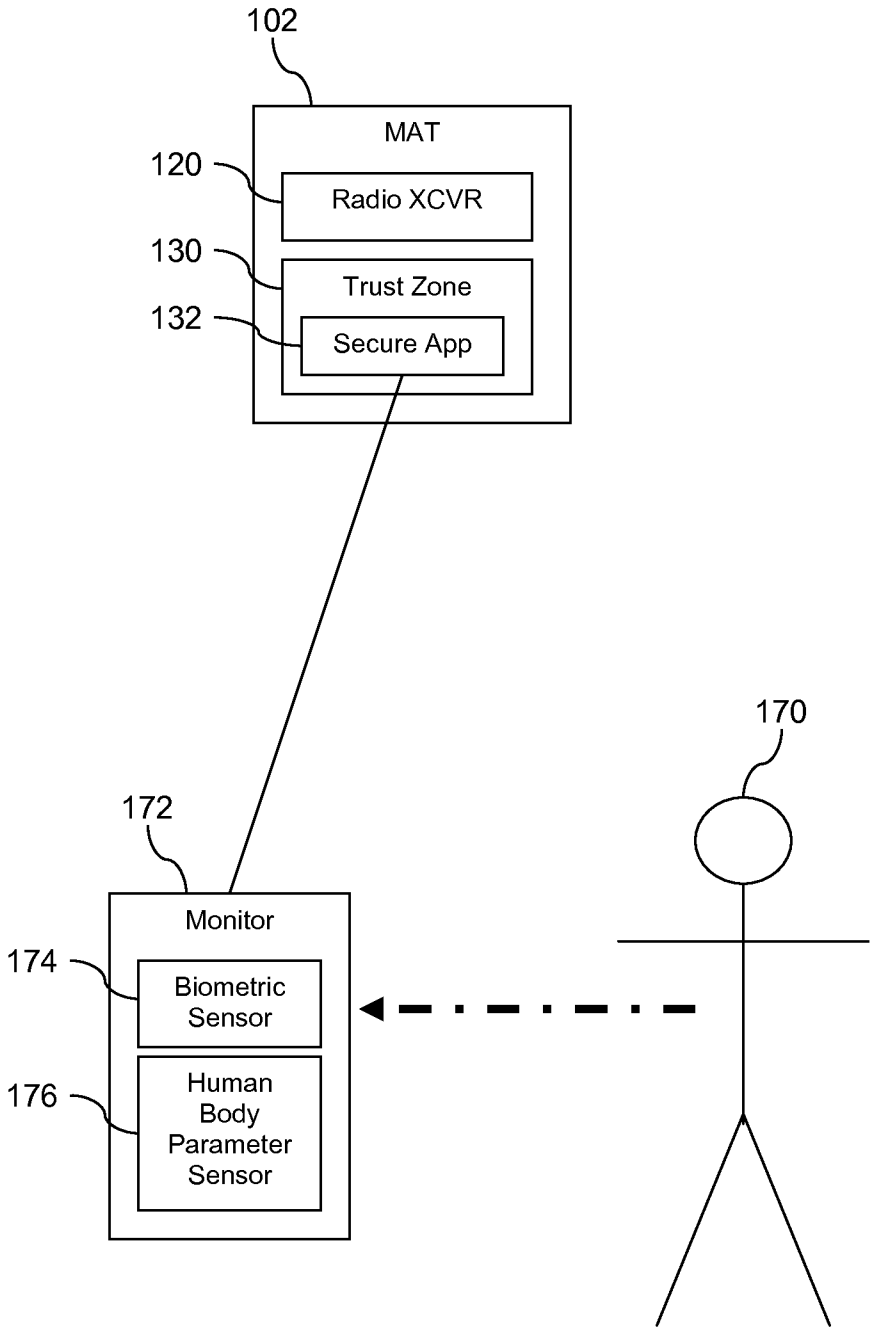
102
MAT
120
Radio XCVR
130
Trust Zone
132
Secure App
170
172
Monitor
174
Biometric Sensor
176
Human Body Parameter Sensor

FIG. 3A

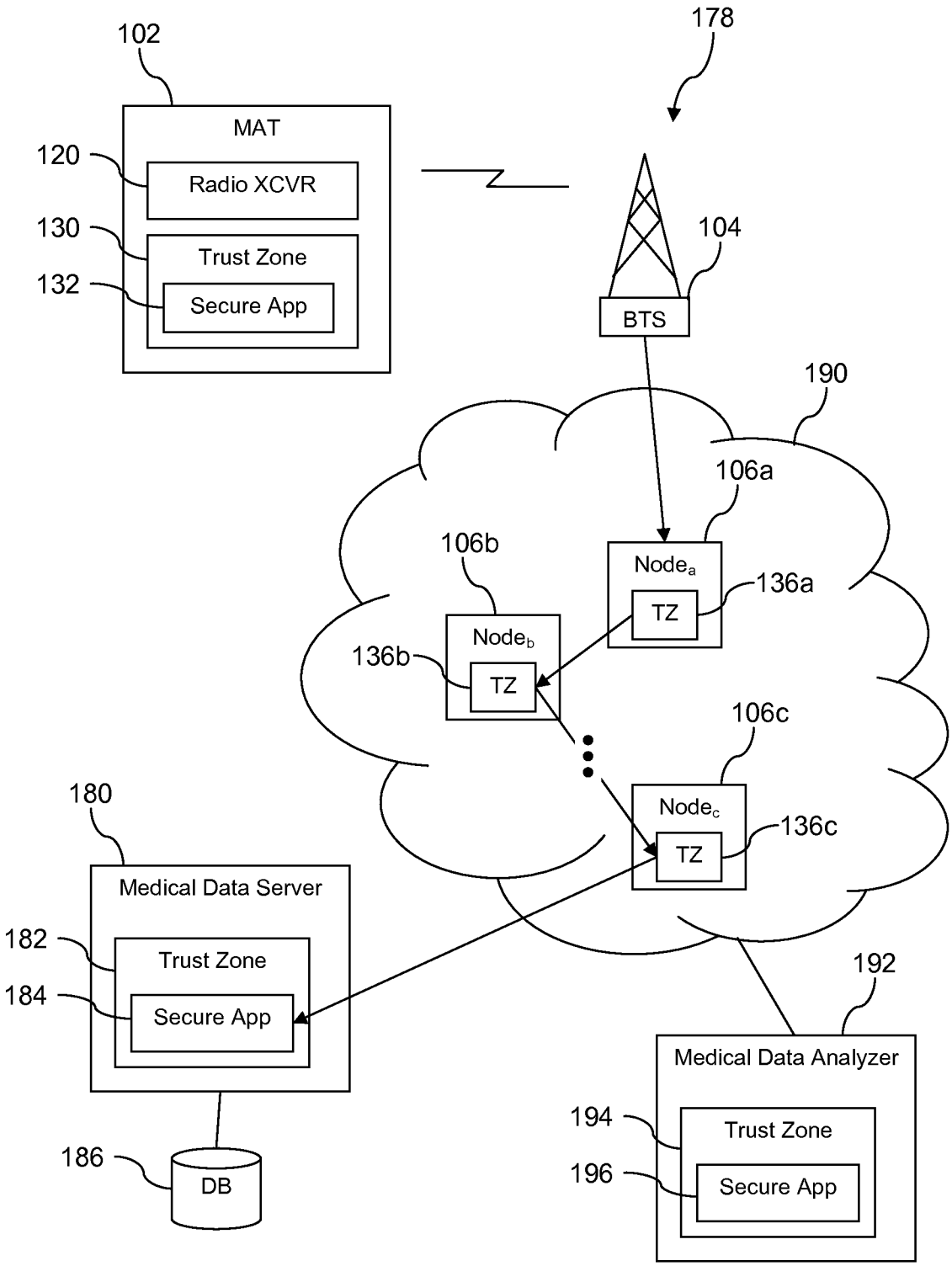
102
MAT
120
Radio XCVR
130
Trust Zone
132
Secure App
178
104
BTS
190
106a
106b
Node$_a$
136a
TZ
Node$_b$
136b
TZ
106c
Node$_c$
136c
TZ
180
Medical Data Server
182
Trust Zone
184
Secure App
186
DB
192
Medical Data Analyzer
194
Trust Zone
196
Secure App

FIG. 3B

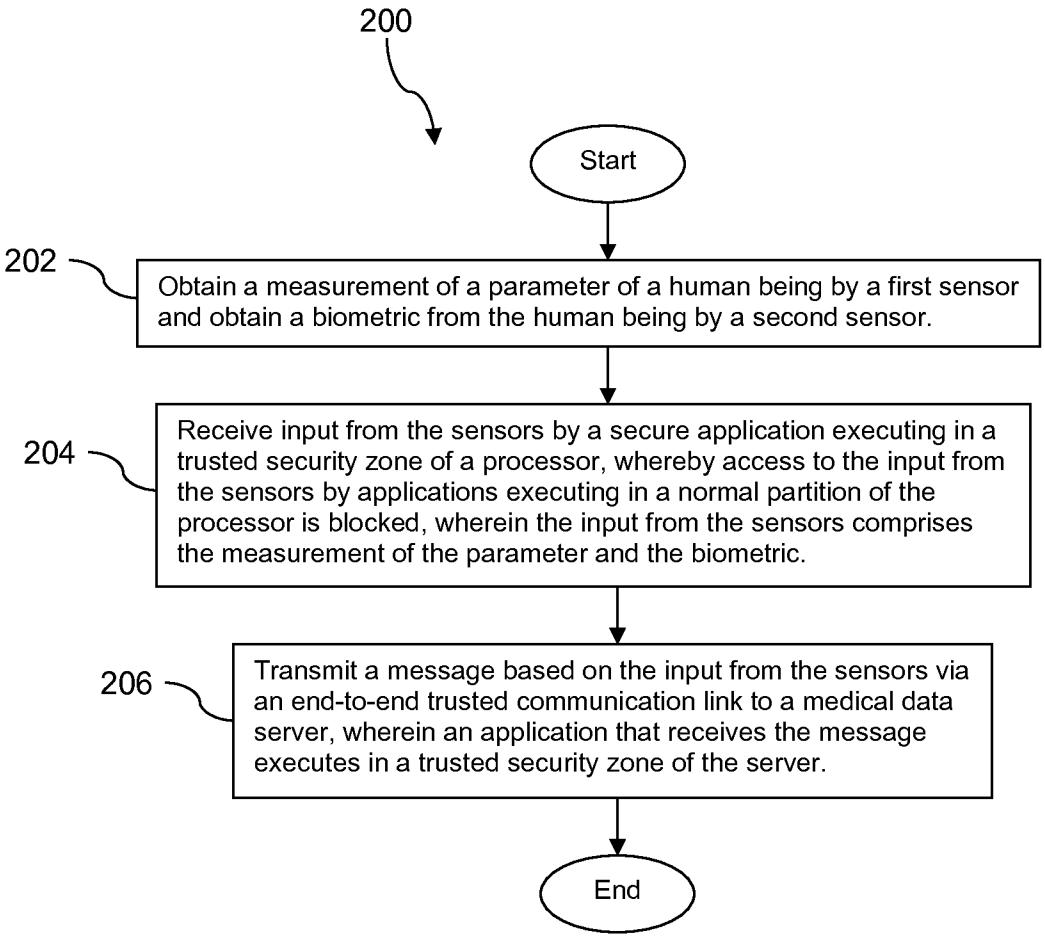
200
Start
202
Obtain a measurement of a parameter of a human being by a first sensor and obtain a biometric from the human being by a second sensor.
204
Receive input from the sensors by a secure application executing in a trusted security zone of a processor, whereby access to the input from the sensors by applications executing in a normal partition of the processor is blocked, wherein the input from the sensors comprises the measurement of the parameter and the biometric.
206
Transmit a message based on the input from the sensors via an end-to-end trusted communication link to a medical data server, wherein an application that receives the message executes in a trusted security zone of the server.
End

FIG. 4

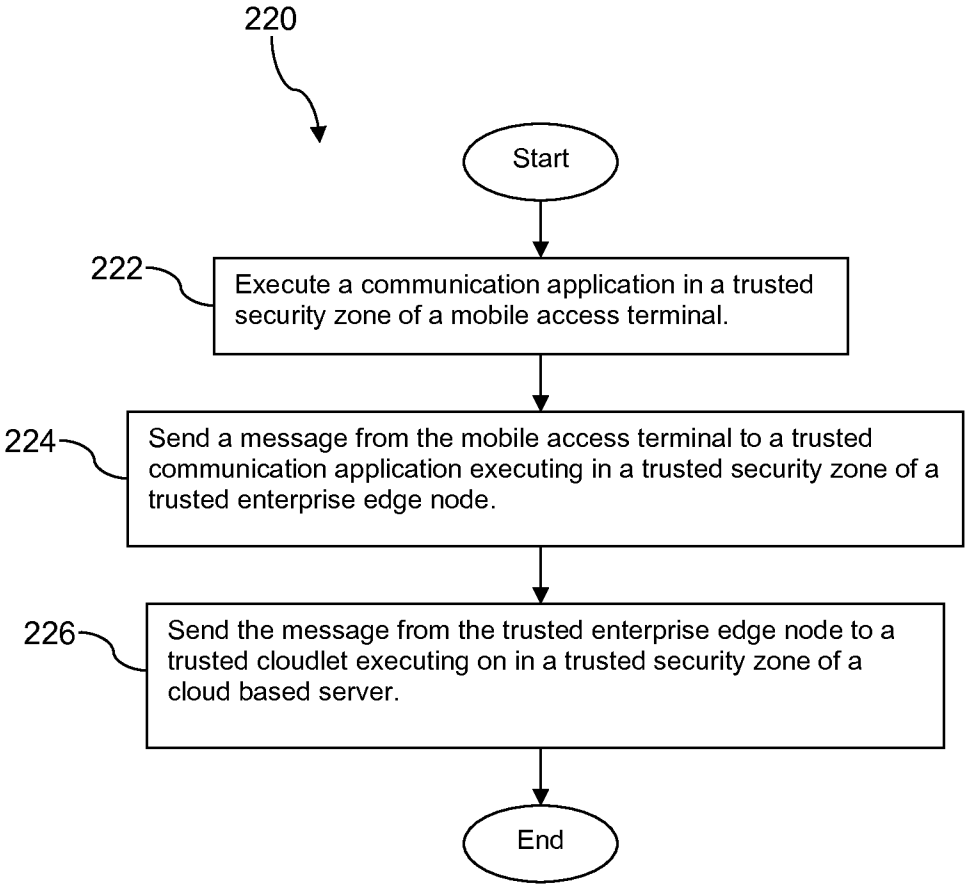
220
Start
222
Execute a communication application in a trusted security zone of a mobile access terminal.
224
Send a message from the mobile access terminal to a trusted communication application executing in a trusted security zone of a trusted enterprise edge node.
226
Send the message from the trusted enterprise edge node to a trusted cloudlet executing on in a trusted security zone of a cloud based server.
End

FIG. 5

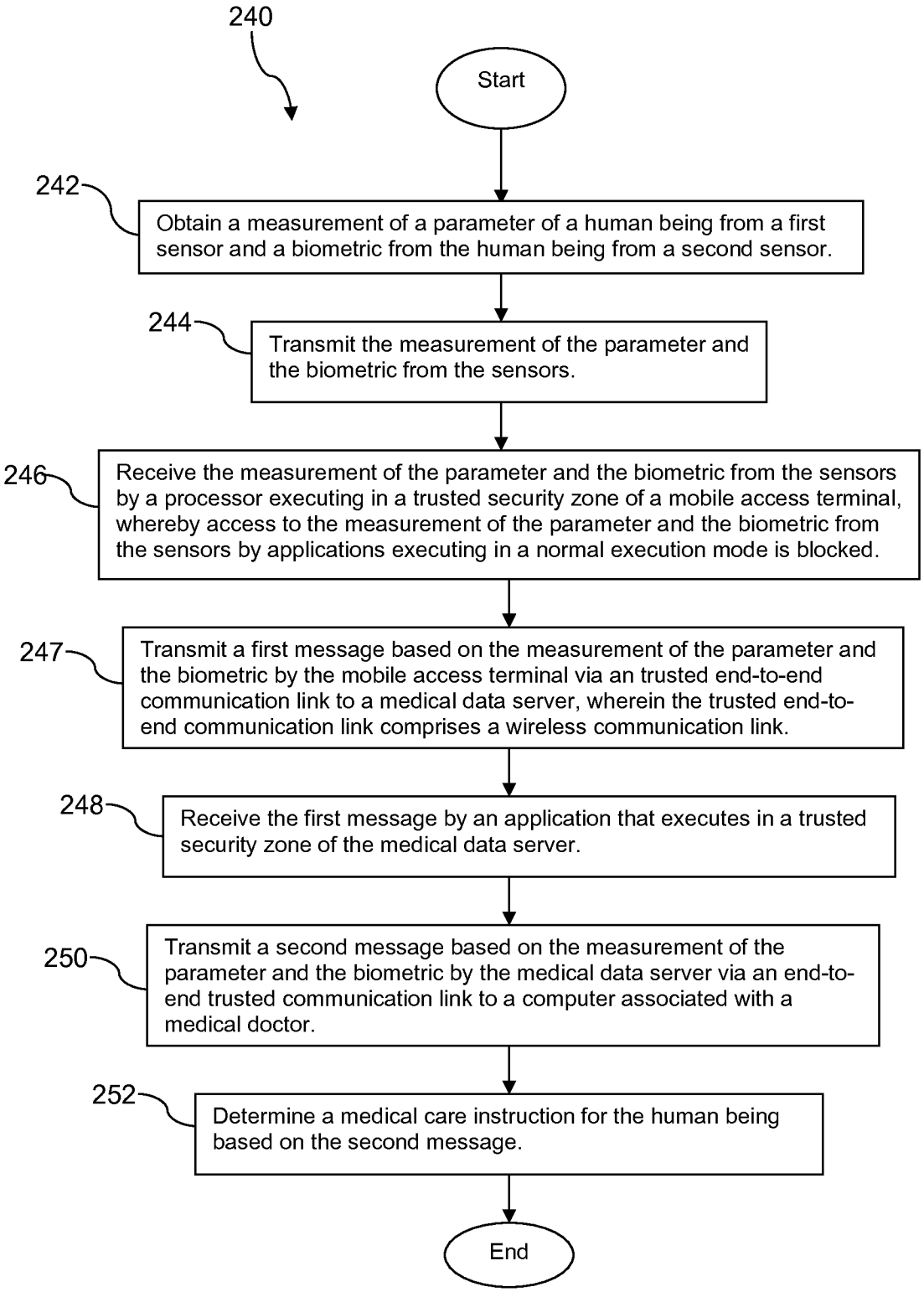
240
Start
242
Obtain a measurement of a parameter of a human being from a first sensor and a biometric from the human being from a second sensor.
244
Transmit the measurement of the parameter and the biometric from the sensors.
246
Receive the measurement of the parameter and the biometric from the sensors by a processor executing in a trusted security zone of a mobile access terminal, whereby access to the measurement of the parameter and the biometric from the sensors by applications executing in a normal execution mode is blocked.
247
Transmit a first message based on the measurement of the parameter and the biometric by the mobile access terminal via an trusted end-to-end communication link to a medical data server, wherein the trusted end-to-end communication link comprises a wireless communication link.
248
Receive the first message by an application that executes in a trusted security zone of the medical data server.
250
Transmit a second message based on the measurement of the parameter and the biometric by the medical data server via an end-to-end trusted communication link to a computer associated with a medical doctor.
252
Determine a medical care instruction for the human being based on the second message.
End

FIG. 6

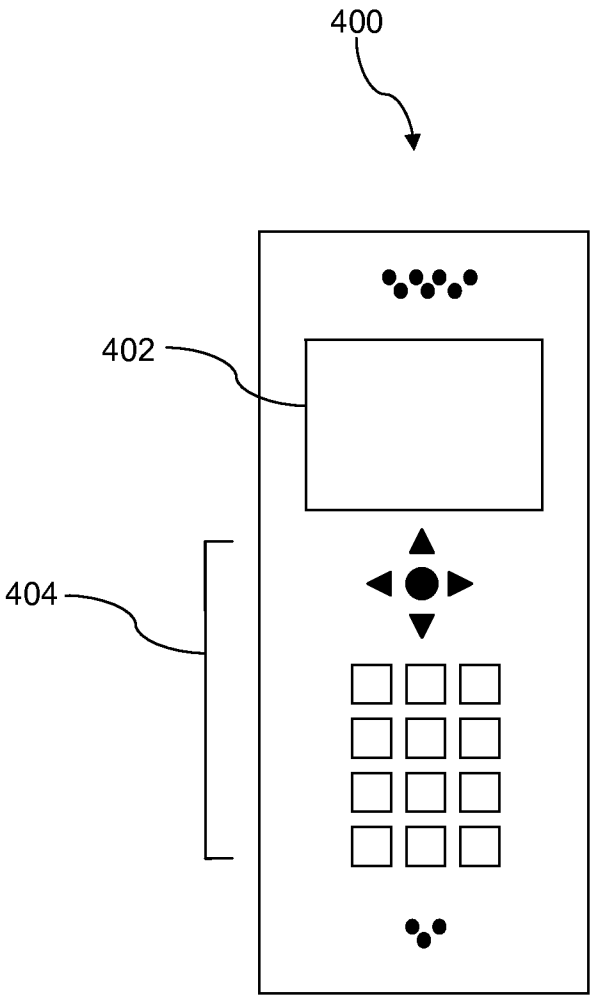

FIG. 7

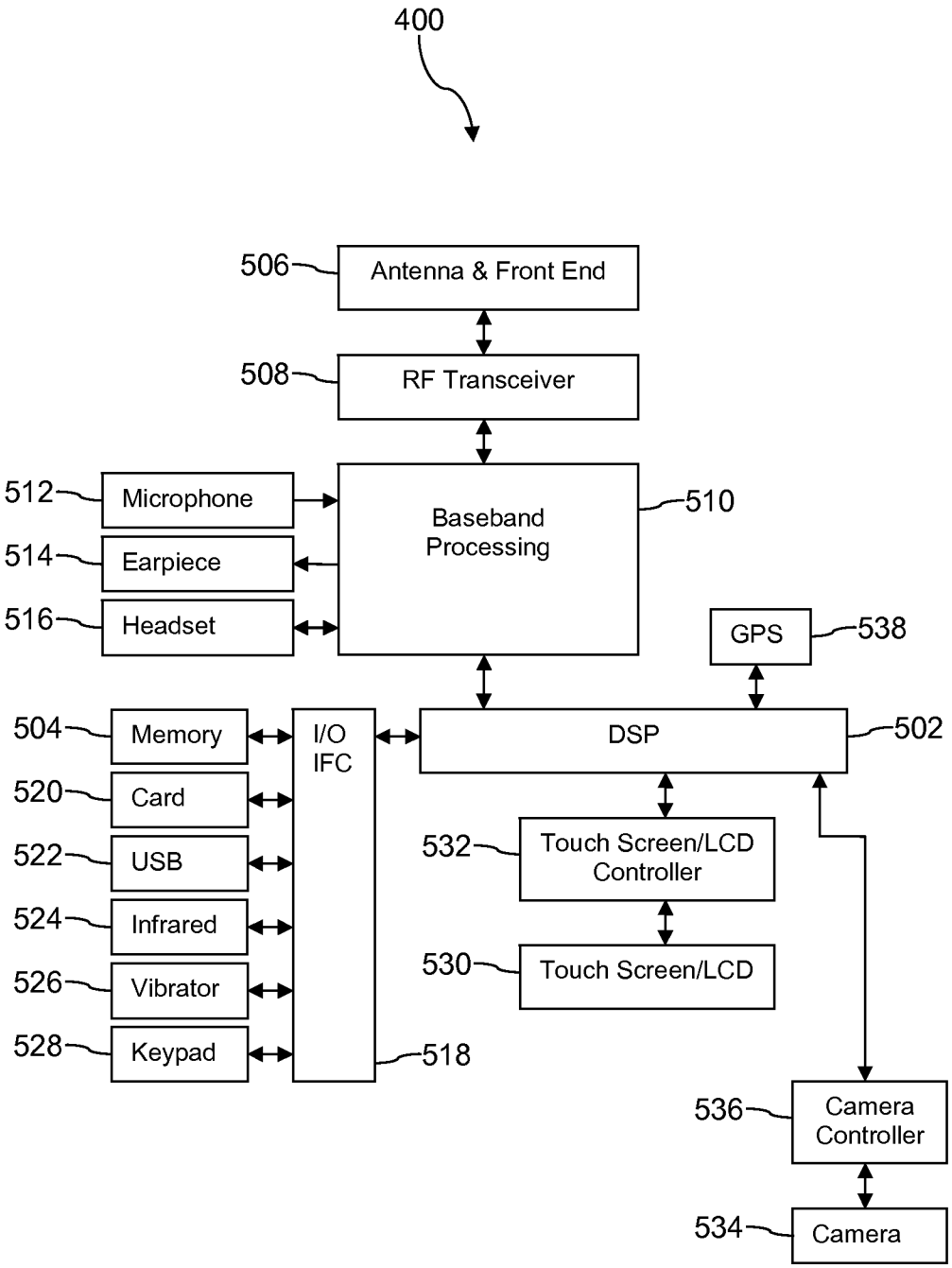
400
506
Antenna & Front End
508
RF Transceiver
512
Microphone
514
Earpiece
516
Headset
Baseband Processing
510
GPS
538
504
Memory
520
Card
522
USB
524
Infrared
526
Vibrator
528
Keypad
I/O IFC
518
DSP
502
532
Touch Screen/LCD Controller
530
Touch Screen/LCD
536
Camera Controller
534
Camera

FIG. 8

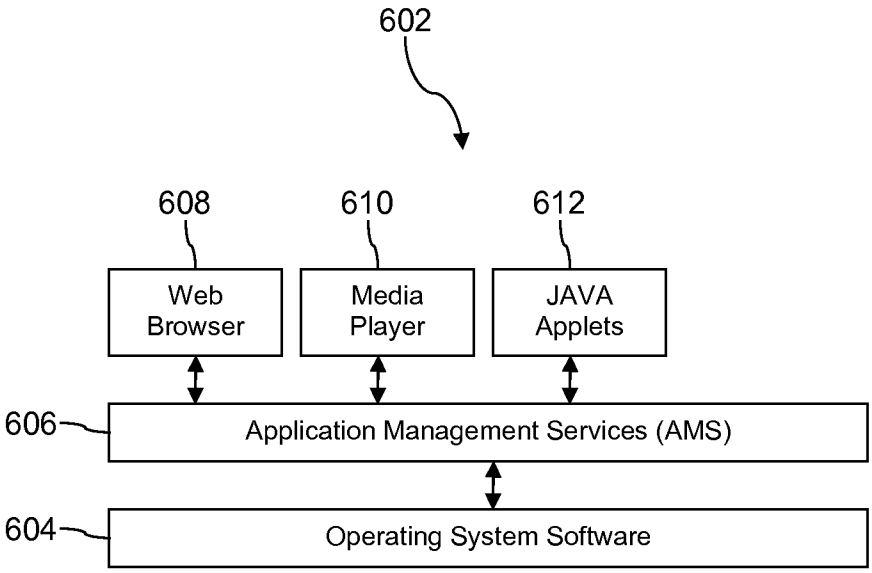
602
608
610
612
Web Browser
Media Player
JAVA Applets
606
Application Management Services (AMS)
604
Operating System Software

FIG. 9A

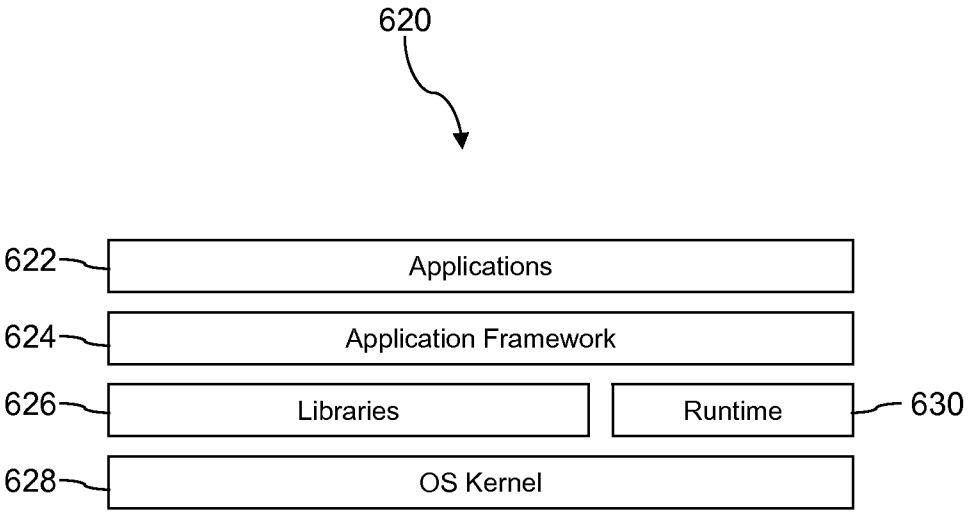
620
622
Applications
624
Application Framework
626
Libraries
Runtime
630
628
OS Kernel

FIG. 9B

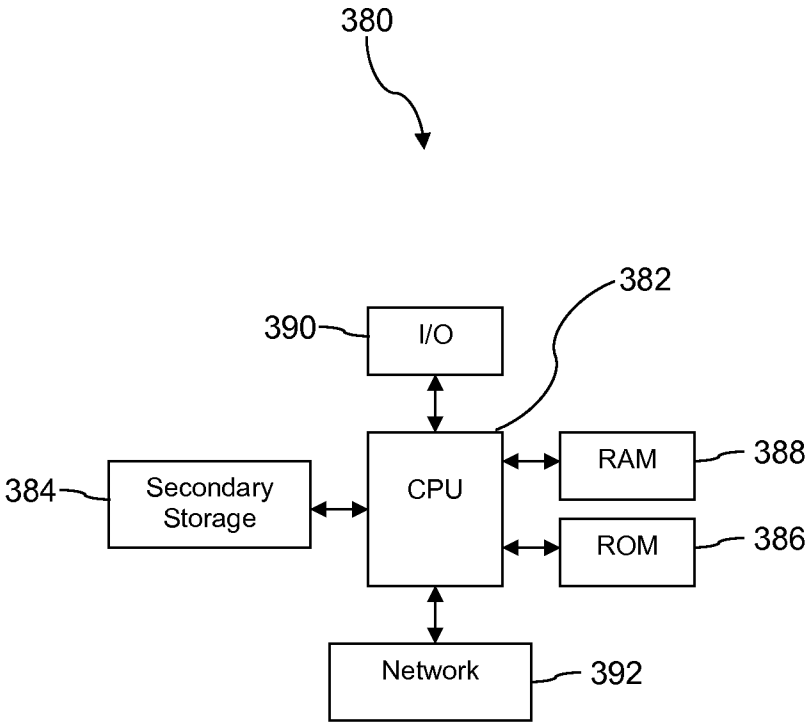
380
382
390
I/O
384
Secondary Storage
CPU
RAM
388
ROM
386
Network
392

FIG. 10