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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 January 2017 (05.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/003583 A1

(51) International Patent Classification:
G06F 21/79 (2013.01) *G06F 21/60* (2013.01)
G06F 21/62 (2013.01) *G06F 9/455* (2006.01)

(21) International Application Number:
PCT/US2016/033854

(22) International Filing Date:
24 May 2016 (24.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/752,914 27 June 2015 (27.06.2015) US

(71) Applicant: **MCAFEE, INC.** [US/US]; 2821 Mission College Boulevard, Santa Clara, CA 95054-1838 (US).

(72) Inventors: **SPURLOCK, Joel, R.**; 3153 NE Hoyt Street, Portland, OR 97232 (US). **ZHANG, Zheng**; 13293 NW Keeton Park Lane, Portland, OR 97229 (US). **KAPOOR, Aditya**; 13686 NW Henninger Lane, Portland, OR 97229 (US). **EDWARDS, Jonathan, L.**; 2535 NE 46th Avenue, Portland, OR 97213 (US). **PHAM, Khai, N.**; 2287 NW Sheffield Avenue, Beaverton, OR 97006 (US).

(74) Agent: **PEMBERTON, John, D.**; Patent Capital Group, c/o CPA Global, 900 Second Avenue South, Suite 600, Minneapolis, MN 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

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

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) Title: VIRTUALIZED TRUSTED STORAGE

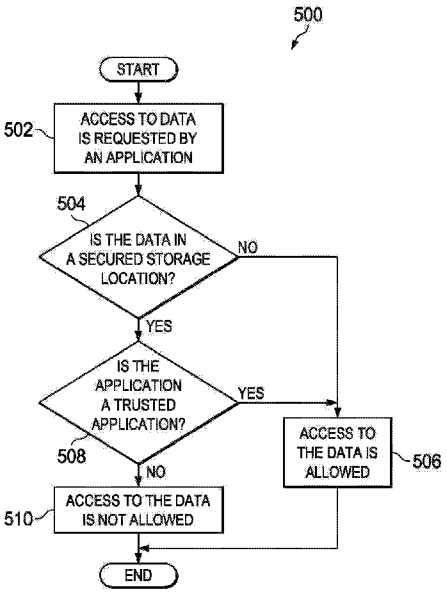


FIG. 5

(57) Abstract: Particular embodiments described herein provide for an electronic device that can be configured to receive a request from a process to access data is a system, determine if the data is in a virtualized protected area of memory in the system, and allow access to the data if the data is in the virtualized protected area of memory and the process is a trusted process. The electronic device can also be configured to determine if new data should be protected, store the new data in the virtualized protected area of memory in the system if the new data should be protected, and store the new data in an unprotected area of memory in the system if the new data should not be protected.

WO 2017/003583 A1

Published:

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

VIRTUALIZED TRUSTED STORAGE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of and priority to U.S. Nonprovisional (Utility) Patent Application No. 14/752,914 filed 27 June 2015 entitled "VIRTUALIZED TRUSTED STORAGE", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] This disclosure relates in general to the field of information security, and more particularly, to virtualized trusted storage.

BACKGROUND

[0003] The field of network security has become increasingly important in today's society. The Internet has enabled interconnection of different computer networks all over the world. In particular, the Internet provides a medium for exchanging data between different users connected to different computer networks via various types of client devices. While the use of the Internet has transformed business and personal communications, it has also been used as a vehicle for malicious operators to gain unauthorized access to computers and computer networks and for intentional or inadvertent disclosure of sensitive information.

[0004] Malicious software ("malware") that infects a host computer may be able to perform any number of malicious actions, such as stealing sensitive information from a business or individual associated with the host computer, propagating to other host computers, and/or assisting with distributed denial of service attacks, sending out spam or malicious emails from the host computer, etc. Hence, significant administrative challenges remain for protecting computers and computer networks from malicious and inadvertent exploitation by malicious software and devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] To provide a more complete understanding of the present disclosure and features and advantages thereof, reference is made to the following description, taken in conjunction with the accompanying figures, wherein like reference numerals represent like parts, in which:

[0006] FIGURE 1A is a simplified block diagram of a communication system for virtualized trusted storage, in accordance with an embodiment of the present disclosure;

[0007] FIGURE 1B is a simplified block diagram of a communication system for virtualized trusted storage, in accordance with an embodiment of the present disclosure;

[0008] FIGURE 2 is a simplified block diagram of a portion of a communication system for virtualized trusted storage, in accordance with an embodiment of the present disclosure;

[0009] FIGURE 3A is a simplified block diagram of a portion of a communication system for virtualized trusted storage, in accordance with an embodiment of the present disclosure;

[0009a] FIGURE 3B is a simplified block diagram of a portion of a communication system for virtualized trusted storage, in accordance with an embodiment of the present disclosure;

[0010] FIGURE 4 is a simplified flowchart illustrating potential operations that may be associated with the communication system in accordance with an embodiment;

[0011] FIGURE 5 is a simplified flowchart illustrating potential operations that may be associated with the communication system in accordance with an embodiment;

[0012] FIGURE 6 is a block diagram illustrating an example computing system that is arranged in a point-to-point configuration in accordance with an embodiment;

[0013] FIGURE 7 is a simplified block diagram associated with an example ARM ecosystem system on chip (SOC) of the present disclosure; and

[0014] FIGURE 8 is a block diagram illustrating an example processor core in accordance with an embodiment.

[0015] The FIGURES of the drawings are not necessarily drawn to scale, as their dimensions can be varied considerably without departing from the scope of the present disclosure.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

EXAMPLE EMBODIMENTS

[0016] FIGURE 1A is a simplified block diagram of a communication system 100a for virtualized trusted storage, in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 1A, an embodiment of communication system 100a can include an electronic device 102a, cloud services 104a, and a server 106a. Electronic device 102a can include memory 110, a processor 112, a trusted process 114, an untrusted process 116, and a security module 118. Memory 110 can include secured storage 120 and unsecured storage 122. Security module 118 can include a security storage module 124. Cloud services 104a and server 106a can each include a network security module 126. Electronic device 102a, cloud services 104a, and server 106a may be in communication using network 108.

[0017] Turning to FIGURE 1B, FIGURE 1B is a simplified block diagram of a communication system 100b for virtualized trusted storage, in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 1B, an embodiment of communication system 100b can include cloud services 104b, a server 106b, one or more trusted electronic devices 130, and one or more untrusted electronic devices 132. Cloud services 104b and server 106b can each include network security module 126 and network memory 136. Network security module 126 can include a network security storage module 134. Network memory 136 can include network secured storage 138 and network unsecured storage 140.

[0018] In an example embodiments, communication systems 100a and 100b can be configured for virtualized trusted secure storage, in accordance with an embodiment of the present disclosure. Security storage module 124 can be configured to use a file system driver and a reputation of process (e.g. trusted or untrusted) to dynamically virtualize a file system and secure critical user data. For example, communication systems 100a and 100b can be configured to receive a request from a process to access data is a system, determine if the data is in a virtualized protected area of memory in the system (e.g., secured storage 120 or network secured storage 138), allow access to the data is the data is not in the virtualized protected area of memory (e.g., unsecured storage 122 or network unsecured storage 140), and allow access to the data if the data is in the virtualized protected area of memory and the

process is a trusted process. For example, security module 118 or network security module 126 can be configured to determine if a process is a trusted or untrusted process. Communication systems 100a and 100b can also be configured to determine if new data should be protected, store the new data in the virtualized protected area of memory in the system if the new data should be protected, and store the new data in an unprotected area of memory in the system if the new data should not be protected.

[0019] Elements of FIGURES 1A and 1B may be coupled to one another through one or more interfaces employing any suitable connections (wired or wireless), which provide viable pathways for network (e.g., network 108, etc.) communications. Additionally, any one or more of these elements of FIGURES 1A and 1B may be combined or removed from the architecture based on particular configuration needs. Communication systems 100a and 100b may include a configuration capable of transmission control protocol/Internet protocol (TCP/IP) communications for the transmission or reception of packets in a network. Communication system systems 100a and 100b may also operate in conjunction with a user datagram protocol/IP (UDP/IP) or any other suitable protocol where appropriate and based on particular needs.

[0020] For purposes of illustrating certain example techniques of communication systems 100a and 100b, it is important to understand the communications that may be traversing the network environment. The following foundational information may be viewed as a basis from which the present disclosure may be properly explained.

[0021] Currently, the various concepts around virtualized trusted storage require the application vendor to write specific code or include binaries that are linked to a single secure storage. In addition, some existing solutions are custom coded for a single application (e.g., green border or other browser security solutions). Some current solutions have not been successful in providing security against malicious code or hackers inspecting, modifying, or removing user information and documents. What is needed is a system and method that can help secure data against ransomware, password stealers, or other threats that harvest or modify data on an electronic device. It would be beneficial is the system and method could use virtualized storage to secure trusted data.

[0022] A communication system for virtualized trusted storage, as outlined in FIGURES 1A and 1B, can resolve these issues (and others). Communication systems 100a and

100b may be configured to virtualize trusted process storage to a secure storage area (secure vault, encrypted file system, cloud storage, etc.). The secure storage area (e.g., secured storage 120 or network secured storage 138) may be virtualized by security storage module 124. Untrusted processes storage cannot access the virtualized trusted storage. In an example, file system drivers can redirect traffic to the virtualized trusted storage to make the virtualized trusted storage invisible to an untrusted application or an untrusted user.

[0023] Communication systems 100a and 100b may be configured to use security storage module 124 and/or a filter driver to redirect input/output (I/O) from trusted processes (e.g. trusted process 114) to secured storage (e.g., secured storage 120) and I/O from untrusted processes (e.g., untrusted process 116) to unsecured storage (e.g., unsecured storage 122). Untrusted processes do not get access to the secured storage and will get an untrusted view of the location. Trusted processes get full access to and a trusted view of the secured storage and unsecured storage.

[0024] The secured storage can be implemented in a variety of ways. For example, in an enterprise space, secured storage could be a cloud vault. In a consumer space, the secured storage could be a secured vault or locally encrypted virtual file system. A policy on minimum reputation can be set for access to the secured storage. In one example, the reputation of a process can be determined by security module 118 or network security module 126. The secured storage can also be protected by the file type trying to access the secured storage or on a per application type basis. The virtualization of the secured storage can be applied to execute on system locations (e.g. My Documents), on specific folders, or for specific applications. The system can mark individual files as important and only to be accessed by trusted applications and add the important file to secure storage. In addition, files can be removed from secure storage or added to the secured storage based on a user configuration. For example, a user may set a configuration where all applications should be able to access a specific file, only trusted applications should be able to access the specific file, only trusted applications of a specific type should be able to access the specific file, etc. Establishing the reputation of a process may be done using cloud services, local certifications, whitelists, etc.

[0025] Turning to the infrastructure of FIGURES 1A and 1B, communication systems 100a and 100b in accordance with an example embodiment is shown. Generally, communication systems 100a and 100b can be implemented in any type or topology of

networks. Network 108 represents a series of points or nodes of interconnected communication paths for receiving and transmitting packets of information that propagate through communication systems 100a and 100b. Network 108 offers a communicative interface between nodes, and may be configured as any local area network (LAN), virtual local area network (VLAN), wide area network (WAN), wireless local area network (WLAN), metropolitan area network (MAN), Intranet, Extranet, virtual private network (VPN), and any other appropriate architecture or system that facilitates communications in a network environment, or any suitable combination thereof, including wired and/or wireless communication.

[0026] In communication systems 100a and 100b, network traffic, which is inclusive of packets, frames, signals, data, etc., can be sent and received according to any suitable communication messaging protocols. Suitable communication messaging protocols can include a multi-layered scheme such as Open Systems Interconnection (OSI) model, or any derivations or variants thereof (e.g., Transmission Control Protocol/Internet Protocol (TCP/IP), user datagram protocol/IP (UDP/IP)). Additionally, radio signal communications over a cellular network may also be provided in communication systems 100a and 100b. Suitable interfaces and infrastructure may be provided to enable communication with the cellular network.

[0027] The term "packet" as used herein, refers to a unit of data that can be routed between a source node and a destination node on a packet switched network. A packet includes a source network address and a destination network address. These network addresses can be Internet Protocol (IP) addresses in a TCP/IP messaging protocol. The term "data" as used herein, refers to any type of binary, numeric, voice, video, textual, or script data, or any type of source or object code, or any other suitable information in any appropriate format that may be communicated from one point to another in electronic devices and/or networks. Additionally, messages, requests, responses, and queries are forms of network traffic, and therefore, may comprise packets, frames, signals, data, etc.

[0028] In an example implementation, electronic device 102a, cloud services 104a and 104b, server 106a and 106b, one or more trusted electronic devices 130, and one or more untrusted electronic devices 132 are network elements, which are meant to encompass network appliances, servers, routers, switches, gateways, bridges, load balancers, processors,

modules, or any other suitable device, component, element, or object operable to exchange information in a network environment. Network elements may include any suitable hardware, software, components, modules, or objects that facilitate the operations thereof, as well as suitable interfaces for receiving, transmitting, and/or otherwise communicating data or information in a network environment. This may be inclusive of appropriate algorithms and communication protocols that allow for the effective exchange of data or information.

[0029] In regards to the internal structure associated with communication systems 100a and 100b, each of electronic device 102a, cloud services 104a and 104b, server 106a and 106b, one or more trusted electronic devices 130, and one or more untrusted electronic devices 132 can include memory elements for storing information to be used in the operations outlined herein. Each of electronic device 102a, cloud services 104a and 104b, server 106a and 106b, one or more trusted electronic devices 130, and one or more untrusted electronic devices 132 may keep information in any suitable memory element (e.g., random access memory (RAM), read-only memory (ROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), application specific integrated circuit (ASIC), etc.), software, hardware, firmware, or in any other suitable component, device, element, or object where appropriate and based on particular needs. Any of the memory items discussed herein should be construed as being encompassed within the broad term 'memory element.' Moreover, the information being used, tracked, sent, or received in communication systems 100a and 100b could be provided in any database, register, queue, table, cache, control list, or other storage structure, all of which can be referenced at any suitable timeframe. Any such storage options may also be included within the broad term 'memory element' as used herein.

[0030] In certain example implementations, the functions outlined herein may be implemented by logic encoded in one or more tangible media (e.g., embedded logic provided in an ASIC, digital signal processor (DSP) instructions, software (potentially inclusive of object code and source code) to be executed by a processor, or other similar machine, etc.), which may be inclusive of non-transitory computer-readable media. In some of these instances, memory elements can store data used for the operations described herein. This includes the

memory elements being able to store software, logic, code, or processor instructions that are executed to carry out the activities described herein.

[0031] In an example implementation, network elements of communication systems 100a and 100b, such as electronic device 102a, cloud services 104a 104b, and server 106a and 106b, may include software modules (e.g., security module 118, security storage module 124, network security module 126, and network security storage module 134) to achieve, or to foster, operations as outlined herein. These modules may be suitably combined in any appropriate manner, which may be based on particular configuration and/or provisioning needs. In example embodiments, such operations may be carried out by hardware, implemented externally to these elements, or included in some other network device to achieve the intended functionality. Furthermore, the modules can be implemented as software, hardware, firmware, or any suitable combination thereof. These elements may also include software (or reciprocating software) that can coordinate with other network elements in order to achieve the operations, as outlined herein.

[0032] Additionally, each of electronic device 102a, cloud services 104a and 104b, server 106a and 106b, one or more trusted electronic devices 130, and one or more untrusted electronic devices 132 may include a processor that can execute software or an algorithm to perform activities as discussed herein. A processor can execute any type of instructions associated with the data to achieve the operations detailed herein. In one example, the processors could transform an element or an article (e.g., data) from one state or thing to another state or thing. In another example, the activities outlined herein may be implemented with fixed logic or programmable logic (e.g., software/computer instructions executed by a processor) and the elements identified herein could be some type of a programmable processor, programmable digital logic (e.g., a field programmable gate array (FPGA), an EPROM, an EEPROM) or an ASIC that includes digital logic, software, code, electronic instructions, or any suitable combination thereof. Any of the potential processing elements, modules, and machines described herein should be construed as being encompassed within the broad term 'processor.'

[0033] Electronic device 102a can be a network element and include, for example, desktop computers, laptop computers, mobile devices, personal digital assistants, smartphones, tablets, or other similar devices. Cloud services 104a is configured to provide

cloud services to electronic device 102a. Cloud services 104b is configured to provide cloud services to one or more trusted electronic devices 130 and one or more untrusted electronic devices 132. Cloud services may generally be defined as the use of computing resources that are delivered as a service over a network, such as the Internet. Typically, compute, storage, and network resources are offered in a cloud infrastructure, effectively shifting the workload from a local network to the cloud network. Server 106a and 106b can be a network element such as a server or virtual server and can be associated with clients, customers, endpoints, or end users wishing to initiate a communication in communication system 100a and 100b via some network (e.g., network 108). The term 'server' is inclusive of devices used to serve the requests of clients and/or perform some computational task on behalf of clients within communication systems 100a and 100b. Although security module 118 is represented in FIGURE 1A as being located in electronic device 102a, this is for illustrative purposes only. Security module 118 could be combined or separated in any suitable configuration. Furthermore, security module 118 could be integrated with or distributed in another network accessible by electronic device 102a such as cloud services 104a or server 106a.

[0034] Turning to FIGURE 2, FIGURE 2 is a simplified block diagram of a portion of a communication system 100a for virtualized trusted secure storage, in accordance with an embodiment of the present disclosure. FIGURE 2 illustrates an embodiment of an electronic device 102b. Electronic device 102b can include memory 110, processor 112, trusted process 114, untrusted process 116, security module 118, and a filter driver 128.

[0035] Security storage module 124 can be configured to use filter driver 128 to redirect I/O from trusted process 114 to secured storage 120 and I/O from untrusted processes 116 to unsecured storage 122. Untrusted processes do not get access to the secured storage and will get an untrusted view of the location. Trusted processes get full access to and a trusted view of the secured storage and unsecured storage.

[0036] Turning to FIGURE 3A, FIGURE 3A is a simplified block diagram of a portion of a communication system for virtualized trusted storage, in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 3A, the virtualization of the secured storage can be applied to execute on system locations such as My Documents. My Documents is the commonly recognized name of a special folder in Microsoft Windows® that is allocated to help users store their personal data files. When a trusted user, trusted process 114, or some

other trusted application, accesses a My Documents folder, a secured view 142 or access of the My Documents folder can include both unsecured files 144 and secured files 146.

[0037] Turning to FIGURE 3B, FIGURE 3B is a simplified block diagram of a portion of a communication system for virtualized trusted storage, in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 3B, when an untrusted trusted user, untrusted process untrusted process 116, or some other untrusted application, accesses the My Documents folder , an unsecured view 148 or access of the My Documents folder can include only unsecured files 144. Because the user, process, or other application is not trusted, secured files 146 are not available.

[0038] Turning to FIGURE 4, FIGURE 4 is an example flowchart illustrating possible operations of a flow 400 that may be associated with virtualized secure storage, in accordance with an embodiment. In an embodiment, one or more operations of flow 400 may be performed by security module 118, security storage module 124, network security module 126, and network security storage module 134. At 402, data is to be stored in a system. At 404, the system determines if access to the data is be restricted. For example, the data may be from a trusted application, a user may set a configuration where access to the data is restricted, etc. If the access to the data should be restricted, then the data is stored in secured storage, as in 406. If the data should not be restricted, then the data is stored in unsecured storage, as in 408.

[0039] Turning to FIGURE 5, FIGURE 5 is an example flowchart illustrating possible operations of a flow 500 that may be associated with virtualized secure storage, in accordance with an embodiment. In an embodiment, one or more operations of flow 500 may be performed by security module 118, security storage module 124, network security module 126, and network security storage module 134. At 502, access to data is requested by an application. At 504, the system determines if the data is in a secured storage location. If the data is not in a secured storage location, then access to the data is allowed, as in 506. If the data is in a secured storage location, then the system determines if the application is a trusted application, as in 508. If the application is a trusted application, then access to the data is allowed, as in 506. If the application is not a trusted application, then access to the data is not allowed, as in 510.

[0040] FIGURE 6 illustrates a computing system 600 that is arranged in a point-to-point (PtP) configuration according to an embodiment. In particular, FIGURE 6 shows a system where processors, memory, and input/output devices are interconnected by a number of point-to-point interfaces. Generally, one or more of the network elements of communication systems 100a and 100b may be configured in the same or similar manner as computing system 600.

[0041] As illustrated in FIGURE 6, system 600 may include several processors, of which only two, processors 670 and 680, are shown for clarity. While two processors 670 and 680 are shown, it is to be understood that an embodiment of system 600 may also include only one such processor. Processors 670 and 680 may each include a set of cores (i.e., processor cores 674A and 674B and processor cores 684A and 684B) to execute multiple threads of a program. The cores may be configured to execute instruction code in a manner similar to that discussed above with reference to FIGURES 1-5. Each processor 670, 680 may include at least one shared cache 671, 681. Shared caches 671, 681 may store data (e.g., instructions) that are utilized by one or more components of processors 670, 680, such as processor cores 674 and 684.

[0042] Processors 670 and 680 may also each include integrated memory controller logic (MC) 672 and 682 to communicate with memory elements 632 and 634. Memory elements 632 and/or 634 may store various data used by processors 670 and 680. In alternative embodiments, memory controller logic 672 and 682 may be discrete logic separate from processors 670 and 680.

[0043] Processors 670 and 680 may be any type of processor and may exchange data via a point-to-point (PtP) interface 650 using point-to-point interface circuits 678 and 688, respectively. Processors 670 and 680 may each exchange data with a chipset 690 via individual point-to-point interfaces 652 and 654 using point-to-point interface circuits 676, 686, 694, and 698. Chipset 690 may also exchange data with a high-performance graphics circuit 638 via a high-performance graphics interface 639, using an interface circuit 692, which could be a PtP interface circuit. In alternative embodiments, any or all of the PtP links illustrated in FIGURE 6 could be implemented as a multi-drop bus rather than a PtP link.

[0044] Chipset 690 may be in communication with a bus 620 via an interface circuit 696. Bus 620 may have one or more devices that communicate over it, such as a bus bridge

618 and I/O devices 616. Via a bus 610, bus bridge 618 may be in communication with other devices such as a keyboard/mouse 612 (or other input devices such as a touch screen, trackball, etc.), communication devices 626 (such as modems, network interface devices, or other types of communication devices that may communicate through a computer network 660), audio I/O devices 614, and/or a data storage device 628. Data storage device 628 may store code 630, which may be executed by processors 670 and/or 680. In alternative embodiments, any portions of the bus architectures could be implemented with one or more PtP links.

[0045] The computer system depicted in FIGURE 6 is a schematic illustration of an embodiment of a computing system that may be utilized to implement various embodiments discussed herein. It will be appreciated that various components of the system depicted in FIGURE 6 may be combined in a system-on-a-chip (SoC) architecture or in any other suitable configuration. For example, embodiments disclosed herein can be incorporated into systems including mobile devices such as smart cellular telephones, tablet computers, personal digital assistants, portable gaming devices, etc. It will be appreciated that these mobile devices may be provided with SoC architectures in at least some embodiments.

[0046] Turning to FIGURE 7, FIGURE 7 is a simplified block diagram associated with an example ARM ecosystem SOC 700 of the present disclosure. At least one example implementation of the present disclosure can include the virtualized trusted storage features discussed herein and an ARM component. For example, the example of FIGURE 7 can be associated with any ARM core (e.g., A-7, A-15, etc.). Further, the architecture can be part of any type of tablet, smartphone (inclusive of Android™ phones, iPhones™), iPad™, Google Nexus™, Microsoft Surface™, personal computer, server, video processing components, laptop computer (inclusive of any type of notebook), Ultrabook™ system, any type of touch-enabled input device, etc.

[0047] In this example of FIGURE 7, ARM ecosystem SOC 700 may include multiple cores 706-707, an L2 cache control 708, a bus interface unit 709, an L2 cache 710, a graphics processing unit (GPU) 715, an interconnect 702, a video codec 720, and a liquid crystal display (LCD) I/F 725, which may be associated with mobile industry processor interface (MIPI)/ high-definition multimedia interface (HDMI) links that couple to an LCD.

[0048] ARM ecosystem SOC 700 may also include a subscriber identity module (SIM) I/F 730, a boot read-only memory (ROM) 735, a synchronous dynamic random access memory (SDRAM) controller 740, a flash controller 745, a serial peripheral interface (SPI) master 750, a suitable power control 755, a dynamic RAM (DRAM) 760, and flash 765. In addition, one or more embodiments include one or more communication capabilities, interfaces, and features such as instances of Bluetooth™ 770, a 3G modem 775, a global positioning system (GPS) 780, and an 802.11 Wi-Fi 785.

[0049] In operation, the example of FIGURE 7 can offer processing capabilities, along with relatively low power consumption to enable computing of various types (e.g., mobile computing, high-end digital home, servers, wireless infrastructure, etc.). In addition, such an architecture can enable any number of software applications (e.g., Android™, Adobe® Flash® Player, Java Platform Standard Edition (Java SE), JavaFX, Linux, Microsoft Windows Embedded, Symbian and Ubuntu, etc.). In at least one example embodiment, the core processor may implement an out-of-order superscalar pipeline with a coupled low-latency level-2 cache.

[0050] FIGURE 8 illustrates a processor core 800 according to an embodiment. Processor core 800 may be the core for any type of processor, such as a micro-processor, an embedded processor, a digital signal processor (DSP), a network processor, or other device to execute code. Although only one processor core 800 is illustrated in Figure 8, a processor may alternatively include more than one of the processor core 800 illustrated in Figure 8. For example, processor core 800 represents one example embodiment of processors cores 674a, 674b, 684a, and 684b shown and described with reference to processors 670 and 680 of FIGURE 6. Processor core 800 may be a single-threaded core or, for at least one embodiment, processor core 800 may be multithreaded in that it may include more than one hardware thread context (or "logical processor") per core.

[0051] FIGURE 8 also illustrates a memory 802 coupled to processor core 800 in accordance with an embodiment. Memory 802 may be any of a wide variety of memories (including various layers of memory hierarchy) as are known or otherwise available to those of skill in the art. Memory 802 may include code 804, which may be one or more instructions, to be executed by processor core 800. Processor core 800 can follow a program sequence of instructions indicated by code 804. Each instruction enters a front-end logic 806 and is

processed by one or more decoders 808. The decoder may generate, as its output, a micro operation such as a fixed width micro operation in a predefined format, or may generate other instructions, microinstructions, or control signals that reflect the original code instruction. Front-end logic 806 also includes register renaming logic 810 and scheduling logic 812, which generally allocate resources and queue the operation corresponding to the instruction for execution.

[0052] Processor core 800 can also include execution logic 814 having a set of execution units 816-1 through 816-N. Some embodiments may include a number of execution units dedicated to specific functions or sets of functions. Other embodiments may include only one execution unit or one execution unit that can perform a particular function. Execution logic 814 performs the operations specified by code instructions.

[0053] After completion of execution of the operations specified by the code instructions, back-end logic 818 can retire the instructions of code 804. In one embodiment, processor core 800 allows out of order execution but requires in order retirement of instructions. Retirement logic 820 may take a variety of known forms (e.g., re-order buffers or the like). In this manner, processor core 800 is transformed during execution of code 804, at least in terms of the output generated by the decoder, hardware registers and tables utilized by register renaming logic 810, and any registers (not shown) modified by execution logic 814.

[0054] Although not illustrated in FIGURE 8, a processor may include other elements on a chip with processor core 800, at least some of which were shown and described herein with reference to FIGURE 6. For example, as shown in FIGURE 6, a processor may include memory control logic along with processor core 800. The processor may include I/O control logic and/or may include I/O control logic integrated with memory control logic.

[0055] Note that with the examples provided herein, interaction may be described in terms of two, three, or more network elements. However, this has been done for purposes of clarity and example only. 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 network elements. It should be appreciated that communication systems 100a and 100b 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 communication systems 100a and 100b as potentially applied to a myriad of other architectures.

[0056] It is also important to note that the operations in the preceding flow diagrams (i.e., FIGURES 4 and 5) illustrate only some of the possible correlating scenarios and patterns that may be executed by, or within, communication systems 100a and 100b. Some of these operations may be deleted or removed where appropriate, or these operations may be modified or changed considerably without departing from the scope of the present disclosure. In addition, a number of these operations have been described as being executed concurrently with, or in parallel to, one or more additional operations. However, the timing of these operations may be altered considerably. The preceding operational flows have been offered for purposes of example and discussion. Substantial flexibility is provided by communication systems 100a and 100b in that any suitable arrangements, chronologies, configurations, and timing mechanisms may be provided without departing from the teachings of the present disclosure.

[0057] Although the present disclosure has been described in detail with reference to particular arrangements and configurations, these example configurations and arrangements may be changed significantly without departing from the scope of the present disclosure. Moreover, certain components may be combined, separated, eliminated, or added based on particular needs and implementations. Additionally, although communication systems 100a and 100b has been illustrated with reference to particular elements and operations that facilitate the communication process, these elements and operations may be replaced by any suitable architecture, protocols, and/or processes that achieve the intended functionality of communication systems 100a and 100b

[0058] 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 as it exists on the date of the filing hereof unless the words "means for" or "step 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 reflected in the appended claims.

OTHER NOTES AND EXAMPLES

[0059] Example C1 is at least one machine readable medium having one or more instructions that when executed by at least one processor, cause the at least processor to receive a request from a process to access data is a system, determine if the data is in a virtualized protected area of memory in the system, and allow access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

[0060] In Example C2, the subject matter of Example C1 can optionally include where the one or more instructions that when executed by the at least one processor, further cause the at least one processor to determine if new data should be protected, store the new data in the virtualized protected area of memory in the system if the new data should be protected, and store the new data in an unprotected area of memory in the system if the new data should not be protected.

[0061] In Example C3, the subject matter of any one of Examples C1-C2 can optionally include where the device characteristics are at least partially based on other device characteristics of similar devices.

[0062] In Example C4, the subject matter of any one of Examples C1-C3 can optionally include where the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

[0063] In Example C5, the subject matter of any one of Examples C1-C4 can optionally include where the virtualized protected area of memory is a cloud vault.

[0064] In Example C6, the subject matter of any one of Example C1-C5 can optionally include where a filter driver controls input and output access to the virtualized protected area of memory.

[0065] In Example A1, an electronic device can include a security storage module, where the security storage module is configured to receive a request from a process to access data is a system, determine if the data is in a virtualized protected area of memory in the

system, and allow access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

[0066] In Example, A2, the subject matter of Example A1 can optionally include where the security storage module is further configured to determine if new data should be protected, store the new data in the virtualized protected area of memory in the system if the new data should be protected, and store the new data in an unprotected area of memory in the system if the new data should not be protected.

[0067] In Example A3, the subject matter of any one of Examples A1-A2 can optionally include where the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

[0068] In Example A4, the subject matter of any one of Examples A1-A3 can optionally include where the virtualized protected area of memory is a cloud vault.

[0069] In Example A5, the subject matter of any one of Examples A1-A4 can optionally include where a filter driver controls input and output access to the virtualized protected area of memory.

[0070] Example M1 is a method including receiving a request from a process to access data is a system, determining if the data is in a virtualized protected area of memory in the system, and allowing access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

[0071] In Example M2, the subject matter of Example M1 can optionally include determining if new data should be protected, storing the new data in the virtualized protected area of memory in the system if the new data should be protected, and storing the new data in an unprotected area of memory in the system if the new data should not be protected.

[0072] In Example M3, the subject matter of any one of the Examples M1-M2 can optionally include where the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

[0073] In Example M4, the subject matter of any one of the Examples M1-M3 can optionally include where the virtualized protected area of memory is a cloud vault.

[0074] In Example M5, the subject matter of any one of the Examples M1-M4 can optionally include denying access to the data if the data is in the virtualized protected area of memory and the process is an untrusted process.

[0075] In Example M6, the subject matter of any one of the Examples M1-M5 can optionally include where a filter driver controls input and output access to the virtualized protected area of memory.

[0076] Example S1 is a system for virtualized trusted secure storage, the system including a security storage module configured to receive a request from a process to access data is a system, determine if the data is in a virtualized protected area of memory in the system, and allow access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

[0077] In Example S2, the subject matter of Example S1 can optionally include where system is further configured to determine if new data should be protected, store the new data in the virtualized protected area of memory in the system if the new data should be protected, and store the new data in an unprotected area of memory in the system if the new data should not be protected.

[0078] In Example S3, the subject matter of any one of the Examples S1-S2 can optionally include where the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

[0079] In Example S4, the subject matter of any one of the Examples S1-S3 can optionally include where the virtualized protected area of memory is a cloud vault.

[0080] In Example S5, the subject matter of any one of the Examples S1-S4 can optionally include a filter driver controls input and output access to the virtualized protected area of memory.

[0081] Example X1 is a machine-readable storage medium including machine-readable instructions to implement a method or realize an apparatus as in any one of the Examples A1-A5, or M1-M6. Example Y1 is an apparatus comprising means for performing of any of the Example methods M1-M6. In Example Y2, the subject matter of Example Y1 can optionally include the means for performing the method comprising a processor and a memory. In Example Y3, the subject matter of Example Y2 can optionally include the memory comprising machine-readable instructions.

CLAIMS:

1. At least one machine readable medium comprising one or more instructions that when executed by at least one processor, cause the at least one processor to:

receive a request from a process to access data in a system;

determine if the data is in a virtualized protected area of memory in the system; and

allow access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

2. The at least one machine readable medium of Claim 1, further comprising one or more instructions that when executed by at least one processor, cause the at least one processor to:

determine if new data should be protected;

store the new data in the virtualized protected area of memory in the system if the new data should be protected; and

store the new data in an unprotected area of memory in the system if the new data should not be protected.

3. The at least one machine readable medium of any of Claims 1 and 2, wherein the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

4. The at least one machine readable medium of any of Claims 1-3, wherein the virtualized protected area of memory is a cloud vault.

5. The at least one machine readable medium of any of Claims 1-4, wherein a filter driver controls input and output access to the virtualized protected area of memory.

6. An apparatus comprising:

security storage module configured to:

receive a request from a process to access data is a system;

determine if the data is in a virtualized protected area of memory in the system; and

allow access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

7. The apparatus of Claim 6, wherein the security storage module is further configured to:

determine if new data should be protected;

store the new data in the virtualized protected area of memory in the system if the new data should be protected; and

store the new data in an unprotected area of memory in the system if the new data should not be protected.

8. The apparatus of any of Claims 6 and 7, wherein the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

9. The apparatus of any of Claims 6-8, wherein the virtualized protected area of memory is a cloud vault.

10. The apparatus of any of Claims 6-9, wherein a filter driver controls input and output access to the virtualized protected area of memory.

11. A method comprising:

receiving a request from a process to access data is a system;

determining if the data is in a virtualized protected area of memory in the system; and

allowing access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

12. The method of Claim 11, further comprising:

determining if new data should be protected;

storing the new data in the virtualized protected area of memory in the system if the new data should be protected; and

storing the new data in an unprotected area of memory in the system if the new data should not be protected.

13. The method of any of Claims 11 and 12, wherein the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

14. The method of any of Claims 11-13, wherein the virtualized protected area of memory is a cloud vault.

15. The method of any of Claims 11-14, further comprising:

denying access to the data if the data is in the virtualized protected area of memory and the process is an untrusted process.

16. A system for virtualized trusted secure storage, the system comprising:

security storage module configured to:

receive a request from a process to access data is a system;

determine if the data is in a virtualized protected area of memory in the system; and

allow access to the data if the data is in the virtualized protected area of memory and the process is a trusted process.

17. The system of Claim 16, wherein the system is further configured to:

determine if new data should be protected;

store the new data in the virtualized protected area of memory in the system if the new data should be protected; and

store the new data in an unprotected area of memory in the system if the new data should not be protected.

18. The system of any of Claims 16 and 17, wherein the virtualized protected area of memory is a secured vault or a locally encrypted virtual file system.

19. The system of any of Claims 16-18, wherein the virtualized protected area of memory is a cloud vault.

20. The system of any of Claims 19-20, wherein a filter driver controls input and output access to the virtualized protected area of memory.

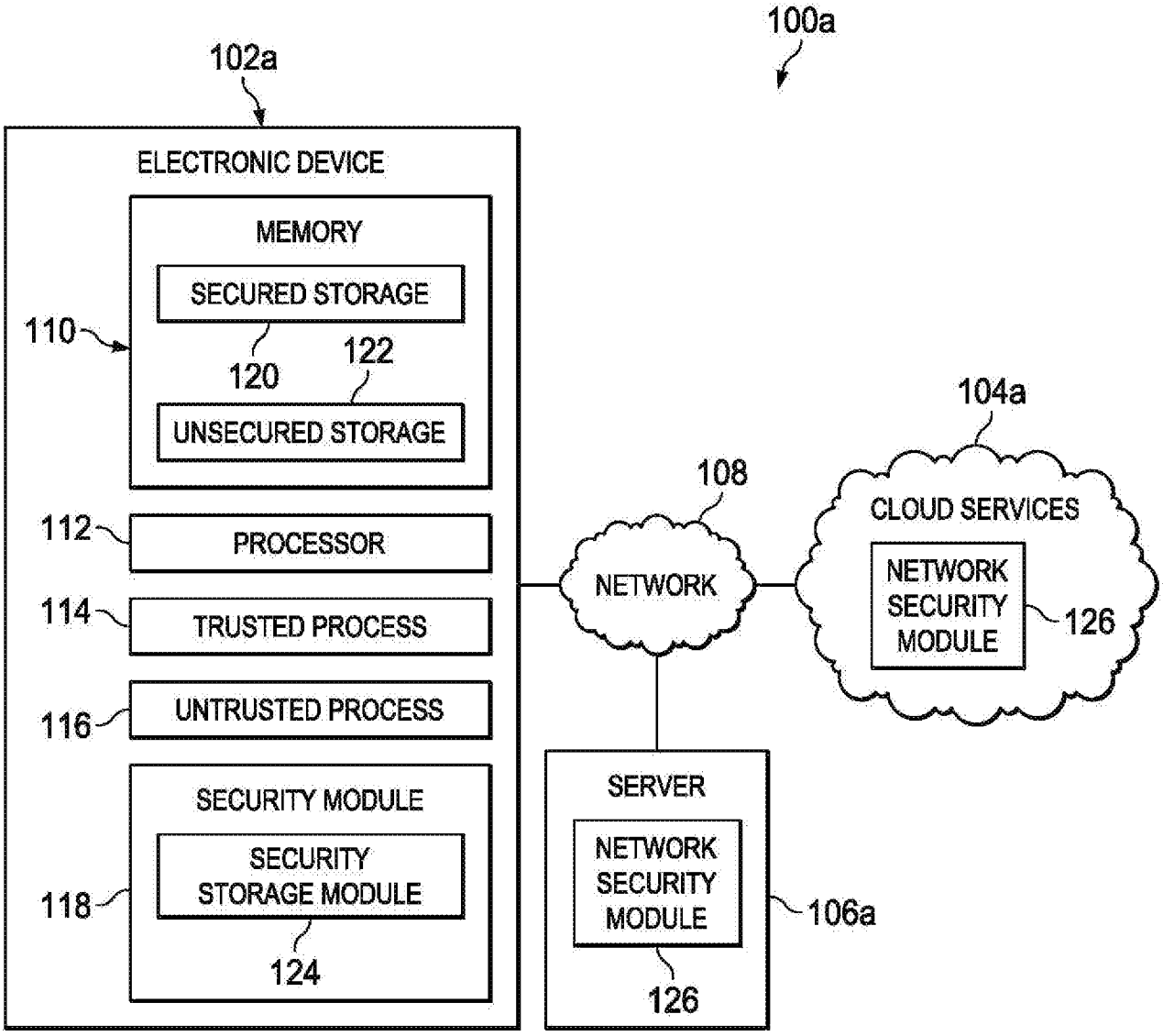

100a
102a
ELECTRONIC DEVICE
MEMORY
SECURED STORAGE
110
120
122
UNSECURED STORAGE
112
PROCESSOR
114
TRUSTED PROCESS
116
UNTRUSTED PROCESS
SECURITY MODULE
SECURITY STORAGE MODULE
118
124
108
NETWORK
104a
CLOUD SERVICES
NETWORK SECURITY MODULE
126
SERVER
NETWORK SECURITY MODULE
126
106a

FIG. 1A

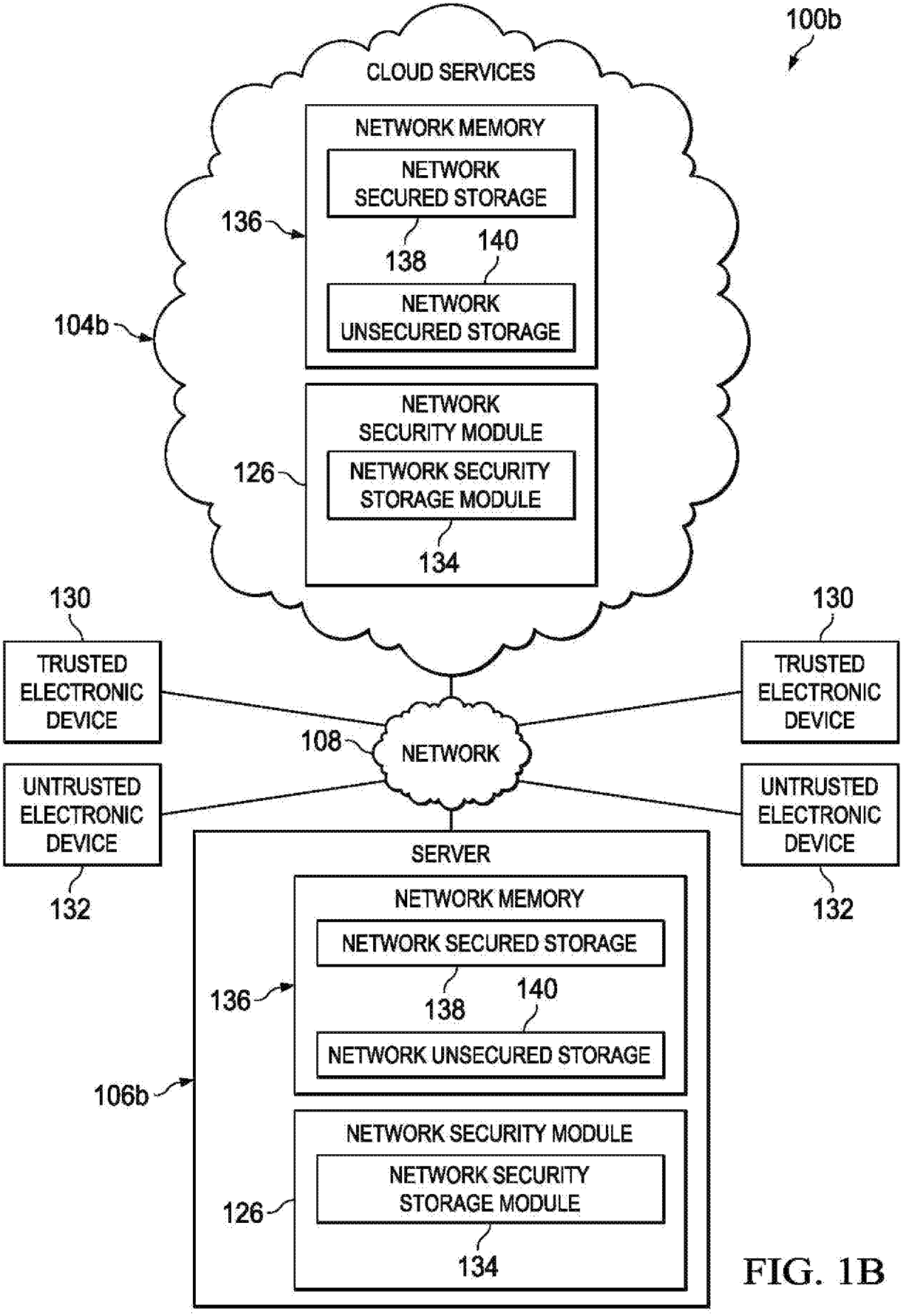

100b
CLOUD SERVICES
NETWORK MEMORY
NETWORK SECURED STORAGE
136
138
140
NETWORK UNSECURED STORAGE
104b
NETWORK SECURITY MODULE
126
NETWORK SECURITY STORAGE MODULE
134
130
TRUSTED ELECTRONIC DEVICE
130
TRUSTED ELECTRONIC DEVICE
108
NETWORK
UNTRUSTED ELECTRONIC DEVICE
UNTRUSTED ELECTRONIC DEVICE
132
132
SERVER
NETWORK MEMORY
NETWORK SECURED STORAGE
136
138
140
NETWORK UNSECURED STORAGE
106b
NETWORK SECURITY MODULE
NETWORK SECURITY STORAGE MODULE
126
134

FIG. 1B

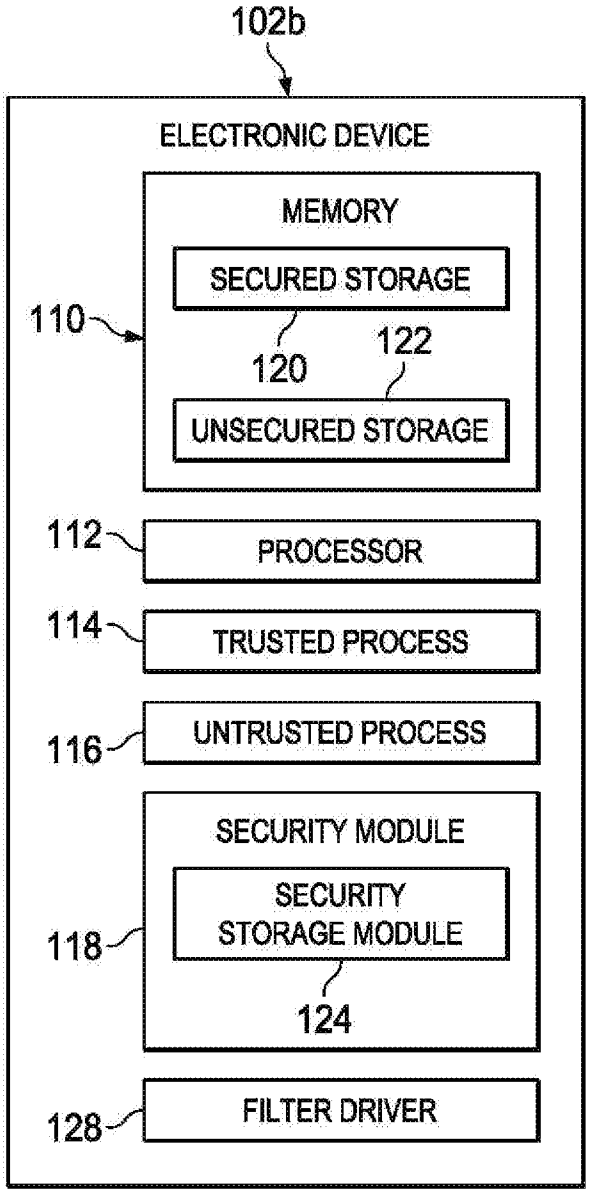

102b
ELECTRONIC DEVICE
MEMORY
SECURED STORAGE
110
120
122
UNSECURED STORAGE
112
PROCESSOR
114
TRUSTED PROCESS
116
UNTRUSTED PROCESS
SECURITY MODULE
SECURITY STORAGE MODULE
118
124
128
FILTER DRIVER

FIG. 2

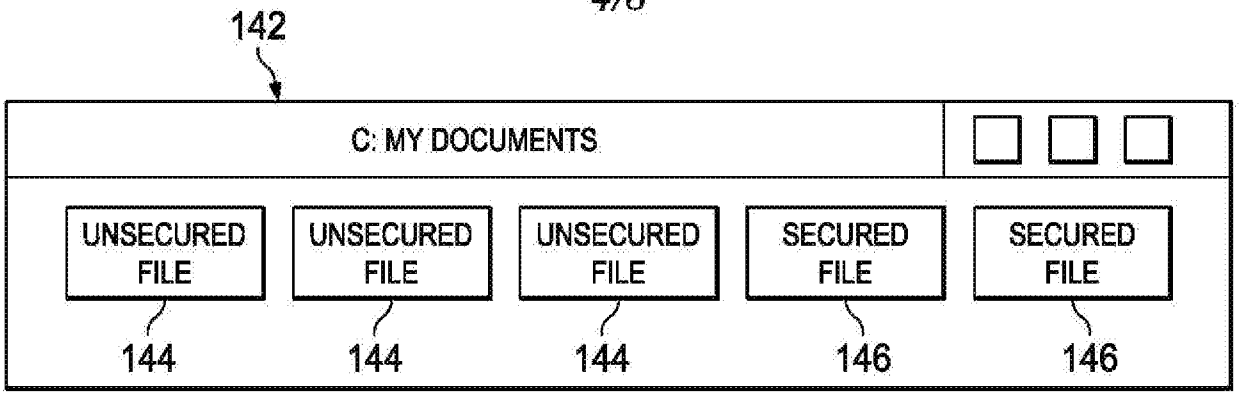


FIG. 3A

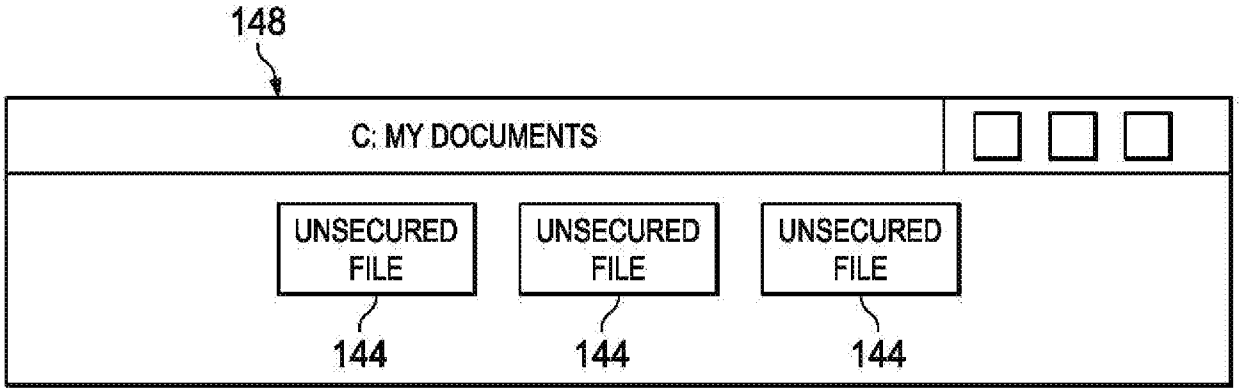


FIG. 3B

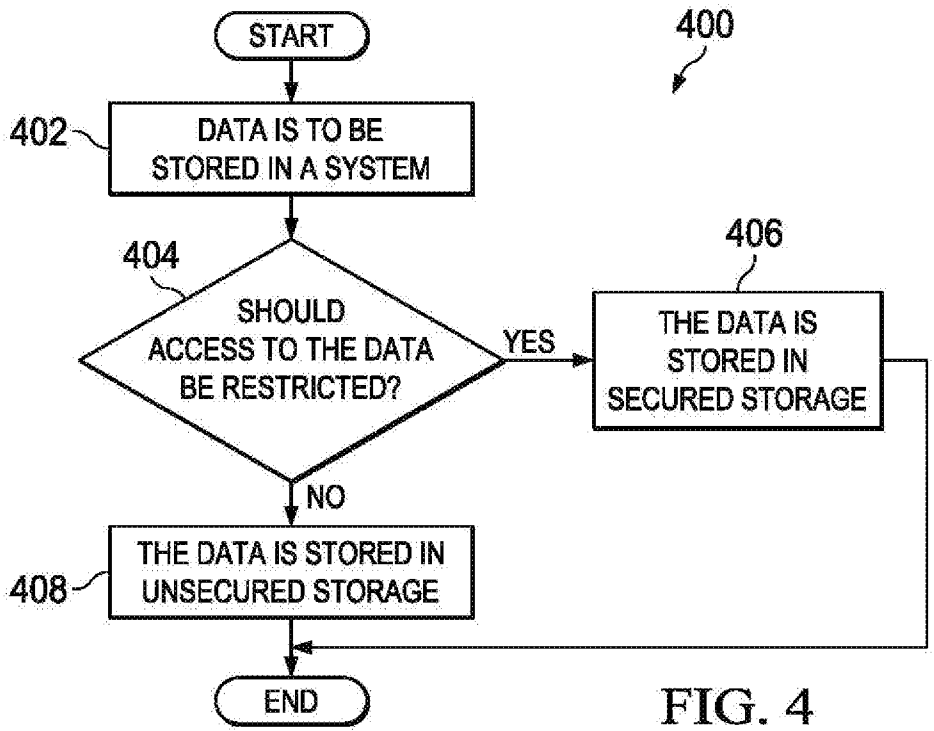


FIG. 4

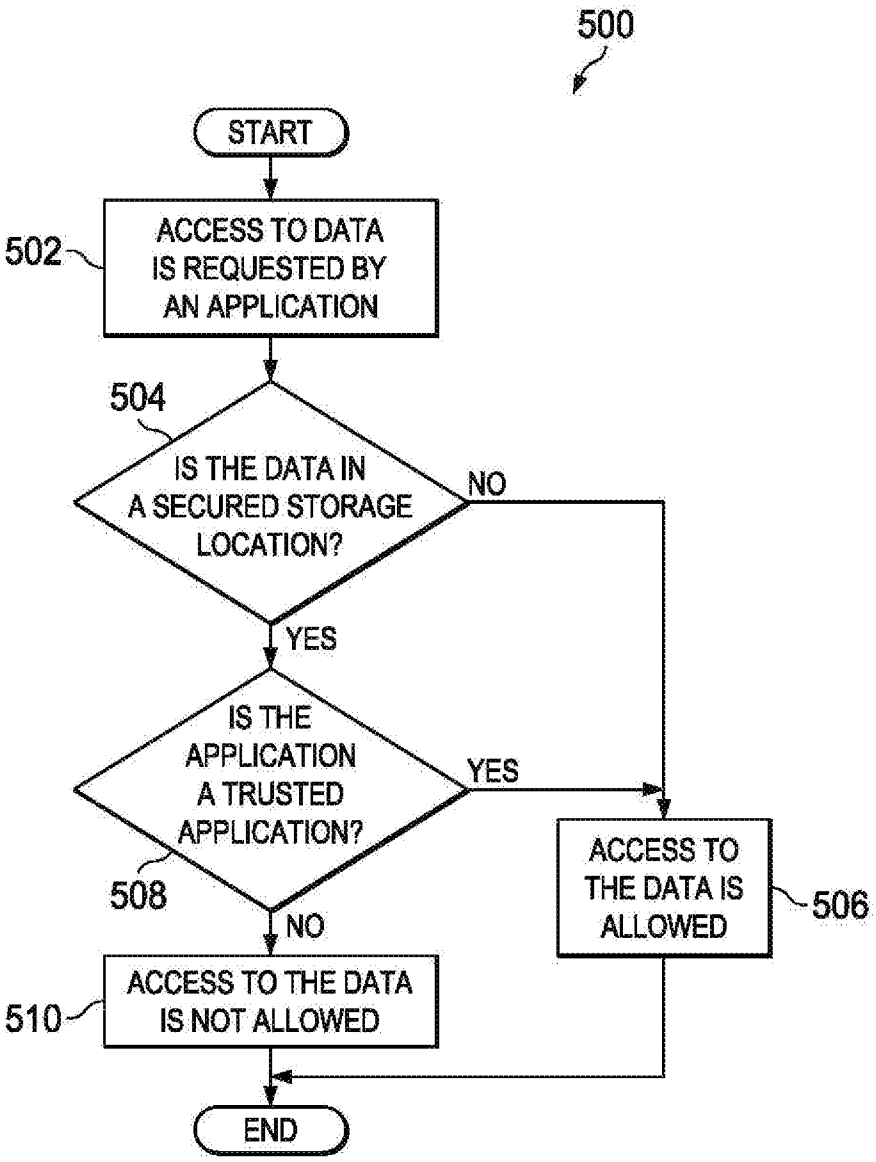

500
START
502
ACCESS TO DATA IS REQUESTED BY AN APPLICATION
504
IS THE DATA IN A SECURED STORAGE LOCATION?
NO
YES
IS THE APPLICATION A TRUSTED APPLICATION?
YES
508
NO
ACCESS TO THE DATA IS ALLOWED
506
510
ACCESS TO THE DATA IS NOT ALLOWED
END

FIG. 5

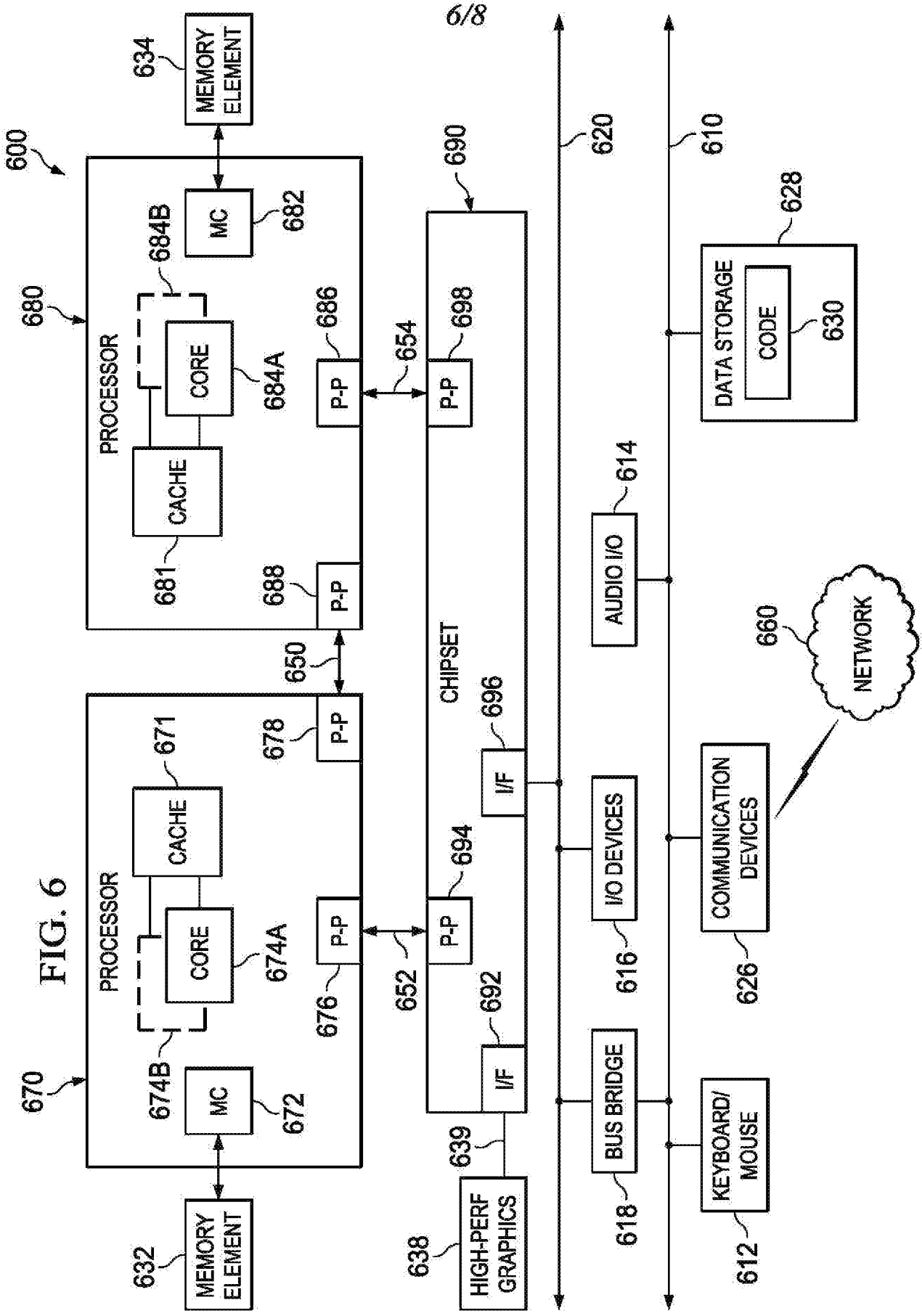
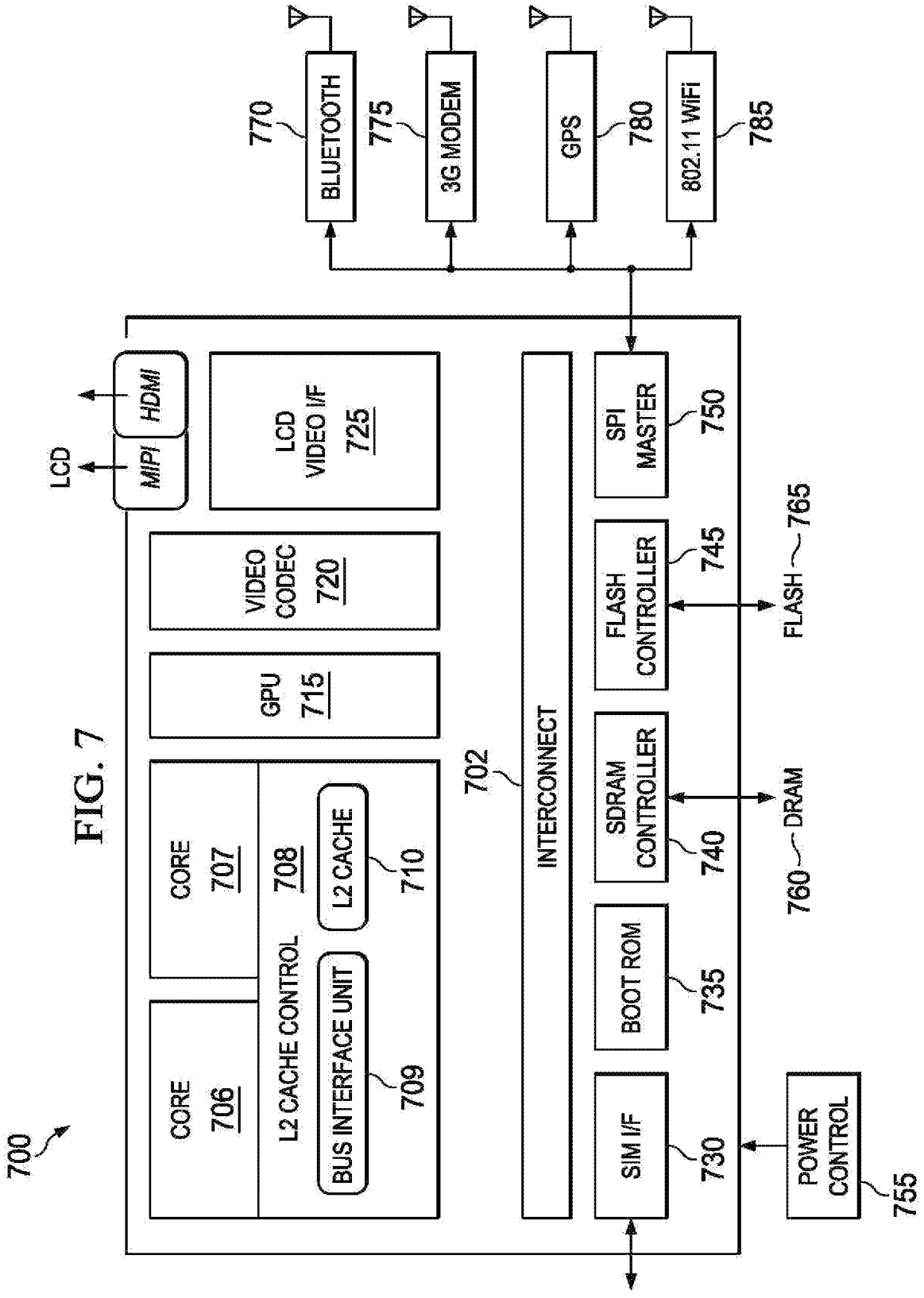

600
634
MEMORY ELEMENT
680
PROCESSOR
684B
MC
682
CORE
684A
CACHE
681
686
P-P
688
P-P
654
650
690
P-P
698
CHIPSET
696
I/F
694
P-P
692
I/F
639
638
HIGH-PERF GRAPHICS
652
676
P-P
678
P-P
670
PROCESSOR
671
CACHE
CORE
674A
674B
MC
672
632
MEMORY ELEMENT
620
610
628
DATA STORAGE
CODE
630
614
AUDIO I/O
660
NETWORK
616
I/O DEVICES
626
COMMUNICATION DEVICES
618
BUS BRIDGE
612
KEYBOARD/ MOUSE

FIG. 6

FIG. 7


700
LCD
HDMI
MIPI
LCD VIDEO I/F 725
VIDEO CODEC 720
GPU 715
CORE 706
CORE 707
L2 CACHE CONTROL 708
BUS INTERFACE UNIT 709
L2 CACHE 710
702
INTERCONNECT
SPI MASTER 750
FLASH CONTROLLER 745
FLASH 765
SDRAM CONTROLLER 740
DRAM 760
BOOT ROM 735
SIM I/F 730
POWER CONTROL 755
770 BLUETOOTH
775 3G MODEM
780 GPS
785 802.11 WiFi

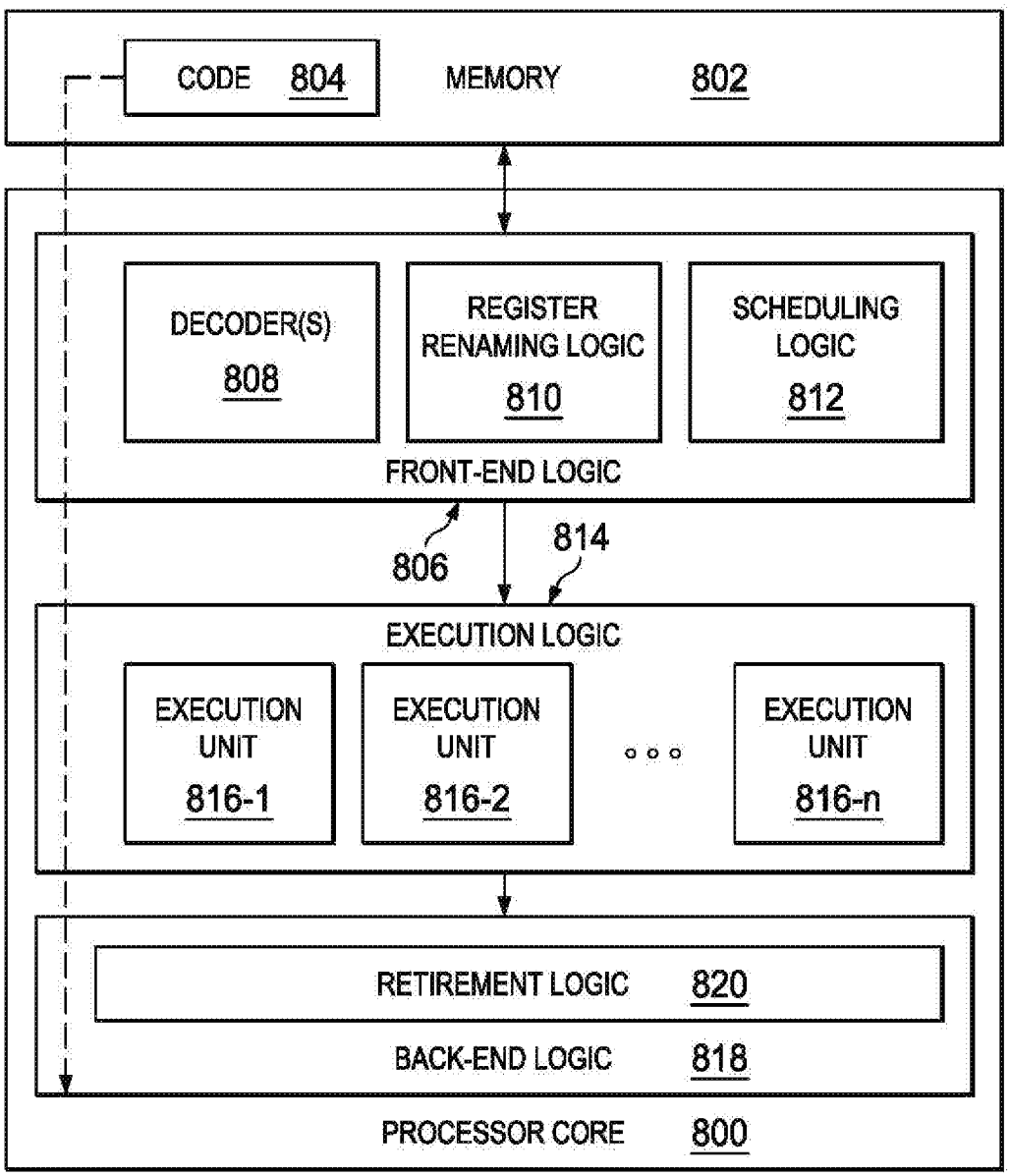

CODE 804
MEMORY 802
DECODER(S) 808
REGISTER RENAMING LOGIC 810
SCHEDULING LOGIC 812
FRONT-END LOGIC
806
814
EXECUTION LOGIC
EXECUTION UNIT 816-1
EXECUTION UNIT 816-2
EXECUTION UNIT 816-n
RETIREMENT LOGIC 820
BACK-END LOGIC 818
PROCESSOR CORE 800

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/033854

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/79(2013.01)I, G06F 21/62(2013.01)I, G06F 21/60(2013.01)I, G06F 9/455(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)
G06F 21/79; H04L 9/08; G06F 12/00; G06F 12/14; H04L 9/32; G06F 21/62; G06F 21/60; G06F 9/455

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:protected area, virtualized, authorized, memory

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008-0256322 A1 (YU-AN CHANG et al.) 16 October 2008 See paragraphs [0007], [0032]-[0036]; claims 11, 17; and figures 3A, 3B.	1-20
Y	US 8156298 B1 (ADAM STUBBLEFIELD) 10 April 2012 See column 5, lines 41-42, column 6, lines 22-25; and figure 1.	1-20
A	US 2010-0169667 A1 (PRASHANT DEWAN) 01 July 2010 See claims 1-3; and figures 2-3.	1-20
A	US 2007-0005919 A1 (HENRI HAN VAN RIEL) 04 January 2007 See abstract; claim 1; and figure 4.	1-20
A	US 2002-0133702 A1 (CURTIS E. STEVENS) 19 September 2002 See claim 1; and figure 4.	1-20

☐ 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	Date of mailing of the international search report
06 September 2016 (06.09.2016)	**06 September 2016 (06.09.2016)**

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
CHIN, Sang Bum
Telephone No. +82-42-481-8398

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2016/033854

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0256322 A1	16/10/2008	US 7900012 B2	01/03/2011
US 8156298 B1	10/04/2012	None	
US 2010-0169667 A1	01/07/2010	CN 101894224 A	24/11/2010
		CN 101894224 B	18/03/2015
		EP 2207121 A1	14/07/2010
		EP 2207121 B1	20/03/2013
		JP 2010-157224 A	15/07/2010
		JP 2012-181862 A	20/09/2012
		KR 10-1158184 B1	20/06/2012
		KR 10-20100080405 A	08/07/2010
		US 8213618 B2	03/07/2012
US 2007-0005919 A1	04/01/2007	US 8856473 B2	07/10/2014
		WO 2007-005718 A2	11/01/2007
		WO 2007-005718 A3	16/04/2009
US 2002-0133702 A1	19/09/2002	None	