



- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *G06Q 50/00* (2006.01)
- (21) **International Application Number:**
PCT/US2016/062160
- (22) **International Filing Date:**
16 November 2016 (16.11.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
14/976,397 21 December 2015 (21.12.2015) US
- (71) **Applicant:** MCAFEE, INC. [US/US]; 2821 Mission College Boulevard, Santa Clara, California 95054-1838 (US).
- (72) **Inventors:** MEHTA, Kunal; 2174 NW Thorncroft Drive, Apartment No. 1034, Hillsboro, Oregon 97124 (US). WOODWARD, Carl D.; 4515 Carlyle Court, Apt. #3303, Santa Clara, California 95054 (US). GROBMAN, Steven; 1511 Southridge Court, El Dorado Hills, CA 95762 (US). DURAND, Ryan; 702 NW Adwick Drive, Hillsboro, Oregon 97006 (US). HUNT, Simon; 2120 Sheepshead Drive, Naples, Florida 34102 (US).
- (74) **Agent:** CRANDALL, Sean C.; Patent Capital Group, 2816 Lago Vista Lane, Rockwall, Texas 75032 (US).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (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).

[Continued on next page]

(54) **Title:** VERIFIED SOCIAL MEDIA CONTENT

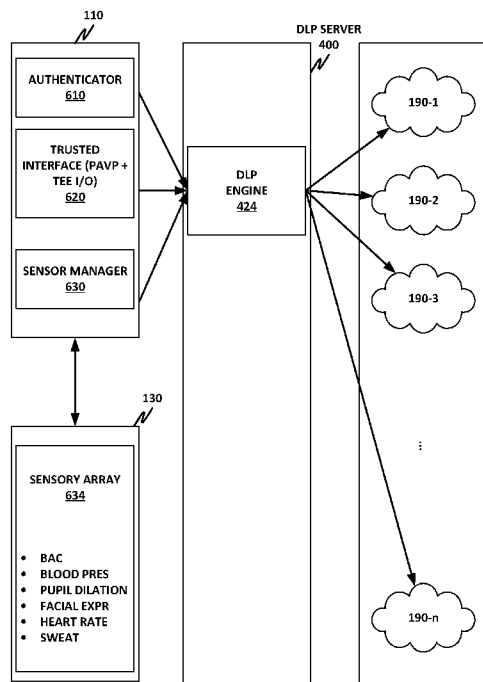


Fig. 6

(57) **Abstract:** In an example, there is disclosed a computing apparatus, comprising: a psychological state data interface to receive psychological state data; one or more logic elements, including at least one hardware element, comprising a verification engine to: receive a requested user action; receive a psychological state input via the psychological state data interface; analyze the psychological state input; and bar the requested user action at least partly responsive to the analyzing.

**Declarations under Rule 4.17:**

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

VERIFIED SOCIAL MEDIA CONTENT

Cross-Reference to Related Application

[0001] This application claims the benefit of priority to U.S. Nonprovisional Patent Application No. 14/976,397 filed 21 December 2015 entitled, "VERIFIED SOCIAL MEDIA CONTENT", which is incorporated herein by reference in its entirety.

Field of the specification

[0002] This disclosure relates in general to the field of network security, and more particularly, though not exclusively to, a system and method for verifying social media content.

Background

[0003] In contemporary social media platforms, such as Facebook, Instagram, Tumblr, or Snapchat, and many others, users have the ability to instantly post their thoughts in a stream-of-consciousness fashion. Users can also post photographs, documents, and links very easily. This ease of use can make for a rich, entertaining social media experience.

Brief Description of the Drawings

[0004] The present disclosure is best understood from the following detailed description when read with the accompanying figures. It is emphasized that, in accordance with the standard practice in the industry, various features are not necessarily drawn to scale, and are used for illustration purposes only. Where a scale is shown, explicitly or implicitly, it provides only one illustrative example. In other embodiments, the dimensions of the various features may be arbitrarily increased or reduced for clarity of discussion.

[0005] FIGURE 1 is a block diagram of a social network according to one or more examples of the present specification.

[0006] FIGURE 2 is a block diagram of a client device according to one or more examples of the present specification.

[0007] FIGURE 3 is a block diagram of a server according to one or more examples of the present specification.

[0008] FIGURE 4 is a block diagram of a data loss prevention (DLP) server according to one or more examples of the present specification.

[0009] FIGURE 5 is a block diagram of a trusted execution environment according to one or more examples of the present specification.

[0010] FIGURE 6 is a block diagram of a verified social media content ecosystem according to one or more examples of the present specification.

[0011] FIGURE 7 is a flow chart of a method of a client device according to one or more examples of the present specification.

[0012] FIGURE 8 is a flow chart of a method of a DLP server according to one or more examples of the present specification.

[0013] FIGURE 9 is a flow chart of a method performed by a client device according to one or more examples of the present specification.

[0014] FIGURE 10 is a flow chart of a method performed by a DLP server according to one or more examples of the present specification.

Summary

[0015] In an example, there is disclosed a computing apparatus, comprising: a psychological state data interface to receive psychological state data; one or more logic elements, including at least one hardware element, comprising a verification engine to: receive a requested user action; receive a psychological state input via the psychological state data interface; analyze the psychological state input; and bar the requested user action at least partly responsive to the analyzing.

Embodiments of the Disclosure

[0016] The following disclosure provides many different embodiments, or examples, for implementing different features of the present disclosure. Specific examples of components and arrangements are described below to simplify the present disclosure. These are, of course, merely examples and are not intended to be limiting. Further, the present disclosure may repeat reference numerals and/or letters in the various examples. This repetition is for the purpose of simplicity and clarity and does not in itself dictate a relationship between the various embodiments and/or configurations discussed. Different embodiments may have different advantages, and no particular advantage is necessarily required of any embodiment.

[0017] As network users' personal lives increasingly crossover with their work lives, data loss prevention (DLP) is a serious concern for any enterprise. A user who is angry, intoxicated, over-stimulated, depressed, anxious, frightened, aroused, under duress, or whose judgment is otherwise compromised may make ill-advised posts, for example to a social media platform. In contemporary social media platforms, such as Facebook, Instagram, Tumblr, or Snapchat, users have the ability to instantly post their thoughts in a stream-of-consciousness fashion with very little forethought. Users can also post photographs, documents, and links very easily. While this ease of use can make for a rich, entertaining social media experience, it can be problematic for an enterprise. Other user actions may be similarly compromised by

an unfit psychological state. For example, an angry user who has just had an altercation with his boss or just received a termination notice (fired or laid off) may, in the heat of the moment, access files and send them to an adverse organization, something he may not do with a level head. In a classic spy example, a user with access to secret data could encounter a sensual enemy agent, and while engaged in unauthorized activities, with impaired judgment, compromise those secret data.

[0018] Even a social media user in full possession of his or her faculties may sometimes make ill-advised or poorly-thought-out posts. In some cases, careers have been harmed and reputations compromised by a person's post without proper regard for potential consequences. Job applicants have been passed over because of old photographs showing poor judgment. Celebrities have been caught in racist or bigoted rants. Companies have fired executives who have said or done things that can damage the reputation of the company by association.

[0019] Thus, it is advantageous to provide a system and method to ensure that social media messages are sent by authorized users, and sent only when those users are in a fit mental or psychological state to post. It is also advantageous to ensure that the users are posting appropriate content, excluding for example malicious or hateful content, proprietary corporate data, government classified data, personally-identifying information, insider trading, content or statements against policy, personal opinions put forth as official corporate policy or without appropriate disclaimers, or other inappropriate content.

[0020] The system may also detect, notify, and challenge the user in case some unauthorized or untrusted post appears on their social media account.

[0021] In an example, the user operates a client device with a trusted execution environment (TEE) and protected audio-video path (PAVP) or other trusted I/O. The user may also have a wearable device with appropriate biometric data for constructing a biometric profile, which may serve as a proxy for or means for inferring the user's psychological state.

[0022] When the user attempts to post to a social media site, he may need to first authenticate to the device. Once authenticated, he may also need to pass a biometric profile to ensure that he is mentally sound to post. If the user fails the initial biometric profile, a second-tier verification may be provided, such as a cognitive ability test that is relatively easy for a sober person, but relatively difficult for a person who is compromised by alcohol, drugs, excitation, nervousness, anger, or some other factor that affects the user's cognitive ability. This verification may be provided by a combination of a verification engine on the user's own machine, and a data loss prevention (DLP) engine on an intermediate DLP server, or any suitable combination of the two.

[0023] Advantageously, a completely secure and attested path may be provided all the way from the wearable device, to the client device, to the DLP server, to the social media server.

[0024] A system and method for verified social media content will now be described with more particular reference to the attached FIGURES. It should be noted that throughout the FIGURES, certain reference numerals may be repeated to indicate that a particular device or block is wholly or substantially consistent across the FIGURES. This is not, however, intended to imply any particular relationship between the various embodiments disclosed. In certain examples, a genus of elements may be referred to by a particular reference numeral (“widget 10”), while individual species or examples of the genus may be referred to by a hyphenated numeral (“first specific widget 10-1” and “second specific widget 10-2”).

[0025] FIGURE 1 is a network-level diagram of enterprise 100 according to one or more examples of the present specification. In this example, enterprise 100 may be configured to provide services or data to one or more customers 162, who may access information or services via external network 172. This may require secured enterprise 100 to at least partly expose certain services and networks to the outside world, thus creating a logical security aperture.

[0026] Within secured enterprise, one or more users 120 operate one or more client devices 110. Each device may include an appropriate operating system, such as Microsoft Windows, Linux, Android, Mac OSX, Apple iOS, Unix, or similar. Some of the foregoing may be more often used on one type of device than another. For example, desktop computers or engineering workstation may be more likely to use one of Microsoft Windows, Linux, Unix, or Mac OSX. Laptop computers, which are usually a portable off-the-shelf device with fewer customization options, may be more likely to run Microsoft Windows or Mac OSX. Mobile devices may be more likely to run Android or iOS. However, these examples are not intended to be limiting.

[0027] Client devices 110 may be communicatively coupled to one another and to other network resources via enterprise network 170. Enterprise network 170 may be any suitable network or combination of one or more networks operating on one or more suitable networking protocols, including for example, a local area network, an intranet, a virtual network, a wide area network, a wireless network, a cellular network, or the Internet (optionally accessed via a proxy, virtual machine, or other similar security mechanism) by way of nonlimiting example. Enterprise network 170 may also include one or more servers, firewalls, routers, switches, security appliances, antivirus servers, or other useful network devices, which in an example may be virtualized within workload cluster 142. In this illustration, enterprise network 170 is shown as a single network for simplicity, but in some embodiments, enterprise network 170 may include a large number of networks, such as one or more enterprise intranets connected to the internet. Enterprise network 170 may also provide access to an external network, such as the Internet, via external network 172. External network 172 may similarly be any suitable type of network.

[0028] A workload cluster 142 may be provided, for example as a virtual cluster running in a hypervisor on a plurality of rack-mounted blade servers, or as a cluster of physical servers. Workload

cluster 142 may provide one or more server functions, or one or more “microclouds” in one or more hypervisors. For example, a virtualization environment such as vCenter may provide the ability to define a plurality of “tenants,” with each tenant being functionally separate from each other tenant, and each tenant operating as a single-purpose microcloud. Each microcloud may serve a distinctive function, and may include a plurality of virtual machines (VMs) of many different flavors, including agentful and agentless VMs. In some embodiments, a DLP server 400 (see FIGURE 4) may be provisioned within workload cluster 142.

[0029] It should also be noted that some functionality of endpoint devices 110 may also be provided via workload cluster 142. For example, one microcloud may provide a remote desktop hypervisor such as a Citrix workspace, which allows users 120 operating endpoints 110 to remotely login to a remote enterprise desktop and access enterprise applications, workspaces, and data. In that case, endpoint 110 could be a “thin client” such as a Google Chromebook, running only a stripped-down operating system, and still provide user 120 useful access to enterprise resources.

[0030] One or more computing devices configured as a management console 140 may also operate on enterprise network 170. Management console 140 may provide a user interface for a security administrator 150 to define enterprise security policies, which management console 140 may enforce on enterprise network 170 and across client devices 110 and workload cluster 142. In an example, management console 140 may run a server-class operating system, such as Linux, Unix, or Windows Server. In other case, management console 140 may be provided as a web interface, on a desktop-class machine, or via a VM provisioned within workload cluster 142.

[0031] Secured enterprise 100 may communicate across enterprise boundary 104 with external network 172. Enterprise boundary 104 may represent a physical, logical, or other boundary. External network 172 may include, for example, websites, servers, network protocols, and other network-based services. In one example, a social media service 190 is available via external network 172.

[0032] In another example, secured enterprise 100 may simply be a family, with parents assuming the role of security administrator 150. The parents may wish to protect their children from undesirable content, such as pornography, adware, spyware, age-inappropriate content, advocacy for certain political, religious, or social movements, or forums for discussing illegal or dangerous activities, by way of non-limiting example. In this case, the parent may perform some or all of the duties of security administrator 150.

[0033] In any of the foregoing examples, enterprise user 120 and customer 162 may wish to interact with social media service 190. However, the enterprise to which these users belong may have concerns, as discussed above, with unrestricted access to social media service 190. Thus, users may be provided with a wearable device 130, which may be configured to provide biometric or other sensors. Data from these sensors may serve as a proxy for or a means to infer the user’s psychological state or

condition. Thus, a verification engine 234 (FIGURE 2) operating on client device 110, or a DLP engine 434 (FIGURE 4) operating on a service node in workload cluster 142, or any other suitable device, may monitor inputs from wearable devices 130, and may restrict access to social media service 190 if the user's state appears to be unsuitable.

[0034] FIGURE 2 is a block diagram of client device 200 according to one or more examples of the present specification. Client device 200 may be any suitable computing device. In various embodiments, a "computing device" may be or comprise, by way of non-limiting example, a computer, workstation, server, mainframe, virtual machine (whether emulated or on a "bare-metal" hypervisor), embedded computer, embedded controller, embedded sensor, personal digital assistant, laptop computer, cellular telephone, IP telephone, smart phone, tablet computer, convertible tablet computer, computing appliance, network appliance, receiver, wearable computer, handheld calculator, or any other electronic, microelectronic, or microelectromechanical device for processing and communicating data. Any computing device may be designated as a host on the network. Each computing device may refer to itself as a "local host," while any computing device external to it may be designated as a "remote host."

[0035] In certain embodiments, client devices 110 may all be examples of client devices 200.

[0036] Client device 200 includes a processor 210 connected to a memory 220, having stored therein executable instructions for providing an operating system 222 and at least software portions of a verification engine 224. Other components of client device 200 include a storage 250, network interface 260, and peripheral interface 240. This architecture is provided by way of example only, and is intended to be non-exclusive and non-limiting. Furthermore, the various parts disclosed are intended to be logical divisions only, and need not necessarily represent physically separate hardware and/or software components. Certain computing devices provide main memory 220 and storage 250, for example, in a single physical memory device, and in other cases, memory 220 and/or storage 250 are functionally distributed across many physical devices. In the case of virtual machines or hypervisors, all or part of a function may be provided in the form of software or firmware running over a virtualization layer to provide the disclosed logical function. In other examples, a device such as a network interface 260 may provide only the minimum hardware interfaces necessary to perform its logical operation, and may rely on a software driver to provide additional necessary logic. Thus, each logical block disclosed herein is broadly intended to include one or more logic elements configured and operable for providing the disclosed logical operation of that block. As used throughout this specification, "logic elements" may include hardware, external hardware (digital, analog, or mixed-signal), software, reciprocating software, services, drivers, interfaces, components, modules, algorithms, sensors, components, firmware, microcode, programmable logic, or objects that can coordinate to achieve a logical operation.

[0037] In an example, processor 210 is communicatively coupled to memory 220 via memory bus 270-3, which may be for example a direct memory access (DMA) bus by way of example, though other

memory architectures are possible, including ones in which memory 220 communicates with processor 210 via system bus 270-1 or some other bus. Processor 210 may be communicatively coupled to other devices via a system bus 270-1. As used throughout this specification, a “bus” includes any wired or wireless interconnection line, network, connection, bundle, single bus, multiple buses, crossbar network, single-stage network, multistage network or other conduction medium operable to carry data, signals, or power between parts of a computing device, or between computing devices. It should be noted that these uses are disclosed by way of non-limiting example only, and that some embodiments may omit one or more of the foregoing buses, while others may employ additional or different buses.

[0038] In various examples, a “processor” may include any combination of logic elements operable to execute instructions, whether loaded from memory, or implemented directly in hardware, including by way of non-limiting example a microprocessor, digital signal processor, field-programmable gate array, graphics processing unit, programmable logic array, application-specific integrated circuit, or virtual machine processor. In certain architectures, a multi-core processor may be provided, in which case processor 210 may be treated as only one core of a multi-core processor, or may be treated as the entire multi-core processor, as appropriate. In some embodiments, one or more co-processor may also be provided for specialized or support functions.

[0039] Processor 210 may be connected to memory 220 in a DMA configuration via DMA bus 270-3. To simplify this disclosure, memory 220 is disclosed as a single logical block, but in a physical embodiment may include one or more blocks of any suitable volatile or non-volatile memory technology or technologies, including for example DDR RAM, SRAM, DRAM, cache, L1 or L2 memory, on-chip memory, registers, flash, ROM, optical media, virtual memory regions, magnetic or tape memory, or similar. In certain embodiments, memory 220 may comprise a relatively low-latency volatile main memory, while storage 250 may comprise a relatively higher-latency non-volatile memory. However, memory 220 and storage 250 need not be physically separate devices, and in some examples may represent simply a logical separation of function. It should also be noted that although DMA is disclosed by way of non-limiting example, DMA is not the only protocol consistent with this specification, and that other memory architectures are available.

[0040] Storage 250 may be any species of memory 220, or may be a separate device. Storage 250 may include one or more non-transitory computer-readable mediums, including by way of non-limiting example, a hard drive, solid-state drive, external storage, redundant array of independent disks (RAID), network-attached storage, optical storage, tape drive, backup system, cloud storage, or any combination of the foregoing. Storage 250 may be, or may include therein, a database or databases or data stored in other configurations, and may include a stored copy of operational software such as operating system 222 and software portions of verification engine 224. Many other configurations are also possible, and are intended to be encompassed within the broad scope of this specification.

[0041] Network interface 260 may be provided to communicatively couple client device 200 to a wired or wireless network. A “network,” as used throughout this specification, may include any communicative platform operable to exchange data or information within or between computing devices, including by way of non-limiting example, an ad-hoc local network, an internet architecture providing computing devices with the ability to electronically interact, a plain old telephone system (POTS), which computing devices could use to perform transactions in which they may be assisted by human operators or in which they may manually key data into a telephone or other suitable electronic equipment, any packet data network (PDN) offering a communications interface or exchange between any two nodes in a system, or any local area network (LAN), metropolitan area network (MAN), wide area network (WAN), wireless local area network (WLAN), virtual private network (VPN), intranet, or any other appropriate architecture or system that facilitates communications in a network or telephonic environment.

[0042] Verification engine 224, in one example, is operable to carry out computer-implemented methods as described in this specification. Verification engine 224 may include one or more tangible non-transitory computer-readable mediums having stored thereon executable instructions operable to instruct a processor to provide a verification engine 224. As used throughout this specification, an “engine” includes any combination of one or more logic elements, of similar or dissimilar species, operable for and configured to perform one or more methods provided by the engine. Thus, verification engine 224 may comprise one or more logic elements configured to provide methods as disclosed in this specification. In some cases, verification engine 224 may include a special integrated circuit designed to carry out a method or a part thereof, and may also include software instructions operable to instruct a processor to perform the method. In some cases, verification engine 224 may run as a “daemon” process. A “daemon” may include any program or series of executable instructions, whether implemented in hardware, software, firmware, or any combination thereof that runs as a background process, a terminate-and-stay-resident program, a service, system extension, control panel, bootup procedure, BIOS subroutine, or any similar program that operates without direct user interaction. In certain embodiments, daemon processes may run with elevated privileges in a “driver space,” or in ring 0, 1, or 2 in a protection ring architecture. It should also be noted that verification engine 224 may also include other hardware and software, including configuration files, registry entries, and interactive or user-mode software by way of non-limiting example.

[0043] In one example, verification engine 224 includes executable instructions stored on a non-transitory medium operable to perform a method according to this specification. At an appropriate time, such as upon booting client device 200 or upon a command from operating system 222 or a user 120, processor 210 may retrieve a copy of the instructions from storage 250 and load it into memory 220.

Processor 210 may then iteratively execute the instructions of verification engine 224 to provide the desired method.

[0044] Verification engine 224 may be configured, in an embodiment, to carry out the method of FIGURE 7, or other suitable methods of this specification. In this example, verification engine 224 operates on client device 110, but all or part may also operate on wearable device 130, or on any other suitable device.

[0045] Peripheral interface 240 may be configured to interface with any auxiliary device that connects to client device 200 but that is not necessarily a part of the core architecture of client device 200. A peripheral may be operable to provide extended functionality to client device 200, and may or may not be wholly dependent on client device 200. In some cases, a peripheral may be a computing device in its own right. Peripherals may include input and output devices such as displays, terminals, printers, keyboards, mice, modems, data ports (e.g., serial, parallel, USB, Firewire, or similar), network controllers, optical media, external storage, sensors, transducers, actuators, controllers, data acquisition buses, cameras, microphones, speakers, or external storage by way of non-limiting example.

[0046] In one example, peripherals include display adapter 242, audio driver 244, and input/output (I/O) driver 246. Display adapter 242 may be configured to provide a human-readable visual output, such as a command-line interface (CLI) or graphical desktop such as Microsoft Windows, Apple OSX desktop, or a Unix/Linux X Window System-based desktop. Display adapter 242 may provide output in any suitable format, such as a coaxial output, composite video, component video, VGA, or digital outputs such as DVI or HDMI, by way of nonlimiting example. In some examples, display adapter 242 may include a hardware graphics card, which may have its own memory and its own graphics processing unit (GPU). Audio driver 244 may provide an interface for audible sounds, and may include in some examples a hardware sound card. Sound output may be provided in analog (such as a 3.5mm stereo jack), component (“RCA”) stereo, or in a digital audio format such as S/PDIF, AES3, AES47, HDMI, USB, Bluetooth or Wi-Fi audio, by way of non-limiting example.

[0047] FIGURE 3 is a block diagram of a server-class device 300 according to one or more examples of the present specification. Server 300 may be any suitable computing device, as described in connection with FIGURE 2. In general, the definitions and examples of FIGURE 2 may be considered as equally applicable to FIGURE 3, unless specifically stated otherwise. Server 300 is described herein separately to illustrate that in certain embodiments, logical operations according to this specification may be divided along a client-server model, wherein client device 200 provides certain localized tasks, while server 300 provides certain other centralized tasks. In contemporary practice, server 300 is more likely than client device 200 to be provided as a “headless” VM running on a computing cluster, or as a standalone appliance, though these configurations are not required.

[0048] Server 300 includes a processor 310 connected to a memory 320, having stored therein executable instructions for providing an operating system 322 and at least software portions of a server engine 324. Other components of server 300 include a storage 350, and network interface 360. As described in FIGURE 2, each logical block may be provided by one or more similar or dissimilar logic elements.

[0049] In an example, processor 310 is communicatively coupled to memory 320 via memory bus 370-3, which may be for example a direct memory access (DMA) bus. Processor 310 may be communicatively coupled to other devices via a system bus 370-1.

[0050] Processor 310 may be connected to memory 320 in a DMA configuration via DMA bus 370-3, or via any other suitable memory configuration. As discussed in FIGURE 2, memory 320 may include one or more logic elements of any suitable type.

[0051] Storage 350 may be any species of memory 320, or may be a separate device, as described in connection with storage 250 of FIGURE 2. Storage 350 may be, or may include therein, a database or databases or data stored in other configurations, and may include a stored copy of operational software such as operating system 322 and software portions of server engine 324.

[0052] Network interface 360 may be provided to communicatively couple server 140 to a wired or wireless network, and may include one or more logic elements as described in FIGURE 2.

[0053] Server engine 324 is an engine as described in FIGURE 2 and, in one example, includes one or more logic elements operable to carry out computer-implemented methods as described in this specification. Software portions of server engine 324 may run as a daemon process.

[0054] Server engine 324 may include one or more non-transitory computer-readable mediums having stored thereon executable instructions operable to instruct a processor to provide a security engine. At an appropriate time, such as upon booting server 140 or upon a command from operating system 322 or a user 120 or security administrator 150, processor 310 may retrieve a copy of server engine 324 (or software portions thereof) from storage 350 and load it into memory 320. Processor 310 may then iteratively execute the instructions of server engine 324 to provide the desired method.

[0055] Server engine 324 may be configured to provide a social media service, such as social media service 190. In some embodiments, server engine 324 may be explicitly configured to operate with end-to-end verification and encryption, in which case unverified inputs may be rejected.

[0056] FIGURE 4 is a block diagram of a server-class device 400 according to one or more examples of the present specification. Server 400 may be any suitable computing device, as described in connection with FIGURE 2. In general, the definitions and examples of FIGURE 2 may be considered as equally applicable to FIGURE 4, unless specifically stated otherwise. Server 400 is described herein separately to illustrate that in certain embodiments, logical operations according to this specification may be divided along a client-server model, wherein client device 200 provides certain localized tasks, while

server 400 provides certain other centralized tasks. In contemporary practice, server 400 is more likely than client device 200 to be provided as a “headless” VM running on a computing cluster, or as a standalone appliance, though these configurations are not required.

[0057] Server 400 includes a processor 410 connected to a memory 420, having stored therein executable instructions for providing an operating system 422 and at least software portions of a DLP engine 424. Other components of server 400 include a storage 450, and network interface 460. As described in FIGURE 2, each logical block may be provided by one or more similar or dissimilar logic elements.

[0058] In an example, processor 410 is communicatively coupled to memory 420 via memory bus 470-3, which may be for example a direct memory access (DMA) bus. Processor 410 may be communicatively coupled to other devices via a system bus 470-1.

[0059] Processor 410 may be connected to memory 420 in a DMA configuration via DMA bus 470-3, or via any other suitable memory configuration. As discussed in FIGURE 2, memory 420 may include one or more logic elements of any suitable type.

[0060] Storage 450 may be any species of memory 420, or may be a separate device, as described in connection with storage 250 of FIGURE 2. Storage 450 may be, or may include therein, a database or databases or data stored in other configurations, and may include a stored copy of operational software such as operating system 422 and software portions of DLP engine 424.

[0061] Network interface 460 may be provided to communicatively couple server 140 to a wired or wireless network, and may include one or more logic elements as described in FIGURE 2.

[0062] DLP engine 424 is an engine as described in FIGURE 2 and, in one example, includes one or more logic elements operable to carry out computer-implemented methods as described in this specification. Software portions of DLP engine 424 may run as a daemon process.

[0063] DLP engine 424 may include one or more non-transitory computer-readable mediums having stored thereon executable instructions operable to instruct a processor to provide a security engine. At an appropriate time, such as upon booting server 140 or upon a command from operating system 422 or a user 120 or security administrator 150, processor 410 may retrieve a copy of DLP engine 424 (or software portions thereof) from storage 450 and load it into memory 420. Processor 410 may then iteratively execute the instructions of DLP engine 424 to provide the desired method.

[0064] In some embodiments, DLP engine 424 may be provided separately on DLP server 400. However, it should be understood that some or all of the functions of DLP server 400 may just as easily be provided on client device 110.

[0065] FIGURE 5 is a block diagram of a trusted execution environment (TEE) 500 according to one or more examples of the present specification.

[0066] In the example of FIGURE 5, memory 220 is addressable by n -bits, ranging in address from 0 to $2^n - 1$. Within memory 220 is an OS 222, enclave 540, application stack 520, and application code 530.

[0067] In this example, enclave 540 is a specially-designated portion of memory 220 that cannot be entered into or exited from except via special instructions, such as Intel® SGX or similar. Enclave 540 is provided as an example of a secure environment which, in conjunction with a secure processing engine 510, forms a trusted execution environment (TEE) 500 on client device 200. A TEE 500 is a combination of hardware, software, and/or memory allocation that provides the ability to securely execute instructions without interference from outside processes, in a verifiable way. By way of example, TEE 500 may include memory enclave 540 or some other protected memory area, and a secure processing engine 510, which includes hardware, software, and instructions for accessing and operating on enclave 540. Non-limiting examples of solutions that either are or that can provide a TEE include Intel® SGX, ARM TrustZone, AMD Platform Security Processor, Kinibi, securiTEE, OP-TEE, TLK, T6, Open TEE, and SierraTEE, CSE, VT-x, MemCore, Canary Island, Docker, and Smack. Thus, it should be noted that in an example, secure processing engine 510 may be a user-mode application that operates via trusted execution framework 524 within enclave 540. TEE 500 may also conceptually include processor instructions that secure processing engine 510 and trusted execution framework 524 require to operate within enclave 540.

[0068] Secure processing engine 510 and trusted execution framework 524 may together form a trusted computing base (TCB), which is a set of programs or computational units that are trusted to be secure. Conceptually, it may be advantageous to keep TCB relatively small so that there are fewer attack vectors for malware objects 182 or for negligent software. Thus, for example, operating system 222 may be excluded from TCB, in addition to the regular application stack 520 and application code 530.

[0069] In certain systems, computing devices equipped with the Intel Software Guard Extension (SGX) or equivalent instructions may be capable of providing an enclave 540. It should be noted however, that many other examples of TEEs are available, and TEE 500 is provided only as one example thereof. Other secure environments may include, by way of nonlimiting example, a virtual machine, sandbox, testbed, test machine, or other similar device or method for providing a TEE 500.

[0070] In an example, enclave 540 provides a protected memory area that cannot be accessed or manipulated by ordinary computer instructions. Enclave 540 is described with particular reference to an Intel® SGX enclave by way of example, but it is intended that enclave 540 encompass any secure processing area with suitable properties, regardless of whether it is called an “enclave.”

[0071] One feature of an enclave is that once an enclave region 540 of memory 220 is defined, as illustrated, a program pointer cannot enter or exit enclave 540 without the use of special enclave instructions or directives, such as those provided by Intel® SGX architecture. For example, SGX processors

provide the ENCLU[EENTER], ENCLU[ERESUME], and ENCLU[EEXIT]. These are the only instructions that may legitimately enter into or exit from enclave 540.

[0072] Thus, once enclave 540 is defined in memory 220, a program executing within enclave 540 may be safely verified to not operate outside of its bounds. This security feature means that secure processing engine 510 is verifiably local to enclave 540. Thus, when an untrusted packet provides its content to be rendered with trusted execution framework 524 of enclave 540, the result of the rendering is verified as secure.

[0073] Enclave 540 may also digitally sign its output, which provides a verifiable means of ensuring that content has not been tampered with or modified since being rendered by secure processing engine 510. A digital signature provided by enclave 540 is unique to enclave 540 and is unique to the hardware of the device hosting enclave 540.

[0074] FIGURE 6 is a block diagram of a verified social media ecosystem according to one or more examples of the present specification. This ecosystem includes a client device 110, a wearable device 130, a DLP server 400, and one or more social media networks 190.

[0075] In this example, a user 120 operates a client device 110. Note that in accordance with the description provided in this specification, user 120 may be a corporate user, customer 162, or any other suitable user.

[0076] Client device 110 may be communicatively coupled to a wearable device 130. Client device 110 and wearable device 130 may together form the first line of defense against a user 120 making an inappropriate post to a social media site 190. Specifically, client device 110 includes, by way of example, an authenticator 610, trusted interface 620, and sensor manager 630.

[0077] Authenticator 610 may allow user 120 to authenticate by any suitable means, such as via a PIN, password, facial recognition, voice recognition, fingerprint, or any other suitable means. In an embodiment, the same biometric sensors of wearable device 130 may be used to provide initial user authentication. In other embodiments, different sensors may be provided, such as where dedicated biometric authentication sensors are used.

[0078] Trusted interface 620 may be the interface by which user 120 actually interoperates with a social media network. Trusted interface 620 may include a TEE, and also may include other security measures such as an Intel® protected audio-video path. This can be used to ensure that all peripherals 240, such as I/O devices, are protected. Memory 220 may also be protected via TEE 500.

[0079] Sensor manager 630 may be configured to securely communicatively couple to wearable device 130, and to engage in secured communications with wearable device 130. Measures such as trusted interface 620 and sensor manager 630 may help to ensure that client device 110 cannot be tampered with, such as to allow a user to post when not authorized.

[0080] As with client device 110, wearable device 130 may also include a TEE 500. Another important component of wearable device 130 is a sensor array 634. Sensor array 634 may include any suitable sensor to measure a user's ability, state of mind, or capacity to engage in an activity such as posting to a social media server. Nonlimiting examples of sensors in sensor array 634 include a blood alcohol content (BAC) sensor, blood pressure sensor, pupil dilation sensor, facial expression sensor, heart rate sensor, or perspiration sensor. These can all be used to help determine that a person is intoxicated, angry, nervous, or otherwise compromised to such an extent that he or she is not in full possession of faculties. Thus, it may be better for that user not to post to social network 190. Note that the biological profile may not, itself, directly implicate the user's ability to post. Rather, the biological profile may server as a proxy for, or a means to infer, a user's instantaneous psychological state. In a compromised psychological state, even if the user is mentally capable of composing a post and posting it, such a course may be ill-advised.

[0081] In an example, when a user 120 authenticates via authenticator 610, and then tries to operate trusted interface 620 to make a social media post, sensor manager 630 engages in a secured or attested communication with wearable device 130.

[0082] Attestation may be in the form of any suitable attestation, such as remote attestation, or "direct anonymous attestation" (DAA). In remote attestation, TEE 500 of wearable device 130 may generate a certificate of its hardware or software configuration. Wearable device 130 can present this certificate to client device 110 or DLP server 400 to prove that it has the required capability to securely measure biometric factors without tampering. This remote attestation may be combined with public-key encryption so that the information sent can only be read by the requesting device.

[0083] In certain embodiments, DAA may also be used to attest operations between wearable device 130 and client device 110, or more generally between any of the devices disclosed herein that perform attestation. In that case, the attesting device (here, wearable device 130, but in general, any of the devices disclosed herein that may perform attestation) may have a DAA certificate issued by a certificate authority, such as a public key infrastructure (PKI) certificate authority. The verifying device may be client device 110, or in general, any of the devices disclosed herein that may verify an attestation.

[0084] Each TEE 500 in the exchange includes an embedded RSA key pair called an Endorsement Key (EK), which the certificate authority is assumed to know. For attestation, TEE 500 of the attesting device (wearable device 130) generates a second RSA key pair called an Attestation Identity Key (AIK). It sends the public AIK, signed by EK, to the certificate authority, which checks its validity and issues a certificate for the AIK. The certificate authority may know the TEE's public EK *a priori*, or a device manufacturer may have provided an endorsement certificate. TEE 500 of wearable device 130 is now able to authenticate itself with respect to the certificate. Through a zero-knowledge proof engine, TEE 500 of

the verifying device (client device 110) may verify the credential without attempting to violate the privacy of wearable device 130.

[0085] Upon a request from client device 110, wearable device 130 measures one or more suitable biometric parameters, and exchanges an encrypted packet with sensor manager 630. Sensor manager 630 then decrypts the packet, examines the data, and determines whether the biometric data are suitable for a post. Note that in some embodiments, more than one biometric datum may be used, in which case a biometric profile of user 120 may be built. The biometric profile may be a simple scalar score, or may be a multi-dimensional vector score with numerous factors. Verification engine 226 may compare this profile to either a scalar threshold, or to a multi-dimensional threshold vector, wherein each vector, or a minimum number of vectors, must exceed a threshold before a post is allowed.

[0086] In some cases, if user 120 fails the biometric profile, he may still be given an opportunity to post if he can pass a second-tier verification protocol, such as a suitable cognitive exercise. For example, the user may be asked to calculate a value such as his age multiplied by his dog's age. This exercise will be fairly simple for a sober person, but may be much more difficult for a person who is angry, intoxicated, or otherwise compromised. Second-tier content may also be based on personal knowledge not broadly known, thus providing an additional authentication factor. Other nonlimiting examples of verification exercises include forming a "word" from the first five letters of the user's first name and the first five letters of his mother's maiden name, sorting several cousins' names by order of age, finding a minimum number of objects in a "hidden picture" drawing, using a stylus or finger to navigate a maze or trace a pattern of straight lines, or solving a numerical or alphanumeric "captcha."

[0087] In some embodiments, verification engine 226 may be a standalone verification process. However, in other embodiments, it may be coupled with a DLP server 400, and/or a secured social media network 190.

[0088] In the case where verification engine 226 is not a standalone measure, verification engine 226 may sign the attempted social media content within TEE 500. Client device 110 may then provide the proposed content to DLP server 400.

[0089] DLP server 400 may receive the signed, encrypted post, and may in some cases perform an attestation with client device 110 to ensure that the content is genuine. DLP engine 424 may then decrypt the encrypted post and perform a natural-language scan of it, checking for content that may be against policy. DLP engine 424 may also scan multimedia files such as pictures, videos, or audio, using image or voice recognition to detect inappropriate content within those. Network administrator 150 may set suitable thresholds for how strictly which policies will be enforced. For example, there may be zero or near-zero tolerance for leakage of proprietary corporate data, while the criteria may be less stringent for something less important, such as appropriate fraternization at a corporate party. Other examples of problematic content may include personally-identifying information, insider trading, hate, or abuse.

[0090] DLP engine 424 may also, in certain embodiments, have responsibility for making decisions about the user's mental state. In those cases, client device 110 may not have logic for determining the user's state, but may rather simply provide a signed user state report, comprising raw or minimally-processed sensor data. DLP engine 424 may then determine whether the user is in condition to post, and may request a second-tier verification as appropriate. All transactions between DLP engine 424 and client device 110 may be securely encrypted and attested. In general, it should be understood that DLP engine 424 provides a verification function, but can be provided on DLP server 400, on client device 110, or on any other suitable device.

[0091] If DLP engine 424 determines that the post is appropriate, DLP engine 424 may sign the post (as necessary) and forward it to the target social media network 190.

[0092] In some embodiments, social media network 190 may be a secured social media network, in which case it may only accept signed content submissions, or it may favor or otherwise perform special classification for signed content. In some embodiments, social media network 190 may be equipped with servers that have TEE capabilities so that it can perform remote attestation with DLP engine 424 or with client device 110.

[0093] Note that while popular networks with a large and diverse user base are less likely to strictly enforce a secure computing model, there are examples of networks where secure computing can be advantageous. For example, a government agency, intelligence agency, or defense agency may wish to provide its own internal social network to further its enterprise purposes. In that case, it may be advantageous to require secure connections. And even large networks with diverse user bases may provide secure connection as a user option, so that users can help to secure their accounts from compromise, either from a third party, or from their own inadvertent errors.

[0094] Advantageously, at a top level, the ecosystem of FIGURE 6 may provide a completely secure, end-to-end encrypted and attested means for interacting with a social network, with every connection from wearable device 130 to social media network 190 secured, attested, and/or encrypted. In that case, an attestation chain may include wearable device 130 → client device 110 → DLP server 400 → social media server 190.

[0095] In appropriate circumstances, attestation may take other forms than ensuring that data are not compromised. For example, attestation may be used between client device 110 and wearable device 130 to ensure that wearable device 130 has the minimum hardware and software capabilities to provide the desired biometric input.

[0096] FIGURE 7 is a flow chart of a method 700 performed by a client device 110 according to one or more examples of the present specification.

[0097] In block 710, a user 120 attempts to take a requested user action that is subject to verification, such as posting to a social media network, accessing sensitive data, or any other action that

may be subject to control of a verification engine 226 or DLP engine 424. Any such action may be referred to herein as a “controlled action.” This action is referred to as a “post” by way of nonlimiting example.

[0098] In block 730, client device 110 may receive biometric data from wearable device 130. Additional details of such an exchange in an example are disclosed in paragraph [0084] above. These data may be received via a secured communication channel, such as via a TEE 500 or by other suitable means. The data may be encrypted, and attestation between client device 110 and wearable device 130 may be performed as appropriate, for example as discussed in paragraphs [0081] – [0083] above.

[0099] In block 730, verification engine 226 determines whether a biometric profile is above a threshold. For example, this may include ensuring that the user’s BAC does not exceed a specified value, that the user’s pulse or perspiration are not above a specified value, or any other suitable input for inferring user 120’s state of mind. As discussed in paragraph [0084] above, the biometric profile may be a single scalar or normalized composite value, or it may be a multi-dimensional vector value. Thus, determining whether the biometric profile is above a value may comprise either comparing the single scalar value to a threshold, or comparing a plurality of values to a plurality of thresholds. The result of this comparing may be a binary indication that the user’s profile has either “passed” or “failed.”

[0100] If the user passes, then in block 798, the post has passed verification. In an embodiment, once verification engine 226 has passed the post, verification engine 226 forwards the post, which may include forwarding the post to social media service 190 in an embodiment where no separate DLP engine 424 is provided, or may include forwarding the post, along with a signed user state report, to separate DLP engine 424.

[0101] If the user fails the biometric profile check, he may be provided with a second opportunity to take his action. For example, the user may receive a second-tier verification request, which in an embodiment is a cognitive activity that will be more difficult to perform while compromised. This may include any of the example activities disclosed in [0085] above, or any other suitable activity.

[0102] FIGURE 8 is a flow chart of a method 800 performed by DLP engine 424 according to one or more examples of the present specification.

[0103] In block 810, DLP engine 424 receives an attempted post or other requested user action from client device 110. Note that this may be received via a network interface and TEE. For example, this may include a signed user state report as in [0089] above.

[0104] In block 820, DLP engine 424 performs an attestation with client 110 to ensure that authenticity of the attempted post. Attestation is discussed in additional detail in paragraphs [0081] – [0083] above.

[0105] In decision block 830, if the attestation fails, then in block 898, the post is rejected. However, if the attestation is successful, in block 840, DLP engine 424 performs a DLP scan on the attempted post. “DLP” in the context of the specification is intended to be construed very broadly to

encompass any factor that may make the post inappropriate. Examples of checks that may be performed in a DLP scan are discussed in paragraph [0088] above.

[0106] In block 850, if the post fails DLP inspection, then in block 898, the post is rejected. As discussed above, a post may be rejected, by way of nonlimiting example, for malicious or hateful content, proprietary corporate data, government classified data, personally-identifying information, insider trading, content or statements against policy, personal opinions put forth as official corporate policy or without appropriate disclaimers, or other inappropriate content.

[0107] If the post passes DLP inspection, then in block 896, DLP engine 424 submits the post to a social media network 190. Note that in some cases, the post is signed with the TEE so that end-to-end encryption and verification can be provided, from wearable device 130 to social media network 190. As appropriate, attestations may be performed as discussed in additional detail in paragraphs [0081] – [0083] above.

[0108] Note that the methods of FIGURES 7 and FIGURE 8 are disclosed as two separate methods, one performed by client device and one performed by DLP server 400. But it should be understood that this division is provided by way of nonlimiting example only. In appropriate circumstances, any of the operations may be suitably combined. For example, DLP server 400 may instead simply be a DLP engine running on client device 110, with no centralized server. In other embodiments, client device 110 may only collect biometric inputs and provide a TEE and PAVP connection to DLP engine 424, in which case all decisions (e.g., blocks 730 forward in FIGURE 7) may be made on DLP server 400.

[0109] FIGURES 9 and 10 are flow charts of methods performed by client device 110 and DLP server 400 in such an example, where client device 110 performs only minimal processing.

[0110] Method 900 of FIGURE 9 is performed by client device 110.

[0111] In block 910, a user attempts to take a controller user action that is subject to verification, (see, e.g., paragraph [0096] above). This action is referred to as a “post” by way of nonlimiting example.

[0112] In block 920, client device 110 may receive biometric data from wearable device 130. Additional details of such an exchange in an example are disclosed in paragraph [0084] above. These data may be received via a secured communication channel, such as via a TEE 500 or by other suitable means. The data may be encrypted, and attestation between client device 110 and wearable device 130 may be performed as appropriate, for example as discussed in paragraphs [0081] – [0083] above.

[0113] In block 930, client device 110 sends the attempted post (or other data, as appropriate to the embodiment), along with a signed user state report to DLP server 400. Additional details of constructing a signed user state report are discussed in paragraph [0089] above. Note that in this embodiment, verification engine 226 may have performed no or minimal processing on the signed user state report.

[0114] In the absence of further communication from DLP server 400, method 900 is done at block 999.

[0115] However, in some cases, verification engine 226 may receive from DLP server 400 a second-tier verification request. This may indicate that the user's biometric profile did not pass scrutiny by DLP server 400. Examples of second-tier verification requests are provided in paragraph [0085] above.

[0116] In block 950, verification engine 226 presents the second-tier verification challenge to user 120, for example via trusted interface 620. The user of trusted interface 620 can help to ensure that there has been no tampering, such as the user preparing macros of correct responses to known tests. The user provides an appropriate input, and in some embodiments, verification engine 226 may score the result. In another embodiment, verification engine 226 may simply send the user's signed and attested input to DLP server 400 for scoring.

[0117] In block 999, method 900 is done.

[0118] FIGURE 10 is a flow chart of method 1000 performed by DLP engine 424 of DLP server 400, in conjunction with client device 110 performing method 900 of FIGURE 9.

[0119] In block 1010, DLP engine 424 receives from client device 110 a signed user state report, for example the one that client device 110 sent in block 930 of FIGURE 9.

[0120] In block 1020, DLP engine 424 may perform an attestation with client device 110. Attestation is described in more detail in paragraphs [0081] – [0083] above.

[0121] In decision block 1030, DLP engine 424 determines whether the attestation was successful. If not, then in block 1098, DLP engine 424 rejects the post.

[0122] If the attestation is successful, then in decision block 1040, DLP engine 424 determines whether the user's biometric profile is above a threshold. For example, this may include ensuring that the user's BAC does not exceed a specified value, that the user's pulse or perspiration are not above a specified value, or any other suitable input for inferring user 120's state of mind. As discussed in paragraph [0084] above, the biometric profile may be a single scalar or normalized composite value, or it may be a multi-dimensional vector value. Thus, determining whether the biometric profile is above a value may comprise either comparing the single scalar value to a threshold, or comparing a plurality of values to a plurality of thresholds. The result of this comparing may be a binary indication that the user's profile has either "passed" or "failed."

[0123] If the user fails the biometric profile check, then in block 1050, DLP engine 424 may request a second-tier verification from client device 110. Examples of second-tier verification exercises are provided in paragraph [0085] above. In response, DLP engine 424 may either receive raw user input, or it may receive a scored second-tier verification report from client device 110.

[0124] In decision block 1060, if the user fails the second-tier verification, then in block 1098, DLP engine 424 rejects the post or other attempted action.

[0125] If the user either passes the biometric profile check in block 1040, or passes the second tier verification in block 1060, then in block 1070, DLP engine 424 performs a DLP scan on the attempted post or other action. Examples of DLP scans are discussed in paragraph [0088] above.

[0126] In decision block 1080, DLP engine 424 determines whether the post has passed the DLP scan. If not, then in block 1098, DLP engine 424 rejects the post.

[0127] In block 1099, if the post passes the DLP scan, then DLP engine 424 submits the post to a social media network 190. Note that in some cases, the post is signed with the TEE so that end-to-end encryption and verification can be provided, from wearable device 130 to social media network 190. As appropriate, attestations may be performed as discussed in additional detail in paragraphs [0081] – [0083] above.

[0128] Note that in combination, FIGURES 7 and 8 and FIGURES 9 and 10 respectively disclose two examples of dividing biometric verification from DLP analysis. In the example of FIGURES 7 and 8, biometric verification is performed on client device 110, while DLP scanning is performed on DLP server 400 or alternatively on client device 110. In the embodiment of FIGURES 9 and 10, client device 110 provides only unprocessed or minimally processed inputs to DLP server 400. These two examples should be understood to be nonlimiting examples. In a general sense, any embodiment may divide responsibilities between DLP server 400 and client device 110 as the demands of the particular embodiment demand. DLP server 400 could also be provided on, or in conjunction with, a social media server 190, or in any other appropriate configuration.

[0129] The foregoing outlines features of several embodiments so that those skilled in the art may better understand various aspects of the present disclosure. Those skilled in the art should appreciate that they may readily use the present disclosure as a basis for designing or modifying other processes and structures for carrying out the same purposes and/or achieving the same advantages of the embodiments introduced herein. Those skilled in the art should also realize that such equivalent constructions do not depart from the spirit and scope of the present disclosure, and that they may make various changes, substitutions, and alterations herein without departing from the spirit and scope of the present disclosure.

[0130] All or part of any hardware element disclosed herein may readily be provided in a system-on-a-chip (SoC), including central processing unit (CPU) package. An SoC represents an integrated circuit (IC) that integrates components of a computer or other electronic system into a single chip. Thus, for example, client devices 110 or server devices 300 may be provided, in whole or in part, in an SoC. The SoC may contain digital, analog, mixed-signal, and radio frequency functions, all of which may be provided on a single chip substrate. Other embodiments may include a multi-chip-module (MCM), with a plurality of chips located within a single electronic package and configured to interact closely with each other through the electronic package. In various other embodiments, the computing functionalities disclosed

herein may be implemented in one or more silicon cores in Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs), and other semiconductor chips.

[0131] Note also that in certain embodiment, some of the components may be omitted or consolidated. In a general sense, the arrangements depicted in the figures may be more logical in their representations, whereas a physical architecture may include various permutations, combinations, and/or hybrids of these elements. It is imperative to note that countless possible design configurations can be used to achieve the operational objectives outlined herein. Accordingly, the associated infrastructure has a myriad of substitute arrangements, design choices, device possibilities, hardware configurations, software implementations, and equipment options.

[0132] In a general sense, any suitably-configured processor, such as processor 210, can execute any type of instructions associated with the data to achieve the operations detailed herein. Any processor disclosed herein could transform an element or an article (for example, data) from one state or thing to another state or thing. In another example, some activities outlined herein may be implemented with fixed logic or programmable logic (for example, software and/or computer instructions executed by a processor) and the elements identified herein could be some type of a programmable processor, programmable digital logic (for example, a field programmable gate array (FPGA), an erasable programmable read only memory (EPROM), an electrically erasable programmable read only memory (EEPROM)), an ASIC that includes digital logic, software, code, electronic instructions, flash memory, optical disks, CD-ROMs, DVD ROMs, magnetic or optical cards, other types of machine-readable mediums suitable for storing electronic instructions, or any suitable combination thereof.

[0133] In operation, a storage such as storage 250 may store information in any suitable type of tangible, non-transitory storage medium (for example, random access memory (RAM), read only memory (ROM), field programmable gate array (FPGA), erasable programmable read only memory (EPROM), electrically erasable programmable ROM (EEPROM), etc.), software, hardware (for example, processor instructions or microcode), or in any other suitable component, device, element, or object where appropriate and based on particular needs. Furthermore, the information being tracked, sent, received, or stored in a processor could be provided in any database, register, table, cache, queue, control list, or storage structure, based on particular needs and implementations, all of which could be referenced in any suitable timeframe. Any of the memory or storage elements disclosed herein, such as memory 220 and storage 250, should be construed as being encompassed within the broad terms 'memory' and 'storage,' as appropriate. A non-transitory storage medium herein is expressly intended to include any non-transitory special-purpose or programmable hardware configured to provide the disclosed operations, or to cause a processor such as processor 210 to perform the disclosed operations.

[0134] Computer program logic implementing all or part of the functionality described herein is embodied in various forms, including, but in no way limited to, a source code form, a computer

executable form, machine instructions or microcode, programmable hardware, and various intermediate forms (for example, forms generated by an assembler, compiler, linker, or locator). In an example, source code includes a series of computer program instructions implemented in various programming languages, such as an object code, an assembly language, or a high-level language such as OpenCL, FORTRAN, C, C++, JAVA, or HTML for use with various operating systems or operating environments, or in hardware description languages such as Spice, Verilog, and VHDL. The source code may define and use various data structures and communication messages. The source code may be in a computer executable form (e.g., via an interpreter), or the source code may be converted (e.g., via a translator, assembler, or compiler) into a computer executable form, or converted to an intermediate form such as byte code. Where appropriate, any of the foregoing may be used to build or describe appropriate discrete or integrated circuits, whether sequential, combinatorial, state machines, or otherwise.

[0135] In one example embodiment, any number of electrical circuits of the FIGURES may be implemented on a board of an associated electronic device. The board can be a general circuit board that can hold various components of the internal electronic system of the electronic device and, further, provide connectors for other peripherals. More specifically, the board can provide the electrical connections by which the other components of the system can communicate electrically. Any suitable processor and memory can be suitably coupled to the board based on particular configuration needs, processing demands, and computing designs. Other components such as external storage, additional sensors, controllers for audio/video display, and peripheral devices may be attached to the board as plug-in cards, via cables, or integrated into the board itself. In another example, the electrical circuits of the FIGURES may be implemented as stand-alone modules (e.g., a device with associated components and circuitry configured to perform a specific application or function) or implemented as plug-in modules into application specific hardware of electronic devices.

[0136] Note that with the numerous examples provided herein, interaction may be described in terms of two, three, four, or more electrical components. However, this has been done for purposes of clarity and example only. It should be appreciated that the system can be consolidated or reconfigured in any suitable manner. Along similar design alternatives, any of the illustrated components, modules, and elements of the FIGURES may be combined in various possible configurations, all of which are within the broad scope of this specification. In certain cases, it may be easier to describe one or more of the functionalities of a given set of flows by only referencing a limited number of electrical elements. It should be appreciated that the electrical circuits of the FIGURES and its teachings are readily scalable and can accommodate a large number of components, as well as more complicated/sophisticated arrangements and configurations. Accordingly, the examples provided should not limit the scope or inhibit the broad teachings of the electrical circuits as potentially applied to a myriad of other architectures.

[0137] Numerous other changes, substitutions, variations, alterations, and modifications may be ascertained to one skilled in the art and it is intended that the present disclosure encompass all such changes, substitutions, variations, alterations, and modifications as falling within the scope of the appended claims. In order to assist the United States Patent and Trademark Office (USPTO) and, additionally, any readers of any patent issued on this application in interpreting the claims appended hereto, Applicant wishes to note that the Applicant: (a) does not intend any of the appended claims to invoke paragraph six (6) of 35 U.S.C. section 112 (pre-AIA) or paragraph (f) of the same section (post-AIA), as it exists on the date of the filing hereof unless the words “means for” or “steps for” are specifically used in the particular claims; and (b) does not intend, by any statement in the specification, to limit this disclosure in any way that is not otherwise expressly reflected in the appended claims.

Example Implementations

[0138] There is disclosed in one example, a computing apparatus, comprising: a psychological state data interface to receive psychological state data; one or more logic elements comprising a verification engine to: receive a requested user action; receive a psychological state input via the psychological state data interface; analyze the psychological state input; and bar the requested user action at least partly responsive to the analyzing.

[0139] There is further disclosed an example, wherein the requested user action is an attempt to interact with a social media network.

[0140] There is further disclosed an example, wherein analyzing the psychological state input comprises determining that the user intoxicated or psychologically compromised.

[0141] There is further disclosed an example, wherein the verification engine comprises a trusted execution environment (TEE).

[0142] There is further disclosed an example, wherein the verification engine is further to perform attestation on the psychological state input via the TEE.

[0143] There is further disclosed an example, wherein the verification engine is further to attest a capability of a device communicatively coupled via the psychological state data interface to perform a psychological state measurement.

[0144] There is further disclosed an example, wherein the verification engine is further to provide the requested user action to a DLP engine.

[0145] There is further disclosed an example, wherein the computing apparatus further comprises second one or more logic elements comprising the DLP engine.

[0146] There is further disclosed an example, wherein the verification engine is further to: provide a second-tier verification; and permit the requested user action at least partly responsive to the second-tier verification.

[0147] There is further disclosed an example, wherein the second-tier verification is a cognitive ability test.

[0148] There is further disclosed an example, wherein the cognitive ability test is designed to be more difficult for a person in a compromised psychological state than for a person not in a compromised psychological state.

[0149] There is further disclosed an example, wherein the cognitive ability test is to include at least partly a datum known to the user but not publicly known.

[0150] There is further disclosed in an example, one or more tangible, non-transitory computer-readable storage mediums having stored thereon executable instructions to instruct a processor to: communicatively couple to a psychological state data interface to receive psychological state data; receive a requested user action; receive a psychological state input via the psychological state data interface; analyze the psychological state input; and bar the requested user action at least partly responsive to the analyzing.

[0151] There is further disclosed an example, wherein the requested user action is an attempt to interact with a social media network.

[0152] There is further disclosed an example, wherein analyzing the psychological state input comprises determining that the user intoxicated or psychologically compromised.

[0153] There is further disclosed an example, wherein the instructions are further to provision a trusted execution environment (TEE).

[0154] There is further disclosed an example, wherein the verification engine is further to perform attestation on the psychological state input via the TEE.

[0155] There is further disclosed an example, wherein the verification engine is further to attest a capability of a device communicatively coupled via the psychological state data interface to perform a psychological state measurement.

[0156] There is further disclosed an example, wherein the instructions are further to provide the requested user action to a DLP engine.

[0157] There is further disclosed an example, wherein the instructions are further to: provide a second-tier verification; and permit the requested user action at least partly responsive to the second-tier verification, wherein the second-tier user verification is a cognitive ability test.

[0158] There is further disclosed an example, wherein the cognitive ability test is designed to be more difficult for a person in a compromised psychological state than for a person not in a compromised psychological state.

[0159] There is further disclosed an example, wherein the cognitive ability test is to include at least partly a datum known to the user but not publicly known.

[0160] There is further disclosed in an example, a computing apparatus comprising: one or more logic elements comprising a data loss prevention (DLP) engine to: receive a requested user action; receive a psychological state input for the requested user action via a first secured communication channel; determine that the user is in a suitable psychological state to perform the requested user action; and export the requested user action to a third-party device via a second secured communication channel.

[0161] There is further disclosed an example, wherein first secured communication channel and second secured communication channel are attested channels.

[0162] There is further disclosed in an example, a social media server, comprising: a network interface; first one or more logic elements comprising a trusted execution environment; and second one or more logic elements comprising a verification engine to: receive a trusted computing post candidate via the network interface, the post candidate being encrypted; perform an attestation via the network interface and the TEE to a data loss prevention (DLP) engine, the DLP engine to verify that a user originating the post candidate is not psychologically compromised; and permit the post only if the attestation succeeds.

[0163] There is further disclosed an example of one or more tangible, non-transitory computer-readable storage mediums having stored thereon executable instructions for instructing one or more processors for providing a verification engine operable for performing any or all of the operations of the preceding examples.

[0164] There is further disclosed an example of a method of providing a verification engine comprising performing any or all of the operations of the preceding examples.

[0165] There is further disclosed an example of an apparatus comprising means for performing the method.

[0166] There is further disclosed an example wherein the means comprise a processor and a memory.

[0167] There is further disclosed an example wherein the means comprise one or more tangible, non-transitory computer-readable storage mediums.

[0168] There is further disclosed an example wherein the apparatus is a computing device.

Claims:

1. A computing apparatus, comprising:

a psychological state data interface to receive psychological state data;

one or more logic elements, including at least one hardware element, comprising a verification engine to:

receive a requested user action;

receive a psychological state input via the psychological state data interface;

analyze the psychological state input; and

bar the requested user action at least partly responsive to the analyzing.
2. The computing apparatus of claim 1, wherein the requested user action is an attempt to interact with a social media network.
3. The computing apparatus of claim 1, wherein analyzing the psychological state input comprises determining that the user intoxicated or psychologically compromised.
4. The computing apparatus of claim 1, wherein the verification engine comprises a trusted execution environment (TEE).
5. The computing apparatus of claim 4, wherein the verification engine is further to perform attestation on the psychological state input via the TEE.
6. The computing apparatus of claim 4, wherein the verification engine is further to attest a capability of a device communicatively coupled via the psychological state data interface to perform a psychological state measurement.
7. The computing apparatus of claim 1, wherein the verification engine is further to provide the requested user action to a DLP engine.
8. The computing apparatus of claim 7, wherein the computing apparatus further comprises second one or more logic elements, including at least one hardware element, comprising the DLP engine.
9. The computing apparatus of any of claims 1 – 8, wherein the verification engine is further to:

provide a second-tier verification; and

permit the requested user action at least partly responsive to the second-tier verification.

10. The computing apparatus of claim 9, wherein the second-tier verification is a cognitive ability test.

11. The computing apparatus of claim 10, wherein the cognitive ability test is designed to be more difficult for a person in a compromised psychological state than for a person not in a compromised psychological state.

12. The computing apparatus of claim 11, wherein the cognitive ability test is to include at least partly a datum known to the user but not publicly known.

13. One or more tangible, non-transitory computer-readable storage mediums having stored thereon executable instructions to instruct a processor to:

communicatively couple to a psychological state data interface to receive psychological state data;

receive a requested user action;

receive a psychological state input via the psychological state data interface;

analyze the psychological state input; and

bar the requested user action at least partly responsive to the analyzing.

14. The one or more tangible, non-transitory computer-readable mediums of claim 13, wherein the requested user action is an attempt to interact with a social media network.

15. The one or more tangible, non-transitory computer-readable mediums of claim 13, wherein analyzing the psychological state input comprises determining that the user intoxicated or psychologically compromised.

16. The one or more tangible, non-transitory computer-readable mediums of claim 13, wherein the instructions are further to provision a trusted execution environment (TEE).

17. The one or more tangible, non-transitory computer-readable mediums of claim 16, wherein the verification engine is further to perform attestation on the psychological state input via the TEE.

18. The one or more tangible, non-transitory computer-readable mediums of claim 17, wherein the verification engine is further to attest a capability of a device communicatively coupled via the psychological state data interface to perform a psychological state measurement.
19. The one or more tangible, non-transitory computer-readable mediums of claim 13, wherein the instructions are further to provide the requested user action to a DLP engine.
20. The one or more tangible, non-transitory computer-readable mediums of any of claims 13 – 19, wherein the instructions are further to:
- provide a second-tier verification; and
 - permit the requested user action at least partly responsive to the second-tier verification, wherein the second-tier user verification is a cognitive ability test.
21. The one or more tangible, non-transitory computer-readable mediums of claim 20, wherein the cognitive ability test is designed to be more difficult for a person in a compromised psychological state than for a person not in a compromised psychological state.
22. The one or more tangible, non-transitory computer-readable mediums of claim 21, wherein the cognitive ability test is to include at least partly a datum known to the user but not publicly known.
23. A computing apparatus comprising:
- one or more logic elements, including at least one hardware element, comprising a data loss prevention (DLP) engine to:
 - receive a requested user action;
 - receive a psychological state input for the requested user action via a first secured communication channel;
 - determine that the user is in a suitable psychological state to perform the requested user action; and
 - export the requested user action to a third-party device via a second secured communication channel.
24. The computing apparatus of claim 13, wherein first secured communication channel and second secured communication channel are attested channels.

25. A social media server, comprising:

a network interface;

first one or more logic elements, including at least one hardware element, comprising a trusted execution environment; and

second one or more logic elements, including at least one hardware element, comprising a verification engine to:

receive a trusted computing post candidate via the network interface, the post candidate being encrypted;

perform an attestation via the network interface and the TEE to a data loss prevention (DLP) engine, the DLP engine to verify that a user originating the post candidate is not psychologically compromised; and

decrypt and permit the post only if the attestation succeeds.

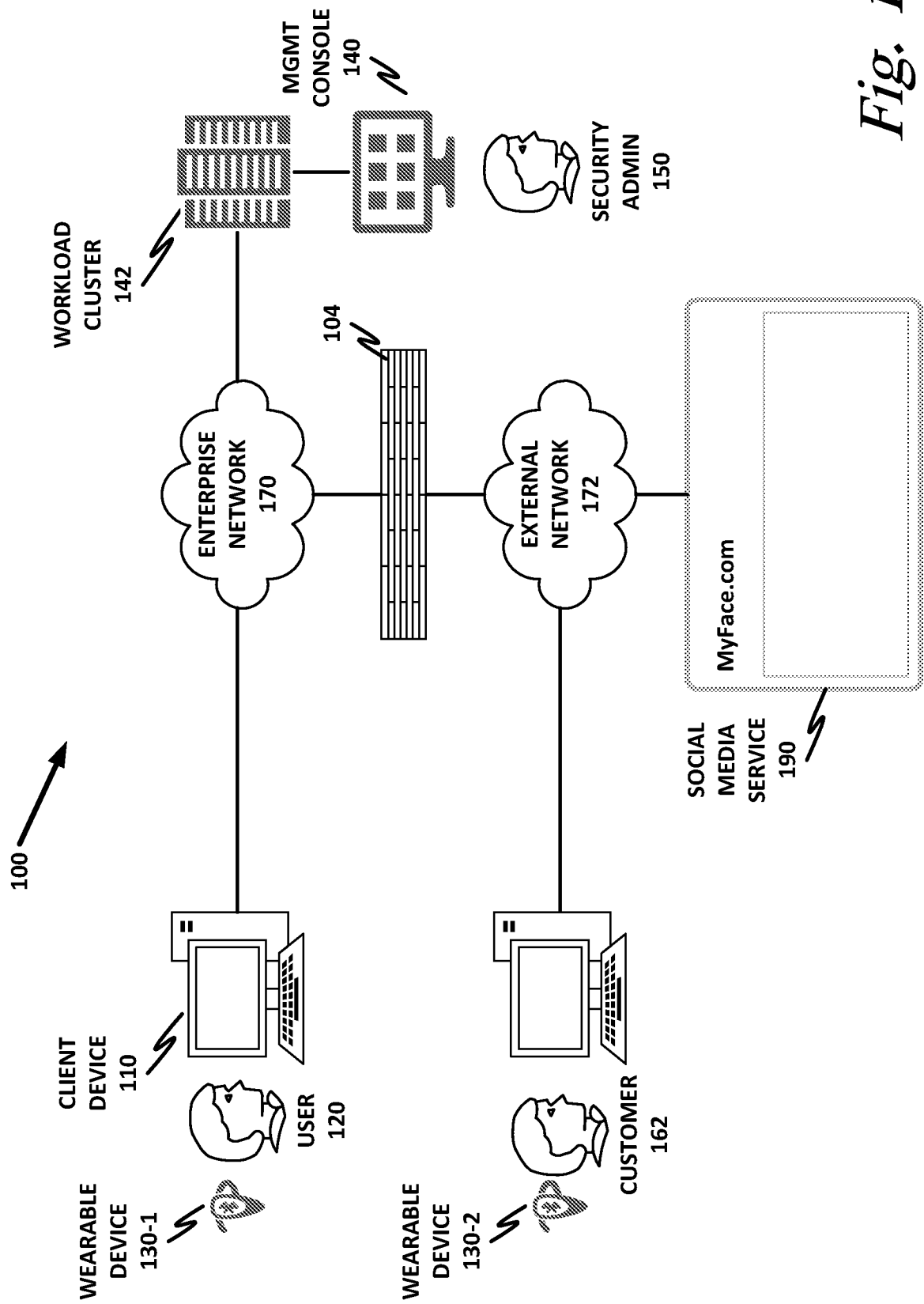


Fig. 1

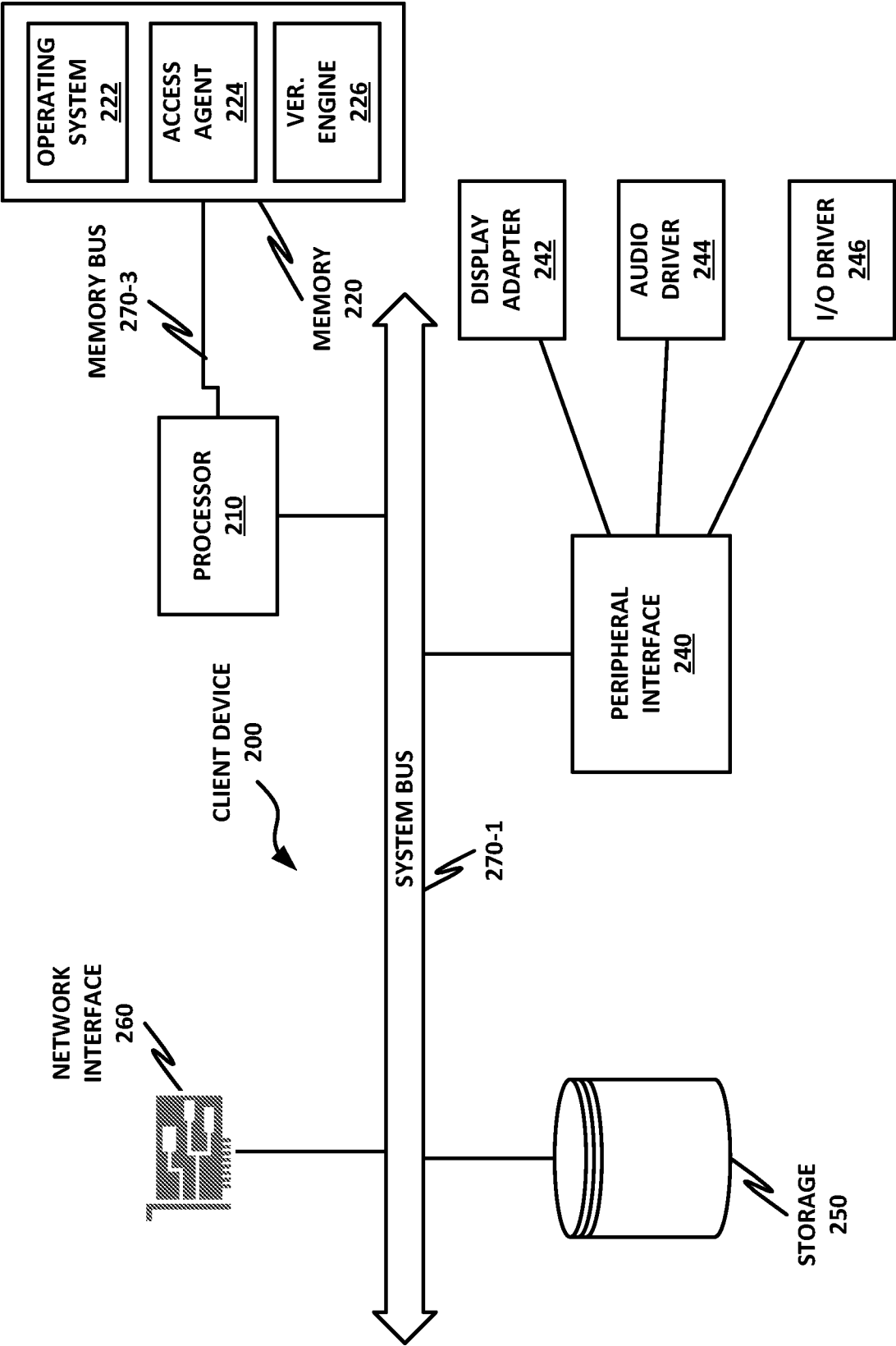


Fig. 2

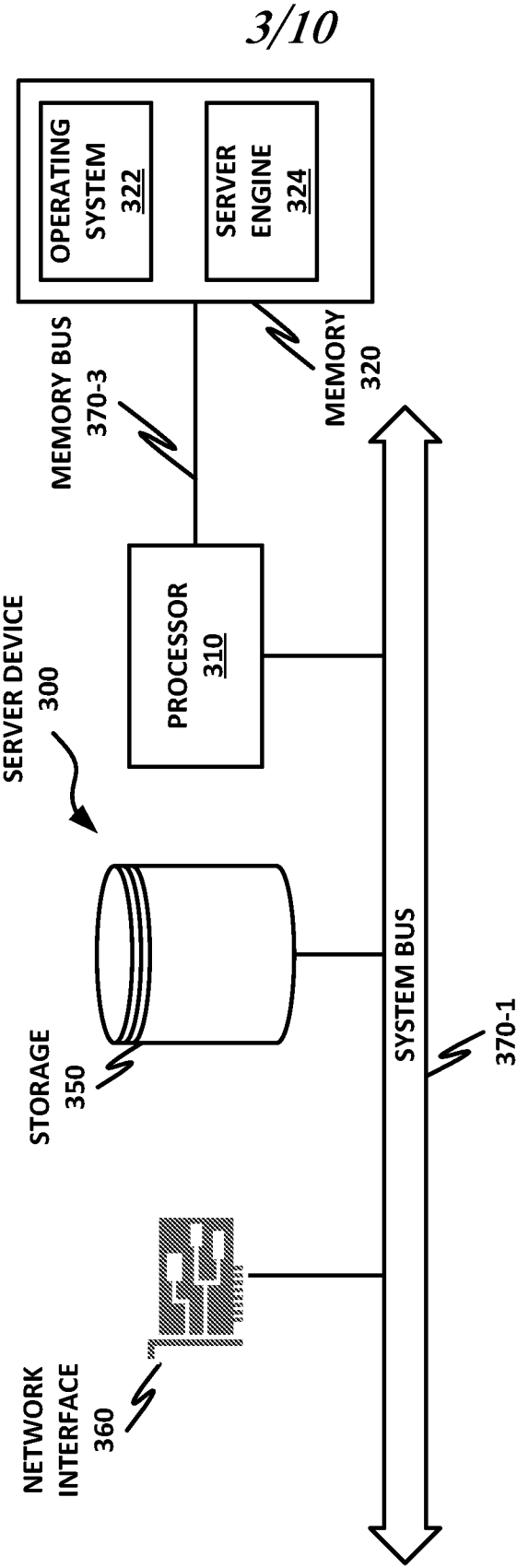


Fig. 3

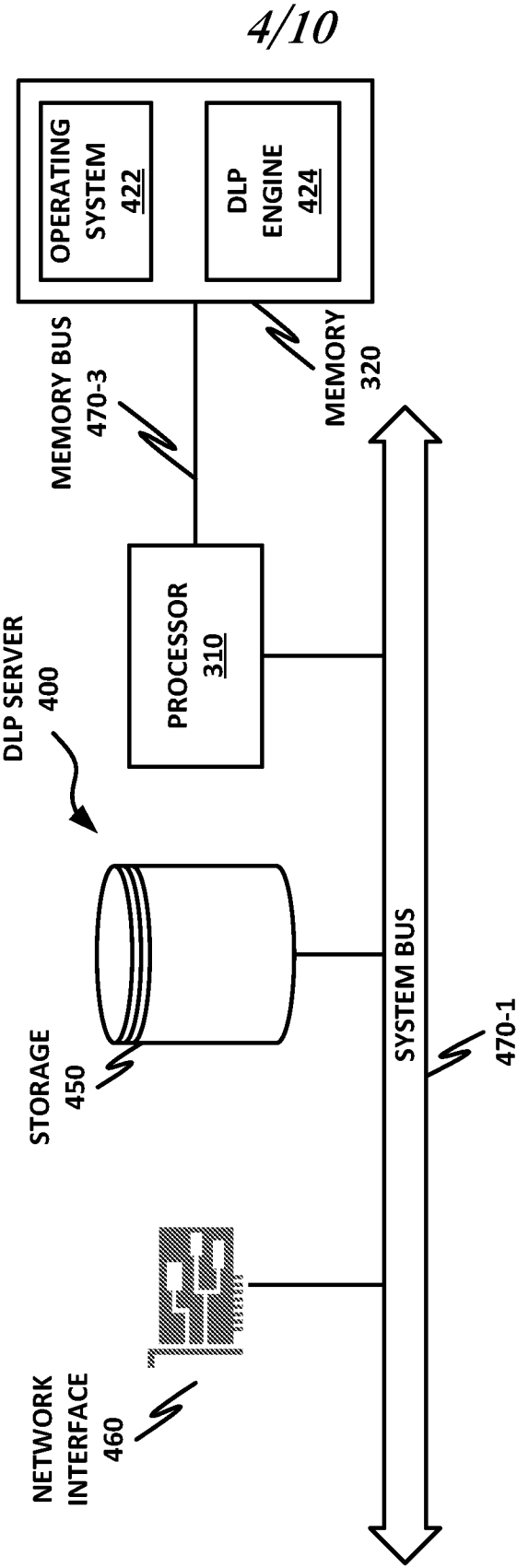
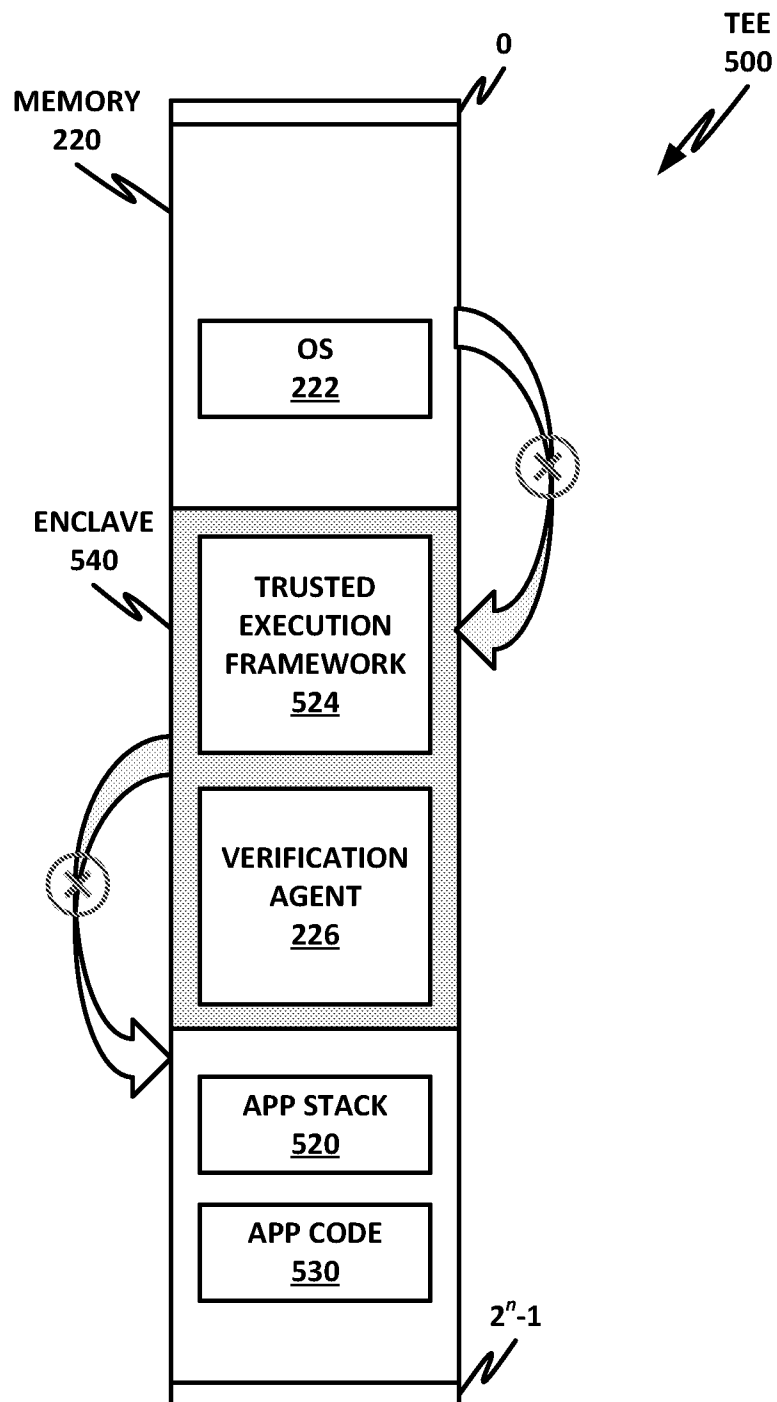
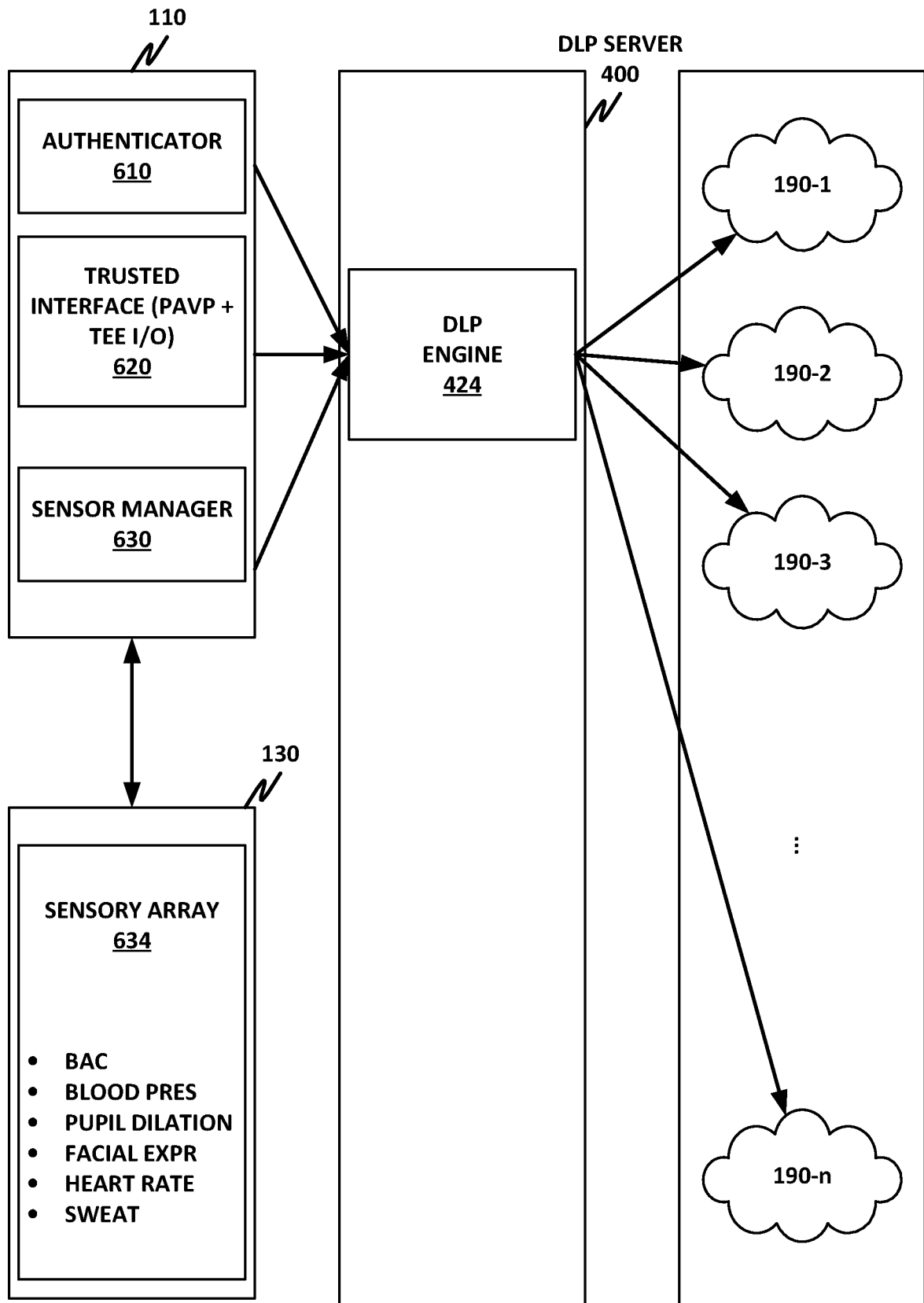


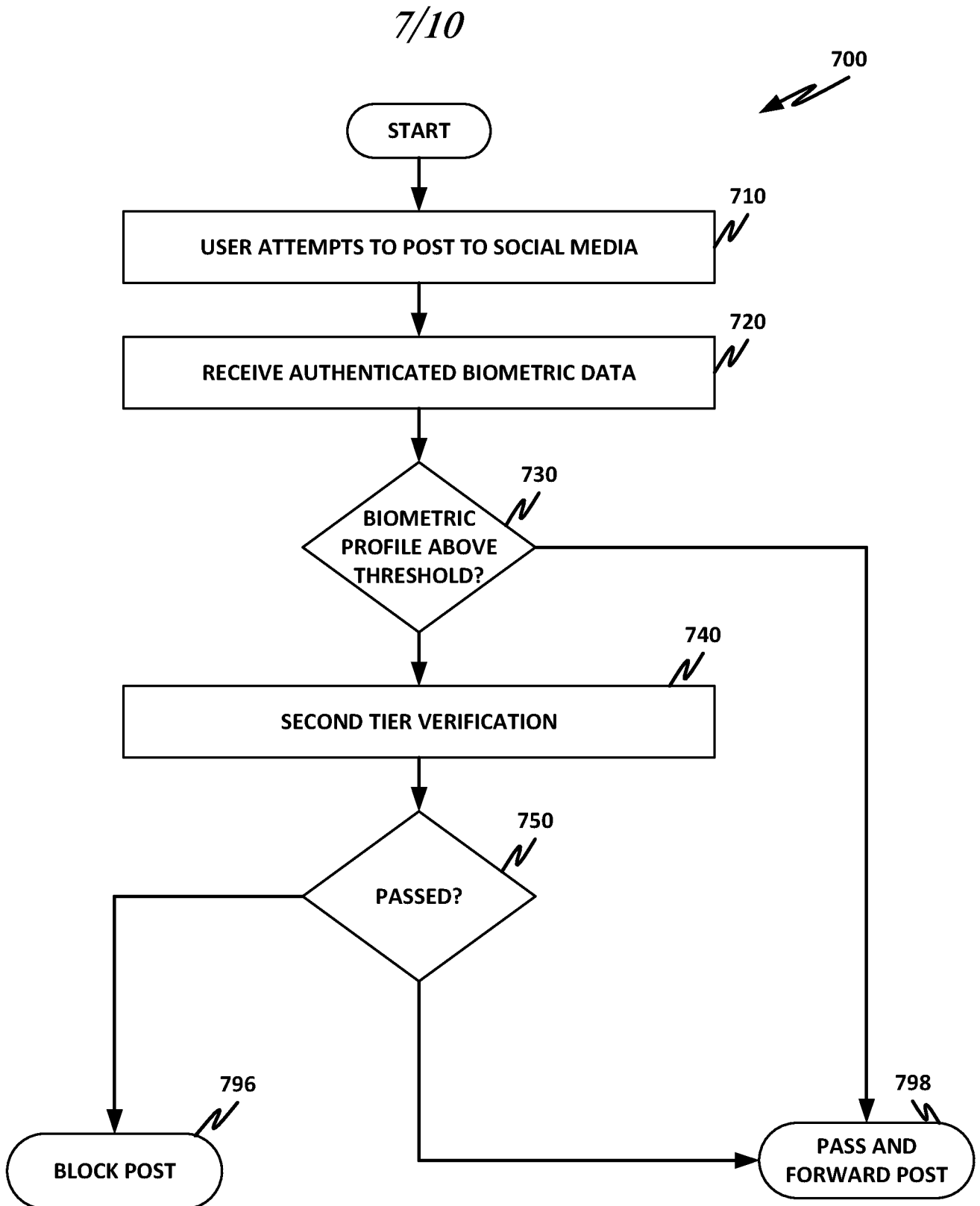
Fig. 4

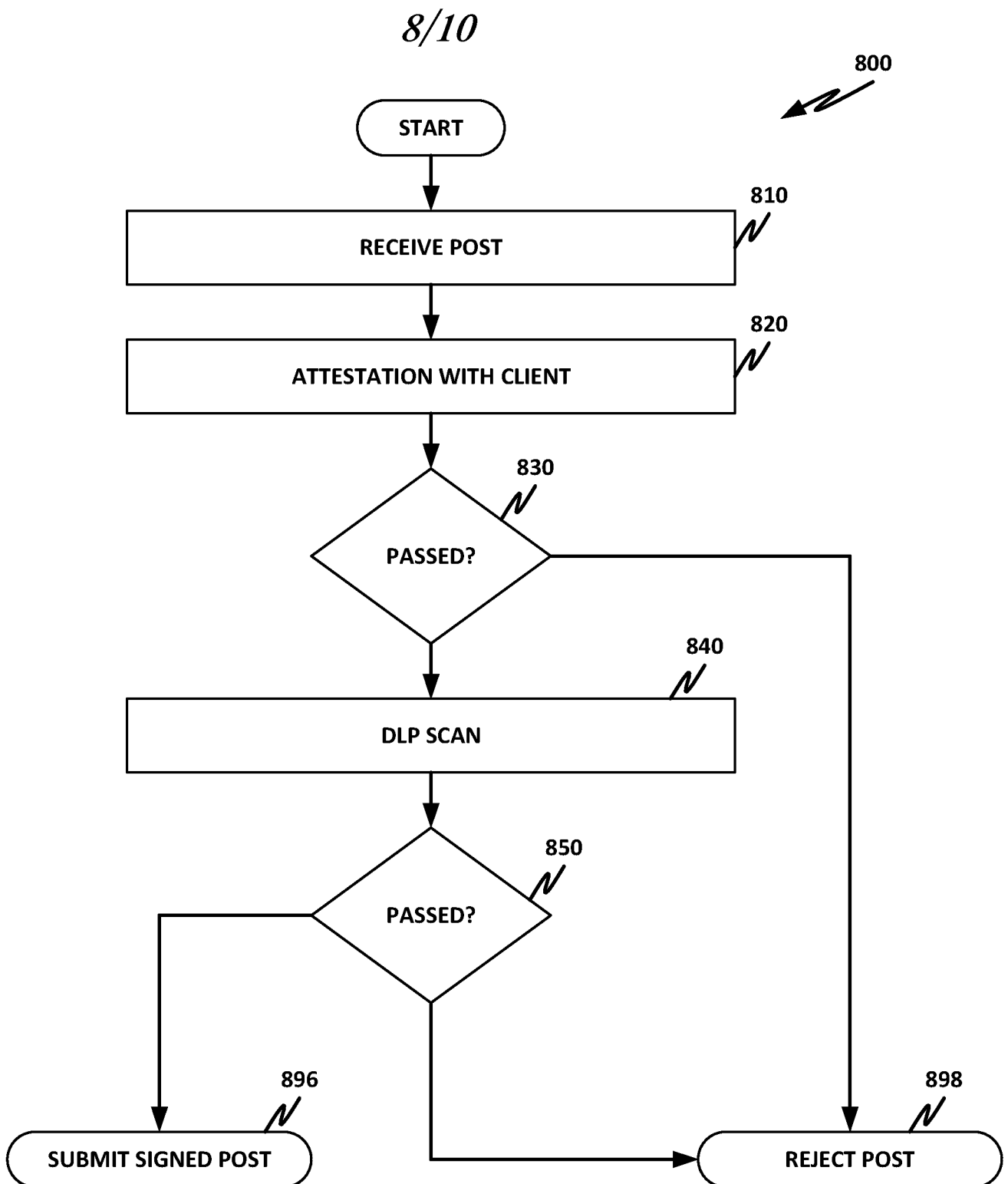
5/10

*Fig. 5*

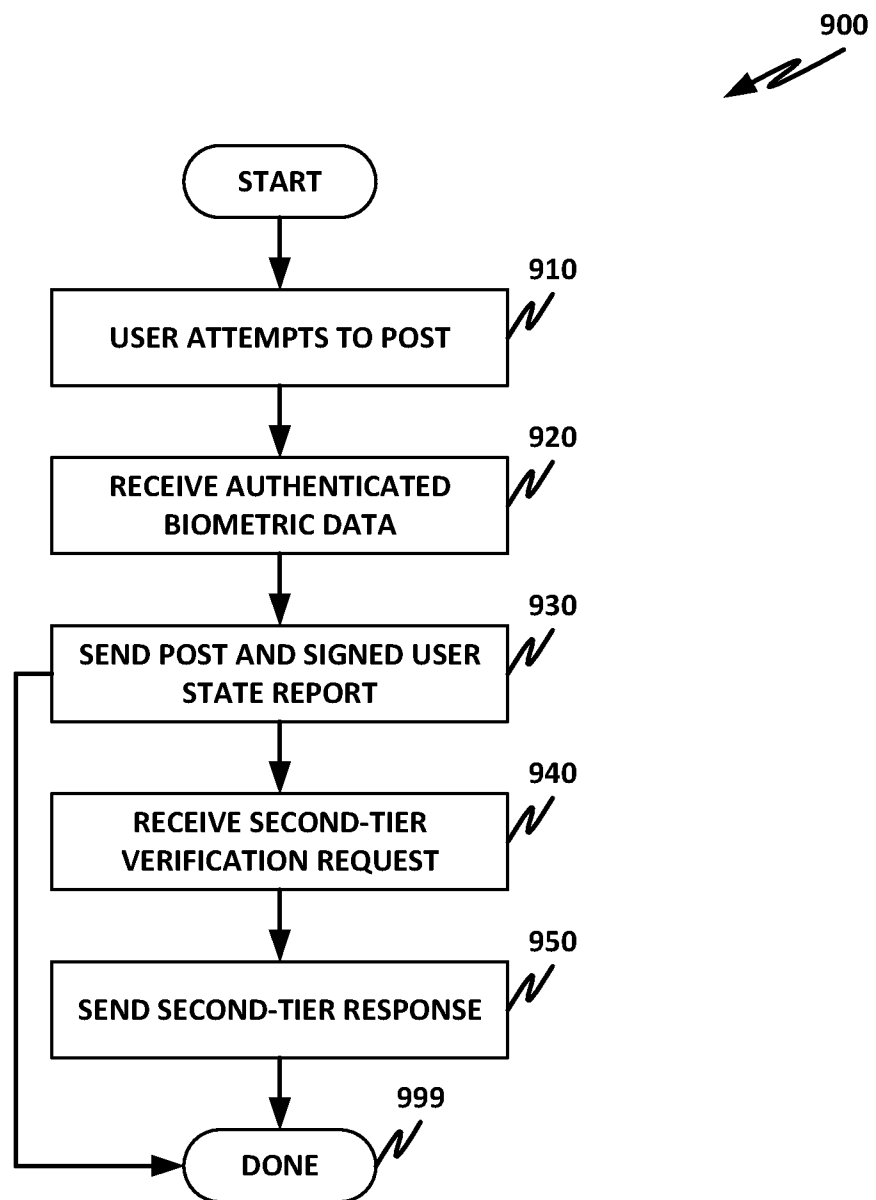
6/10

*Fig. 6*

*Fig. 7*

*Fig. 8*

9/10

*Fig. 9*

10/10

1000

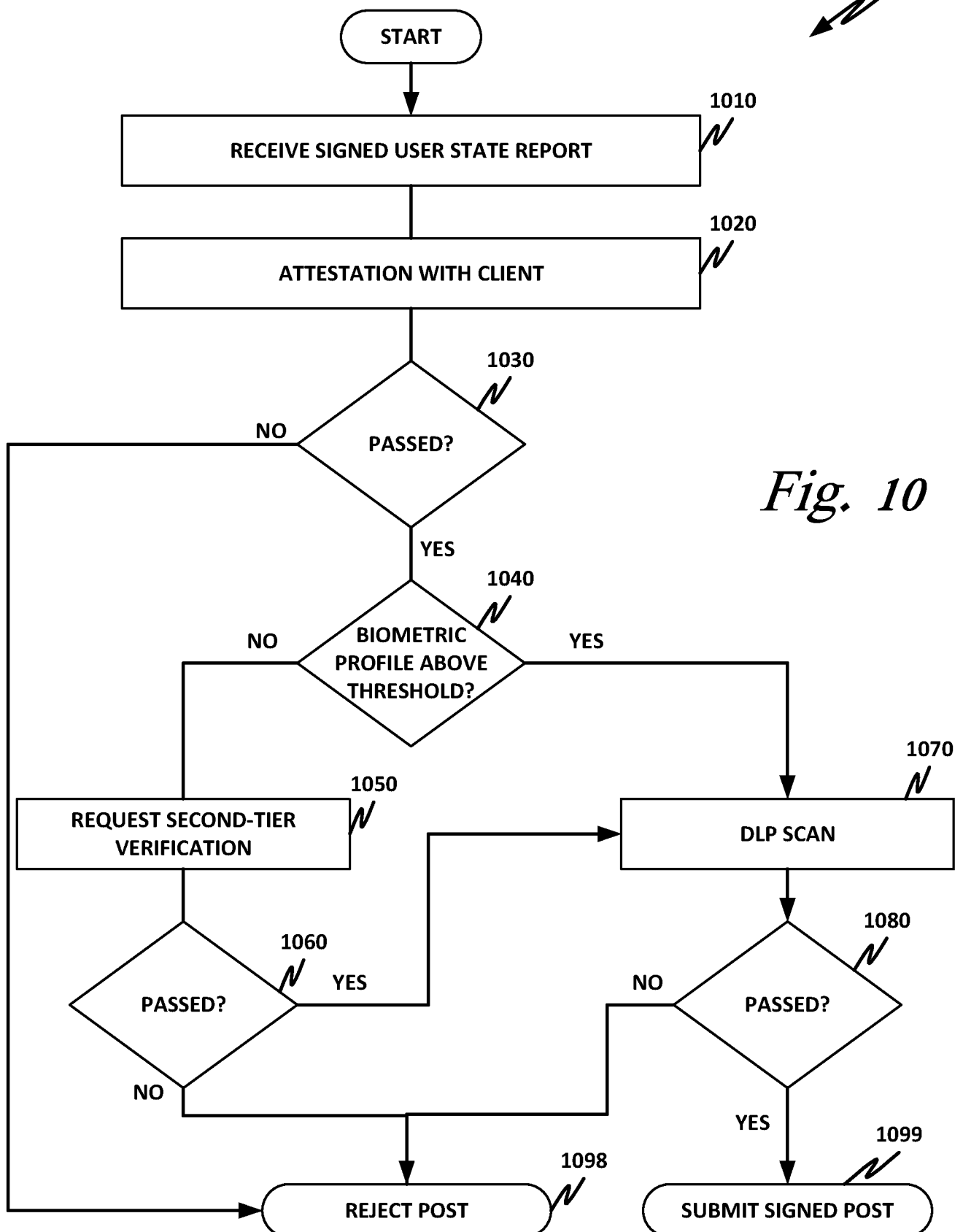


Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/062160**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/32(2006.01)i, G06Q 50/00(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 9/32; A61B 5/04; G06F 21/32; G06N 5/04; A61B 5/02; G06F 7/00; A61B 5/00; G06Q 50/00

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: psychological state data, analyze, user action, social media network, post

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014-0114899 A1 (EMPIRE TECHNOLOGY DEVELOPMENT LLC) 24 April 2014	1-3, 7-9, 13-15
Y	See paragraphs [0019], [0024]-[0029], [0033], [0048], [0049]; and figures 1-6.	, 19-20, 23
Y	US 2014-0195815 A1 (SYNAPTICS INCORPORATED) 10 July 2014	4-6, 10-12, 16-18
Y	See paragraphs [0035], [0043], [0047], [0058]; and figures 2, 5.	, 21-22, 24-25
Y	US 2008-0033303 A1 (RAMESH WARIAR et al.) 07 February 2008	4-6, 16-18, 24-25
Y	See paragraph [0023]; and figure 2.	10-12, 21-22
A	US 2007-0173733 A1 (TAN THI THAI LE et al.) 26 July 2007	1-25
A	See paragraphs [0047]-[0100]; and figures 3-9.	
A	US 2014-0107894 A1 (AUTO DIRECTOR TECHNOLOGIES, INC.) 17 April 2014	1-25
A	See paragraphs [0051]-[0061]; and figures 5, 6.	

☐ 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

16 February 2017 (16.02.2017)

Date of mailing of the international search report

17 February 2017 (17.02.2017)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea



Facsimile No. +82-42-481-8578

Authorized officer

Lee, Eun Kyu

Telephone No. +82-42-481-3580



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2016/062160

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0114899 A1	24/04/2014	US 9483736 B2 WO 2014-065781 A1	01/11/2016 01/05/2014
US 2014-0195815 A1	10/07/2014	US 9183365 B2	10/11/2015
US 2008-0033303 A1	07/02/2008	US 8337408 B2	25/12/2012
US 2007-0173733 A1	26/07/2007	CN 101331490 A EP 1924940 A2 JP 2009-521246 A KR 10-2008-0074099 A WO 2007-096706 A2 WO 2007-096706 A3	24/12/2008 28/05/2008 04/06/2009 12/08/2008 30/08/2007 20/03/2008
US 2014-0107894 A1	17/04/2014	US 2008-0082623 A1 US 2011-0160964 A1 US 2015-0200911 A1 US 8626382 B2 US 8990367 B2	03/04/2008 30/06/2011 16/07/2015 07/01/2014 24/03/2015