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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 June 2016 (30.06.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/105826 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2015/062597

(22) International Filing Date:
25 November 2015 (25.11.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/581,965 23 December 2014 (23.12.2014) 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). **TEDDY, John, D.**; 11370 NW Skyline Blvd, Portland, OR 97231 (US).

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD TO COMBINE MULTIPLE REPUTATIONS

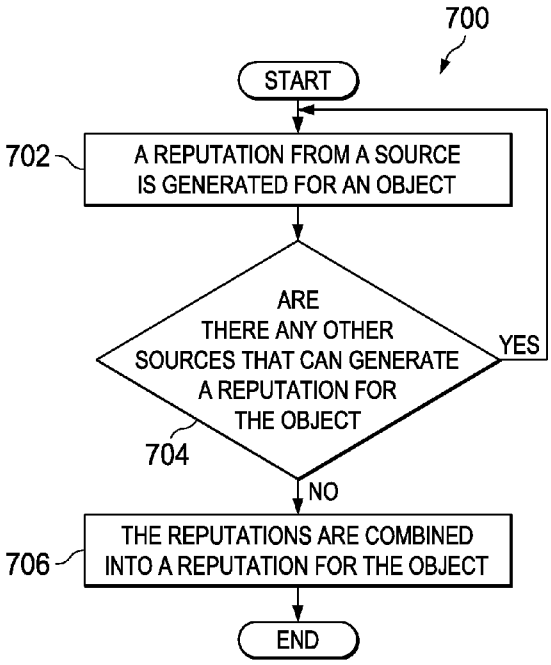


FIG. 7

(57) Abstract: Particular embodiments described herein provide for an electronic device that can be configured to acquire a plurality of reputations related to an object and combine the plurality of reputations to create a total reputation for the object. The object can include a plurality of sub-objects and each of the plurality of reputations can correspond to one of the sub-objects.

WO 2016/105826 A1

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))*

SYSTEM AND METHOD TO COMBINE MULTIPLE REPUTATIONS

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of and priority to U.S. Non-Provisional Patent Application No. 14/581,965 filed 23 December 2014 entitled "SYSTEM AND METHOD TO COMBINE MULTIPLE REPUTATIONS", 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 combine multiple reputations.

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. One system for protecting computers and computer networks includes assigning a reputation to process 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 1 is a simplified block diagram of a communication system to combine multiple reputations in accordance with an embodiment of the present disclosure;

[0007] FIGURE 2 is a simplified block diagram of example details of a communication system to combine multiple reputations in accordance with an embodiment of the present disclosure;

[0008] FIGURE 3 is a simplified block diagram of example details of a portion of a communication system to combine multiple reputations in accordance with an embodiment of the present disclosure;

[0009] FIGURE 4 is a simplified block diagram of example details of a communication system to combine multiple reputations in accordance with an embodiment of the present disclosure;

[0010] FIGURE 5 is a simplified flowchart illustrating potential operations that may be associated with the communication system in accordance with an embodiment;

[0011] FIGURE 6 is a simplified flowchart illustrating potential operations that may be associated with the communication system in accordance with an embodiment;

[0012] FIGURE 7 is a simplified flowchart illustrating potential operations that may be associated with the communication system in accordance with an embodiment;

[0013] FIGURE 8 is a block diagram illustrating an example computing system that is arranged in a point-to-point configuration in accordance with an embodiment;

[0014] FIGURE 9 is a simplified block diagram associated with an example ARM ecosystem system on chip (SOC) of the present disclosure; and

[0015] FIGURE 10 is a block diagram illustrating an example processor core in accordance with an embodiment.

[0016] 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

[0017] FIGURE 1 is a simplified block diagram of a communication system 100 to combine multiple reputations in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 1, an embodiment of communication system 100 can include electronic devices 102a–102d, a server 104, and a cloud 106. Electronic device 102a can include a local network reputation module 112a. Each electronic device 102a–102d can include memory 114a-d respectively and a processor 116a-d respectively. Server 104 can include memory 114e, a processor 116e, and a network reputation module 118a. Memory 114e can include network data 136. Cloud 106 can include memory 114f, a processor 116f, and a network reputation module 118b. Electronic device 102a, server 104, and cloud 106 may be in communication using network 108. Electronic devices 102a–102d may be in communication using local network 110a.

[0018] In example embodiments, communication system 100 can be configured to combine multiple reputations in accordance with an embodiment of the present disclosure. Local network reputation module 112a can be configured to acquire a plurality of reputations related to an object and combine the plurality of reputations to create a total reputation for the object. The object can include a plurality of sub-objects and each of the plurality of reputations can correspond to one of the sub-objects. In an example, a Bayesian algorithm may be used to combine the multiple reputations.

[0019] Elements of FIGURE 1 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, local network 110a, etc.) communications. Additionally, any one or more of these elements of FIGURE 1 may be combined or removed from the architecture based on particular configuration needs. Communication system 100 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 100 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 system 100, 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 device and network reputations can generate a reputation for an object or generate a finding that can be converted into a reputation. However, existing solutions primarily rely on determining the reputation using updatable content and do not allow for an efficient system to combine multiple reputations. The existing solutions require frequent updates to content in order to determine a reputation. This can be expensive to sustain, virtually impossible for end user reputations, and cannot meet the target functionality for customer reputation sources. What is needed is the ability to determine a reputation and include arbitrary end user generated reputations not visible on the backend.

[0022] A communication system for combining multiple reputations, as outlined in FIGURE 1, can resolve these issues (and others). Communication system 100 may be configured to use probabilistic math with an external weight and confidence normalizing values to achieve a final reputation. A series of flags may be used to identify appropriate remediation for the final reputation. A reputation can be mapped to a trust score (0-100) and may include a series of attributes associated with that reputation. For example, a reputation can include, a backend reputation, a service provider reputation, and an external reputation.

[0023] Backend reputations can include reputations that are provided by the backend of the system (e.g., server 104 and cloud 106). The backend reputations can include, but are not limited to, a server enterprise reputation, global threat reputations for file, cert, URL reputations, anti-virus scan engine reputations, zero-day reputations, etc.

[0024] Service provider reputations can include reputations that are provided in content from the service provider. The service provider reputations could come from any scanner or module which provides reputation related data, such as Raptor, JTI rules, anti-virus engine, DATs, host intrusion prevention system rules, etc.

[0025] External reputations are reputations which are defined by end users or systems used by end users and not provided by the backend. External reputations may be

referred to as end user or customer reputations. When an end user or an electronic device associated with an end user creates a custom reputation type, the custom reputation type will need at minimum a trust score and the trust score can be calculated by code. For example, external anti-virus and parsing detection can be used to determine threshold level reputations as an output (e.g., known malicious for confirmed detections, most likely malicious for heuristics, etc.). Also, the trust score can be, at least partially, determined as part of an import scheme (e.g., all hashes imported from a specific feed could be considered most likely malicious).

[0026] The following is example of data that may be used to allow a reputation to be interpreted by a generic rule. A trust score can be a numeric value 0-100 and is the reputation score. A reputation confidence can be a numeric value 00.0-1.0 and represents how much a particular reputation is trusted. Reputation weight can be a numeric value 0.0-1.0 and represents how important the reputation is to the final results.

[0027] An external customer reputation can be many different things and can include firewall, OPENIOC sources, third party anti-virus scanners, etc. For external reputations, especially those from machine learning, the weight and confidence values could be determined by considering not only the confidence that the model produces the correct classification in context, but also the attributes source reputation. Note that a model may produce a different reputation confidence each time it is rebuilt. Thus, the reputation confidence may change over time for a given source. For instance, if a particular machine learning model uses attributes from multiple reputation sources, the confidence and weight could be an average of the individual confidence and weight values from the reputations which source the attributes.

[0028] Regarding the end user, or end user electronic device, a generic rule is required to interpret the various reputations provided by the electronic device, the server or cloud, as well as local scanners. A Bayesian algorithm approach with flags to control when a repair is applied may be used to interpret the various reputations. Bayesian math works very efficiently to combine multiple independent classifiers (in this case reputations) to determine a final class and probability of a class. In an example, reputations can range from 0-100 for the explicit purpose of being able to be used in probabilistic math. Note that one can convert any arbitrary scale to the 0-100 scale easily enough and a 0-199 scale can

produce superior results to a weight based algorithm almost all the time. The Bayesian algorithm is only used as an illustrative example and other algorithms may be used and are within the scope of this disclosure.

[0029] In a specific example, an initial probability of maliciousness can be defined as Pim = 0.2 (note that the probability of maliciousness can be defined as any number and for this example, is defined as a number between 0.0 and 1.0). The initial probability of trusted can be defined as Pit = 0.8 (note that the initial probability of trust can be defined as any number and for this example, is defined as a number between 0.0 and 1.0). For each reputation (e.g., backend reputation, service provider reputation, external reputation, etc.), a reputation trust score can be defined as R, the confidence as C, and the weight a W. The probability of maliciousness can be calculated as (Pm) = ((100-(R*C*W))/100). The probability of trusted can be calculated as (Pt) = (R/100)*C*W. The new initial probability of maliciousness will be (Pim*Pm)/((Pim*Pm)+(Pit*Pt)). The new initial probability of trusted will be (Pit*Pt)/((Pim*Pm)+(Pit*Pt))

[0030] In another example, if a system has a global threat file reputation of 70 and a confidence of 1.0, then Pm = 0.3 (1.0 – 0.7) and Pt = 0.7 (1.0 X 0.7). Given the initial probabilities, the final probabilities are Pim = 0.0967 and Pit = 0.9032. This means that there is roughly a 90% chance that the file can be trusted. The final local reputation (Rl) value can be mapped from the probabilities back to the reputation ranges as follows: if Pic is greater than Pit then Rl is set to 100; if Pic is not greater than Pit, then RI is set equal to Pit*100 (i.e., if Pic > Pit then 100; else Pit * 100). While the initial probability values of 0.2 and 0.8 are used in the above examples, any rational number between 0.00 and 1.00 can be selected. Likewise, the reputation confidence and weight could exceed 1.00, although should not be less than 0.00.

[0031] Flags can be set for an object, file, or data and determine if general remediation or repair to the object, file, or data is allowed (e.g., NO_FLAGS=0, ALLOW_REPAIR=1, DISALLOW_REPAIR=2, DISALLOW_BLOCK=3, etc.). For example, if an allow repair flag is set, then general remediation will be allowed if the external reputation agrees with the final reputation score. More specifically, if the final result is malicious and the policy allows general remediation for that reputation level and the reputation is also malicious, then general remediation will be allowed. If a disallow repair flag is set, then a

general remediation would be prevented if the external reputation agrees with the final result and blocking may occur. If a disallow block flag is set, then a block would be prevented or not allowed if the external reputation agrees with the final result. If a block is triggered but the disallow block flag is sent, then a prompt action or an alert could be issued. In a specific example, where the object for which a reputation is being calculated is a file or is a process, general remediation such as removing the file from memory or terminating the process can be determined using flags.

[0032] Repair is determined for each reputation. If R<Unknown&&Rl<Unknown then the flags of that reputation are applied to the final repair status and determined by comparing the flags of the reputation (R) with the final local reputation (Rl). After each reputation has been examined, if the final repair status has the DISALLOW_REPAIR flag set, repair will be explicitly denied. Otherwise if it has the ALLOW_REPAIR flag set, repair will be enabled. The DISALLOW_BLOCK flag will prevent blocking and implicitly repair. If no flag is set, then repair will not occur. The above values used for the flags are merely illustrative examples and other similar examples could be used.

[0033] Turning to the infrastructure of FIGURE 1, communication system 100 in accordance with an example embodiment is shown. Generally, communication system 100 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 system 100. 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. Local network 110a represents a series of points or nodes of interconnected communication paths for receiving and transmitting packets of information that propagate through electronic devices 102a-102d. Local network 110a offers a communicative interface between nodes, and may be configured as any local area network (LAN), virtual local area network (VLAN), 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.

[0034] In communication system 100, 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 system 100. Suitable interfaces and infrastructure may be provided to enable communication with the cellular network.

[0035] 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.

[0036] In an example implementation, electronic devices 102a-d, server 104, and cloud 106 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.

[0037] In regards to the internal structure associated with communication system 100, each of electronic devices 102a-d, server 104, and cloud 106 can include memory

elements (e.g., memory 114a-114f) for storing information to be used in the operations outlined herein. Each of electronic devices 102a-d, server 104, and cloud 106 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 system 100 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.

[0038] 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.

[0039] In an example implementation, network elements of communication system 100, such as electronic devices 102a-d, server 104, and cloud 106 may include software modules (e.g., local network reputation module 112a and network reputation module 118a and 118b) 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.

[0040] Additionally, each of electronic devices 102a-d, server 104, and cloud 106 may include a processor (e.g., processor 116a-116f) 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.'

[0041] Electronic devices 102a-d can each be a network element and includes, for example, desktop computers, laptop computers, mobile devices, personal digital assistants, smartphones, tablets, or other similar devices. Server 104 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 systems 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 system 100. Although local network reputation module 112a is represented in FIGURE 1 as being located in electronic device 102a, this is for illustrative purposes only. Local network reputation module 112a could be combined or separated in any suitable configuration. Furthermore, local network reputation module 112a could be integrated with or distributed in another network accessible by electronic devices 102a-d such as server 104 or cloud 106. Cloud 106 is configured to provide cloud services to electronic devices 102a-d. 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.

[0042] Turning to FIGURE 2, FIGURE 2 is a simplified block diagram of a portion of a communication system 100 to combine multiple reputations in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 2, each electronic device 102a-102c can include a device reputation module 120a-120c respectively. Device reputation modules 120a-120c can be configured to determine a reputation for the device where the device reputation module is located. For example, device reputation module 120a can be configured to determine the reputation for electronic device 102a, device reputation module 120b can be configured to determine the reputation for electronic device 102b, and device reputation module 120c can be configured to determine the reputation for electronic device 102c. Electronic device 102d is illustrated as not including a reputation module and the system can be configured to include a plurality of electronic devices that do not include a reputation data module. In such an example, local network reputation module 112a can be configured to determine the reputation for electronic device 102d using data or information related to electronic device 102d. For example, local network reputation module 112a may determine the reputation of electronic device by using the data that flows to and from electronic device 102d, the connections to and from electronic device 102d, the type of electronic device 102d, etc. Each device reputation module 120a-120c can be configured to communicate the determined reputation to local network reputation module 112a where a reputation of electronic devices 102a-102d as a group can be determined.

[0043] Turning to FIGURE 3, FIGURE 3 is a simplified block diagram of a portion of a communication system 300 to combine multiple reputations in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 3, electronic device 102b can include memory 114b, processor 116b, device reputation module 120b, process reputation module 122, and one or more process 124a -124c. Memory 116b can include loaded libraries 136. Process 124a can include loaded process library 126, main executable code 128, executing code 130, interpreted content 132, and data 134. Each process 124b and 124c can include the same or similar elements as illustrated in process 124a. Similarly, each of the other electronic devices 102a, 102c, and 102d can include the same or similar elements as illustrated in electronic device 102b in FIGURE 3.

[0044] Process reputation module 122 can be configured to determine a reputation for each process 124a-124c. For example, process reputation module 122 can determine or receive a reputation for loaded process library 126, main executable code 128, executing code 130, interpreted content 132, and data 134 and combine those reputations into a reputation for process 124a. Loaded process library 126, main executable code 128, executing code 130, interpreted content 132, and data 134 are provided as an illustrative example only and any combination may be used to determine a reputation for process 124a or other examples may be used to determine a reputation for process 124a. Also, process reputation module 122 can use a similar means of determining a reputation for processes 124b and 124c. Device reputation module 120b can be configured to determine a reputation for electronic device 102b by combining the reputation of each process 124a-124c as well as other reputations related to electronic device 102b.

[0045] Turning to FIGURE 4, FIGURE 4 is a simplified block diagram of communication system 100 to combine multiple reputations in accordance with an embodiment of the present disclosure. As illustrated in FIGURE 4, communication system can include electronic devices 102a-102i. Electronic device 102a-102d may be grouped or linked together through local network 110a. Electronic devices 102e-102g may be grouped or linked together through a local network 110b. Electronic devices 102h and 102i may be grouped or linked together through a local network 110c. Each electronic device 102a-102i can include a device reputation module 120a-120i respectively. As discuss above with reference to electronic device 102b in FIGURE 3, device reputation module 120b can be configured to determine a reputation for electronic device 102b. Similarly, each device reputation module 120a and 120c-120i can be configured to determine a reputation for electronic device 102a and 120c-120i respectively. Further, as discussed above, local network reputation module 112a can be configured to determine a reputation for electronic devices 102a-102d as a group. Electronic device 102e can include a local network reputation module 112b and local network reputation module 112b can be configured to determine a reputation for electronic devices 102e-102g as a group. Also, electronic device 102h can include a local network reputation modules 112c and local network reputation module 112c can be configured to determine a reputation for electronic devices 102h and 102i as a group. Local network reputation modules 112a-112c can communicate the

determined reputation for their respective group to network reputation module 118a and 118b. Network reputation modules 118a and 118b can be configured to use the reputations communicated from local network reputation modules 112a-112c and determine a reputation for communication system 100.

[0046] Turning to FIGURE 5, FIGURE 5 is an example flowchart illustrating possible operations of a flow 500 that may be associated with combining multiple reputations, in accordance with an embodiment. In an embodiment, one or more operations of flow 500 may be performed by local network reputation modules 112a-112c, network reputation module 118a and 118b, and device reputation module 120a-i. At 502, a reputation for an electronic device connected to a local network is determined. At 504, the determined reputation is communicated to an electronic device that includes a local network reputation module. At 506, the electronic device that includes the local network reputation module receives determined reputations from other electronic devices connected to the local network. At 508, a local network reputation is determined.

[0047] Turning to FIGURE 6, FIGURE 6 is an example flowchart illustrating possible operations of a flow 600 that may be associated with combining multiple reputations, in accordance with an embodiment. In an embodiment, one or more operations of flow 600 may be performed by local network reputation modules 112a-112c, network reputation module 118a and 118b, and device reputation module 120a-i. At 602, a local reputation is determined for a local network. At 604, the determined local network reputation is communicated to a network electronic device that includes a network reputation module. At 606, the network electronic device that includes the network reputation module receives determined local network reputations from other local networks. At 608, a network reputation is determined.

[0048] Turning to FIGURE 7, FIGURE 7 is an example flowchart illustrating possible operations of a flow 700 that may be associated with combining multiple reputations, in accordance with an embodiment. In an embodiment, one or more operations of flow 700 may be performed by local network reputation modules 112a-112c, network reputation module 118a and 118b, and device reputation module 120a-i. At 702, a reputation from a source is generated for an object. At 704, the system determines if there are any other sources that can generate a reputation for the object. If there are any other sources that

can generate a reputation for the object, then a reputation from the source (i.e., the other source) is generated for the object, as in 702. If there are not any other sources than can generate a reputation for the object, then the reputations are combined into a reputation for the object, as in 706. Using this process, a reputation for an object can be created or determined using multiple sources.

[0049] FIGURE 8 illustrates a computing system 800 that is arranged in a point-to-point (PtP) configuration according to an embodiment. In particular, FIGURE 8 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 system 10 may be configured in the same or similar manner as computing system 800.

[0050] As illustrated in FIGURE 8, system 800 may include several processors, of which only two, processors 870 and 880, are shown for clarity. While two processors 870 and 880 are shown, it is to be understood that an embodiment of system 800 may also include only one such processor. Processors 870 and 880 may each include a set of cores (i.e., processor cores 874A and 874B and processor cores 884A and 884B) 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 1-7. Each processor 870, 880 may include at least one shared cache 871, 881. Shared caches 871, 881 may store data (e.g., instructions) that are utilized by one or more components of processors 870, 880, such as processor cores 874 and 884.

[0051] Processors 870 and 880 may also each include integrated memory controller logic (MC) 872 and 882 to communicate with memory elements 832 and 834. Memory elements 832 and/or 834 may store various data used by processors 870 and 880. In alternative embodiments, memory controller logic 872 and 882 may be discrete logic separate from processors 870 and 880.

[0052] Processors 870 and 880 may be any type of processor and may exchange data via a point-to-point (PtP) interface 850 using point-to-point interface circuits 878 and 888, respectively. Processors 870 and 880 may each exchange data with a chipset 890 via individual point-to-point interfaces 852 and 854 using point-to-point interface circuits 876, 886, 894, and 898. Chipset 890 may also exchange data with a high-performance graphics

circuit 838 via a high-performance graphics interface 839, using an interface circuit 892, which could be a PtP interface circuit. In alternative embodiments, any or all of the PtP links illustrated in FIGURE 8 could be implemented as a multi-drop bus rather than a PtP link.

[0053] Chipset 890 may be in communication with a bus 820 via an interface circuit 896. Bus 820 may have one or more devices that communicate over it, such as a bus bridge 818 and I/O devices 816. Via a bus 810, bus bridge 818 may be in communication with other devices such as a keyboard/mouse 812 (or other input devices such as a touch screen, trackball, etc.), communication devices 826 (such as modems, network interface devices, or other types of communication devices that may communicate through a computer network 860), audio I/O devices 814, and/or a data storage device 828. Data storage device 828 may store code 830, which may be executed by processors 870 and/or 880. In alternative embodiments, any portions of the bus architectures could be implemented with one or more PtP links.

[0054] The computer system depicted in FIGURE 8 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 8 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.

[0055] Turning to FIGURE 9, FIGURE 9 is a simplified block diagram associated with an example ARM ecosystem SOC 900 of the present disclosure. At least one example implementation of the present disclosure can include the combination of multiple reputations features discussed herein and an ARM component. For example, the example of FIGURE 9 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.

[0056] In this example of FIGURE 9, ARM ecosystem SOC 900 may include multiple cores 906-907, an L2 cache control 908, a bus interface unit 909, an L2 cache 910, a graphics processing unit (GPU) 915, an interconnect 902, a video codec 920, and a liquid crystal display (LCD) I/F 925, which may be associated with mobile industry processor interface (MIPI)/ high-definition multimedia interface (HDMI) links that couple to an LCD.

[0057] ARM ecosystem SOC 900 may also include a subscriber identity module (SIM) I/F 930, a boot read-only memory (ROM) 935, a synchronous dynamic random access memory (SDRAM) controller 940, a flash controller 945, a serial peripheral interface (SPI) master 950, a suitable power control 955, a dynamic RAM (DRAM) 960, and flash 965. In addition, one or more example embodiments include one or more communication capabilities, interfaces, and features such as instances of Bluetooth™ 970, a 3G modem 975, a global positioning system (GPS) 980, and an 802.11 Wi-Fi 985.

[0058] In operation, the example of FIGURE 9 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.

[0059] FIGURE 10 illustrates a processor core 1000 according to an embodiment. Processor core 1000 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 1000 is illustrated in Figure 10, a processor may alternatively include more than one of the processor core 1000 illustrated in Figure 10. For example, processor core 1000 represents one example embodiment of processors cores 874a, 874b, 884a, and 884b shown and described with reference to processors 870 and 880 of FIGURE 8. Processor core 1000 may be a single-threaded core or, for at least one embodiment, processor core 1000 may be multithreaded in that it may include more than one hardware thread context (or “logical processor”) per core.

[0060] FIGURE 10 also illustrates a memory 1002 coupled to processor core 1000 in accordance with an embodiment. Memory 1002 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 1002 may include code 1004, which may be one or more instructions, to be executed by processor core 1000. Processor core 1000 can follow a program sequence of instructions indicated by code 1004. Each instruction enters a front-end logic 1006 and is processed by one or more decoders 1008. 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 1006 also includes register renaming logic 1010 and scheduling logic 1012, which generally allocate resources and queue the operation corresponding to the instruction for execution.

[0061] Processor core 1000 can also include execution logic 1014 having a set of execution units 1016-1 through 1016-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 1014 performs the operations specified by code instructions.

[0062] After completion of execution of the operations specified by the code instructions, back-end logic 1018 can retire the instructions of code 1004. In one embodiment, processor core 1000 allows out of order execution but requires in order retirement of instructions. Retirement logic 1020 may take a variety of known forms (e.g., re-order buffers or the like). In this manner, processor core 1000 is transformed during execution of code 1004, at least in terms of the output generated by the decoder, hardware registers and tables utilized by register renaming logic 1010, and any registers (not shown) modified by execution logic 1014.

[0063] Although not illustrated in FIGURE 10, a processor may include other elements on a chip with processor core 1000, at least some of which were shown and described herein with reference to FIGURE 8. For example, as shown in FIGURE 8, a processor may include memory control logic along with processor core 1000. The processor may include I/O control logic and/or may include I/O control logic integrated with memory control logic.

[0064] 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 system 10 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 system 10 as potentially applied to a myriad of other architectures.

[0065] It is also important to note that the operations in the preceding flow diagrams (i.e., FIGURES 3-7) illustrate only some of the possible correlating scenarios and patterns that may be executed by, or within, communication system 100. 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 system 100 in that any suitable arrangements, chronologies, configurations, and timing mechanisms may be provided without departing from the teachings of the present disclosure.

[0066] 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 system 100 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 system 100.

[0067] 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

[0068] Example C1 is at least one machine readable storage medium having one or more instructions that when executed by at least one processor, cause the at least one processor to acquire a plurality of reputations related to an object, where the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects, and combine the plurality of reputations to create a total reputation for the object.

[0069] In Example C2, the subject matter of Example C1 can optionally include where the object is an electronic device and the sub-objects are processes running on the electronic device and each of the plurality of reputations is a reputation related to one of the processes.

[0070] In Example C3, the subject matter of any one of Examples C1-C2 can optionally include where a Bayesian algorithm is used to combine the plurality of reputations.

[0071] In Example C4, the subject matter of any one of Examples C1-C3 can optionally include where each of the plurality of reputations includes a reputation confidence and a reputation weight.

[0072] In Example C5, the subject matter of any one of Examples C1-C4 can optionally include where the one or more instructions that when executed by the at least

one processor, further cause the processor to allow general remediation for a malicious reputation when an allow repair flag is set for a sub-object related to the malicious reputation.

[0073] In Example C6, the subject matter of any one of Example C1-C5 can optionally include where at least one of the plurality of reputations for a sub-object was determined by combining multiple reputations for the sub-object.

[0074] In Example C7, the subject matter of any one of Examples C1-C6 can optionally include where the object is an electronic device and the total reputation for the object is communicated to a second electronic device.

[0075] In Example C8, the subject matter of any one of Examples C1-C7 can optionally include where the one or more instructions that when executed by the at least one processor, further cause the processor to acquire, at the second electronic device, a plurality of reputations related to a plurality of objects connected to a network, where the object is included in the plurality of objects, and combine the plurality of reputations to create a total reputation for the network.

[0076] In Example A1, an electronic device can include a reputation module, where the reputation module is configured to acquire a plurality of reputations related to an object, where the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects, and combine the plurality of reputations to create a total reputation for the object.

[0077] In Example, A2, the subject matter of Example A1 can optionally include where the object is an electronic device and the sub-objects are processes running on the electronic device and each of the plurality of reputations is a reputation related to one of the processes.

[0078] In Example A3, the subject matter of any one of Examples A1-A2 can optionally include where a Bayesian algorithm is used to combine the plurality of reputations.

[0079] In Example A4, the subject matter of any one of Examples A1-A3 can optionally include where each of the plurality of reputations includes a reputation confidence and a reputation weight.

[0080] In Example A5, the subject matter of any one of Examples A1-A4 can optionally include where the reputation module is further configured to allow general remediation for a malicious reputation when an allow repair flag is set for a sub-object related to the malicious reputation.

[0081] In Example A6, the subject matter of any one of Examples A1-A5 can optionally include where at least one of the plurality of reputations for a sub-object was determined by combining multiple reputations for the sub-object.

[0082] In Example A7, the subject matter of any one of Examples A1-A6 can optionally include where the object is an electronic device and the total reputation for the object is communicated to a second electronic device.

[0083] In Example A8, the subject matter of any one of Examples A1-A7 can optionally include where the reputation module is further configured to acquire, at the second electronic device, a plurality of reputations related to a plurality of objects connected to a network, where the object is included in the plurality of objects, and combine the plurality of reputations to create a total reputation for the network.

[0084] Example M1 is a method including acquiring a plurality of reputations related to an object, where the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects, and combining the plurality of reputations to create a total reputation for the object.

[0085] In Example M2, the subject matter of Example M1 can optionally include where the object is an electronic device and the sub-objects are processes running on the electronic device and each of the plurality of reputations is a reputation related to one of the processes.

[0086] In Example M3, the subject matter of any one of the Examples M1-M2 can optionally include where a Bayesian algorithm is used to combine the plurality of reputations.

[0087] In Example M4, the subject matter of any one of the Examples M1-M3 can optionally include where each of the plurality of reputations includes a reputation confidence and a reputation weight.

[0088] In Example M5, the subject matter of any one of the Examples M1-M4 can optionally include where at least one of the plurality of reputations for a sub-object was determined by combining multiple reputations for the sub-object.

[0089] In Example M6, the subject matter of any one of the Examples M1-M5 can optionally include where the object is an electronic device and the total reputation for the object is communicated to a second electronic device.

[0090] In Example M7, the subject matter of any one of the Examples M1-M6 can optionally include acquiring, at the second electronic device, a plurality of reputations related to a plurality of objects connected to a network, where the object is included in the plurality of objects, and combining the plurality of reputations to create a total reputation for the network.

[0091] Example S1 is a system for combining multiple reputations, the system including a reputation module configured for acquiring a plurality of reputations related to an object, where the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects, and combining the plurality of reputations to create a total reputation for the object.

[0092] In Example S2, the subject matter of Example S1 can optionally include where a Bayesian algorithm is used to combine the plurality of reputations.

[0093] 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-A8, or M1-M7. Example Y1 is an apparatus comprising means for performing of any of the Example methods M1-M7. 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 computer-readable medium comprising one or more instructions that when executed by at least one processor, cause the at least one processor to:

acquire a plurality of reputations related to an object, wherein the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects; and

combine the plurality of reputations to create a total reputation for the object.

2. The at least one computer-readable medium of Claim 1, wherein the object is an electronic device and the sub-objects are processes running on the electronic device and each of the plurality of reputations is a reputation related to one of the processes.

3. The at least one computer-readable medium of any of Claims 1 and 2, wherein a Bayesian algorithm is used to combine the plurality of reputations.

4. The at least one computer-readable medium of any of Claims 1-3, wherein each of the plurality of reputations includes a reputation confidence and a reputation weight.

5. The at least one computer-readable medium of any of Claims 1-4, further comprising one or more instructions that when executed by the at least one processor, further cause the at least one processor to:

allow general remediation for a malicious reputation when an allow repair flag is set for a sub-object related to the malicious reputation.

6. The at least one computer-readable medium of any of Claims 1-5, wherein at least one of the plurality of reputations for a sub-object was determined by combining multiple reputations for the sub-object.

7. The at least one computer-readable medium of any of Claims 1-6, wherein the object is an electronic device and the total reputation for the object is communicated to a second electronic device.

8. The at least one computer-readable medium of any of Claims 1-7, further comprising one or more instructions that when executed by the at least one processor, further cause the at least one processor to:

acquire, at the second electronic device, a plurality of reputations related to a plurality of objects connected to a network, wherein the object is included in the plurality of objects; and

combine the plurality of reputations to create a total reputation for the network.

9. An apparatus comprising:

reputation module configured to:

acquire a plurality of reputations related to an object, wherein the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects; and

combine the plurality of reputations to create a total reputation for the object.

10. The apparatus of Claim 9, wherein the object is an electronic device and the sub-objects are processes running on the electronic device and each of the plurality of reputations is a reputation related to one of the processes.

11. The apparatus of any of Claims 9 and 10, wherein a Bayesian algorithm is used to combine the plurality of reputations.

12. The apparatus of any of Claims 9-11, wherein each of the plurality of reputations includes a reputation confidence and a reputation weight.

13. The apparatus of any of Claims 9-12, wherein the reputation module is further configured to:

allow general remediation for a malicious reputation when an allow repair flag is set for a sub-object related to the malicious reputation.

14. The apparatus of any of Claims 9-13, wherein at least one of the plurality of reputations for a sub-object was determined by combining multiple reputations for the sub-object.

15. The apparatus of any of Claims 9-14, wherein the object is an electronic device and the total reputation for the object is communicated to a second electronic device.

16. The apparatus of any of Claims 9-15, wherein reputation module configured to:

acquire, at the second electronic device, a plurality of reputations related to a plurality of objects connected to a network, wherein the object is included in the plurality of objects; and

combine the plurality of reputations to create a total reputation for the network.

17. A method comprising:

acquiring a plurality of reputations related to an object, wherein the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects; and

combining the plurality of reputations to create a total reputation for the object.

18. The method of Claim 17, wherein the object is an electronic device and the sub-objects are processes running on the electronic device and each of the plurality of reputations is a reputation related to one of the processes.

19. The method of any of Claims 17 and 18, wherein a Bayesian algorithm is used to combine the plurality of reputations.

20. The method of any of Claims 17-19, wherein each of the plurality of reputations includes a reputation confidence and a reputation weight.

21. The method of any of Claims 17-20, wherein at least one of the plurality of reputations for a sub-object was determined by combining multiple reputations for the sub-object.

22. The method of any of Claims 17-21, wherein the object is an electronic device and the total reputation for the object is communicated to a second electronic device.

23. The method of any of Claims 17-22, further comprising:

acquiring, at the second electronic device, a plurality of reputations related to a plurality of objects connected to a network, wherein the object is included in the plurality of objects; and

combining the plurality of reputations to create a total reputation for the network.

24. A system for combining multiple reputations, the system comprising:

a reputation module configured for:

acquiring a plurality of reputations related to an object, wherein the object includes a plurality of sub-objects and each of the plurality of reputations corresponds to one of the plurality of sub-objects; and

combining the plurality of reputations to create a total reputation for the object.

25. The system of Claim 24, wherein a Bayesian algorithm is used to combine the plurality of reputations.

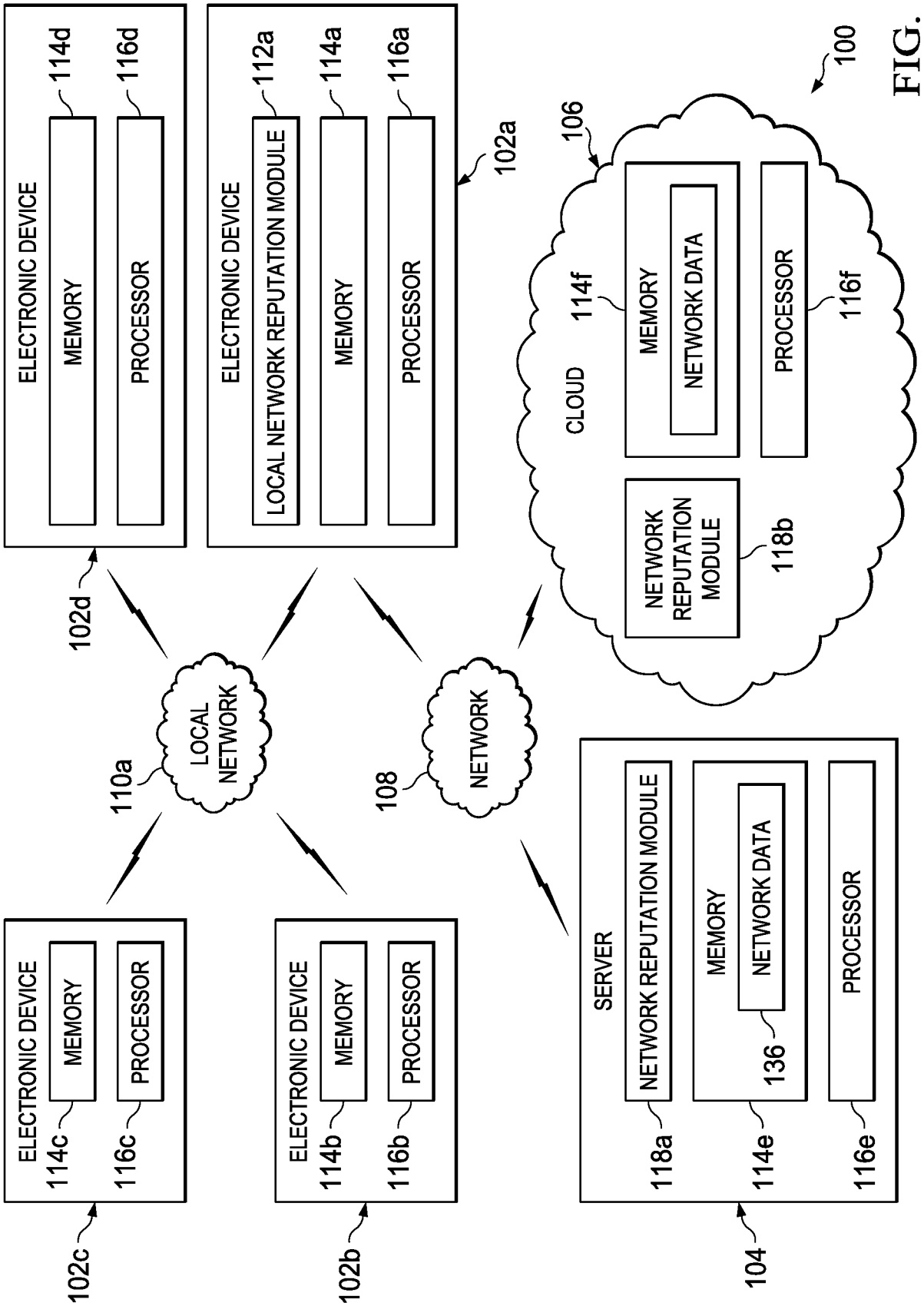

100
ELECTRONIC DEVICE
MEMORY
PROCESSOR
114d
116d
102d
ELECTRONIC DEVICE
LOCAL NETWORK REPUTATION MODULE
MEMORY
PROCESSOR
112a
114a
116a
102a
106
CLOUD
MEMORY
NETWORK DATA
PROCESSOR
114f
116f
NETWORK REPUTATION MODULE
118b
LOCAL NETWORK
110a
NETWORK
108
ELECTRONIC DEVICE
MEMORY
PROCESSOR
114c
116c
102c
ELECTRONIC DEVICE
MEMORY
PROCESSOR
114b
116b
102b
SERVER
NETWORK REPUTATION MODULE
MEMORY
NETWORK DATA
136
PROCESSOR
118a
114e
116e
104

FIG. 1

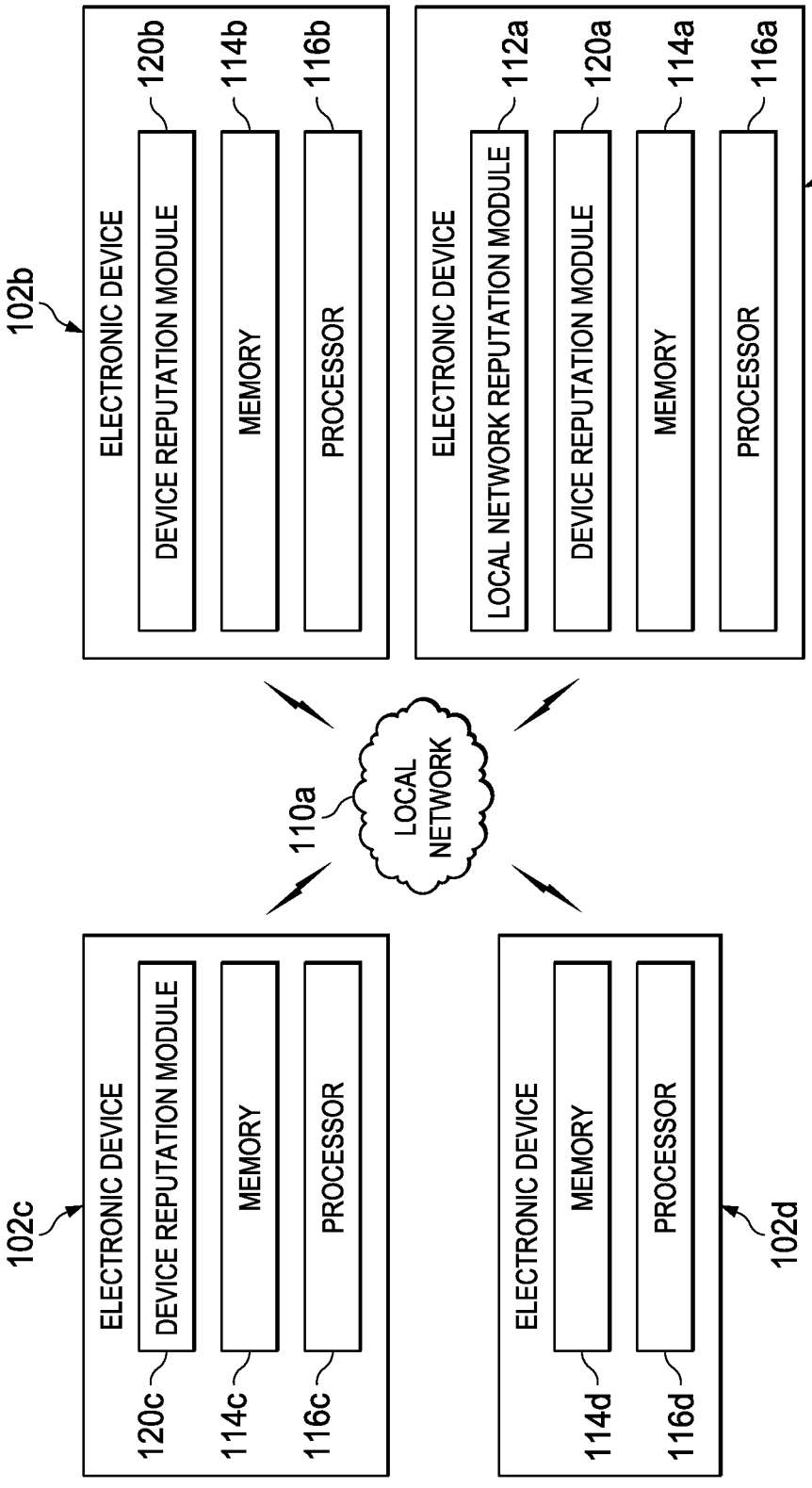

ELECTRONIC DEVICE
LOCAL NETWORK REPUTATION MODULE
DEVICE REPUTATION MODULE
MEMORY
PROCESSOR
112a
120a
114a
116a
102a
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
MEMORY
PROCESSOR
120b
114b
116b
102b
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
MEMORY
PROCESSOR
120c
114c
116c
102c
ELECTRONIC DEVICE
MEMORY
PROCESSOR
114d
116d
102d
110a
LOCAL NETWORK

FIG. 2

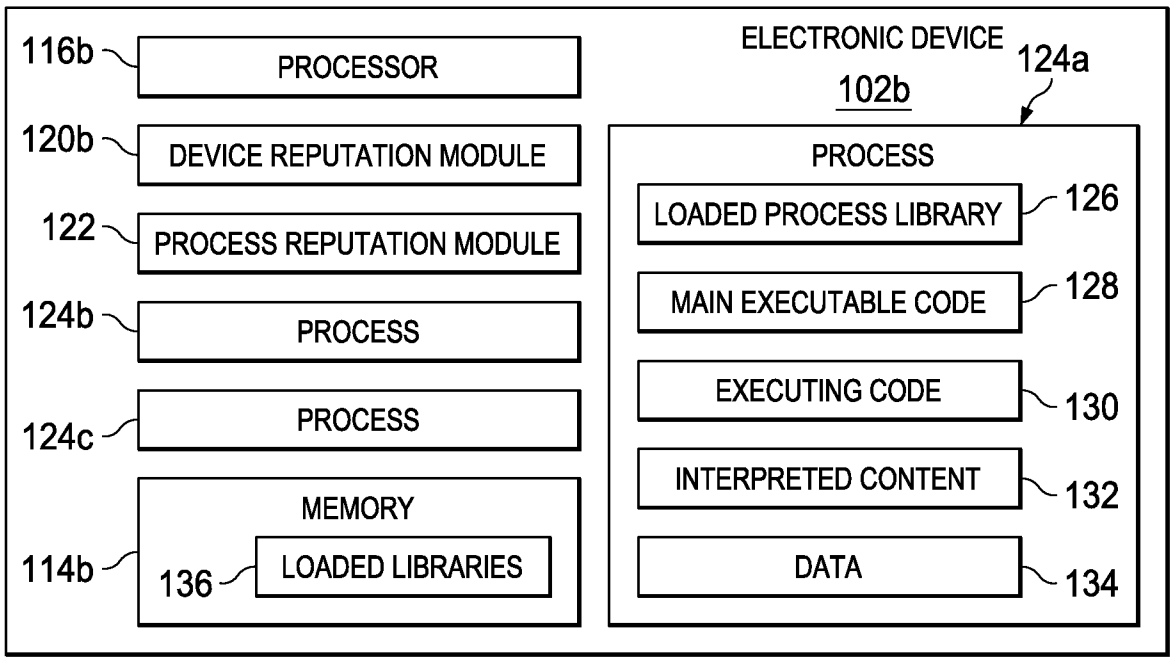

116b
PROCESSOR
120b
DEVICE REPUTATION MODULE
122
PROCESS REPUTATION MODULE
124b
PROCESS
124c
PROCESS
114b
MEMORY
136
LOADED LIBRARIES
ELECTRONIC DEVICE
102b
124a
PROCESS
LOADED PROCESS LIBRARY
126
MAIN EXECUTABLE CODE
128
EXECUTING CODE
130
INTERPRETED CONTENT
132
DATA
134

FIG. 3

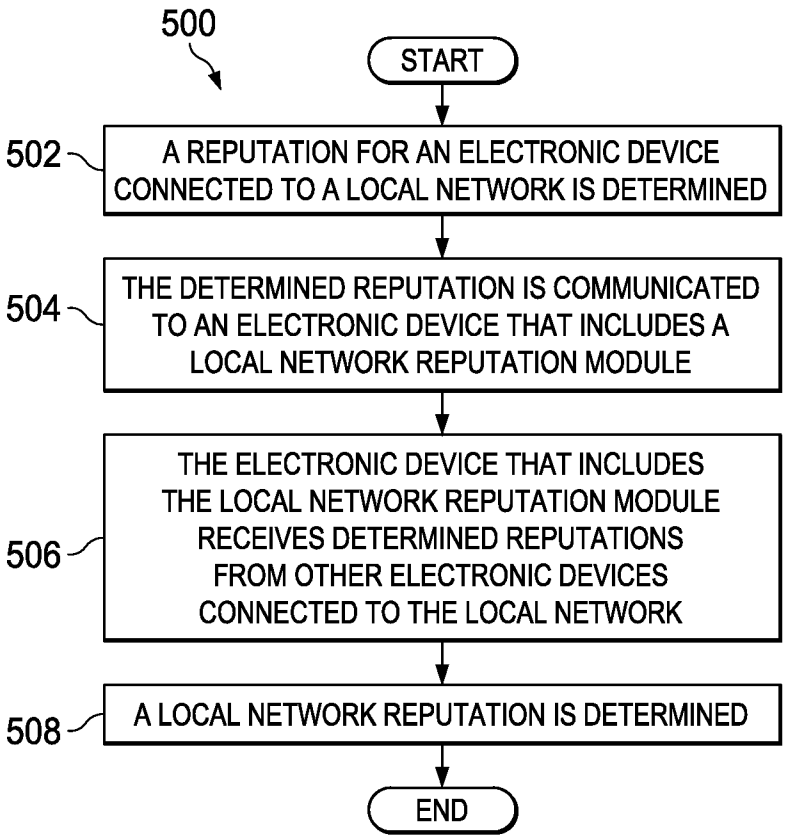

500
START
502
A REPUTATION FOR AN ELECTRONIC DEVICE CONNECTED TO A LOCAL NETWORK IS DETERMINED
504
THE DETERMINED REPUTATION IS COMMUNICATED TO AN ELECTRONIC DEVICE THAT INCLUDES A LOCAL NETWORK REPUTATION MODULE
506
THE ELECTRONIC DEVICE THAT INCLUDES THE LOCAL NETWORK REPUTATION MODULE RECEIVES DETERMINED REPUTATIONS FROM OTHER ELECTRONIC DEVICES CONNECTED TO THE LOCAL NETWORK
508
A LOCAL NETWORK REPUTATION IS DETERMINED
END

FIG. 5

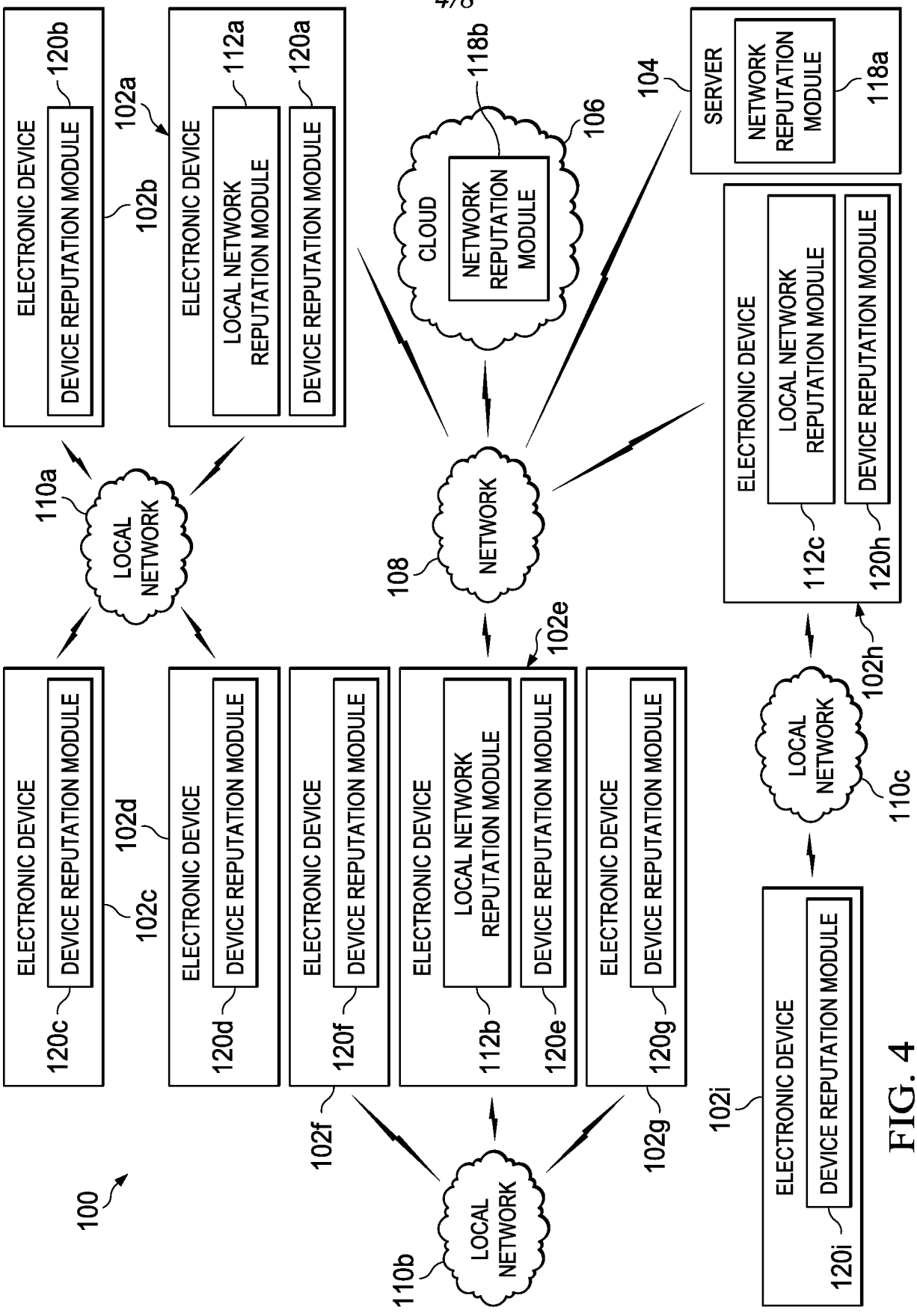

100
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
120b
102b
102a
ELECTRONIC DEVICE
LOCAL NETWORK REPUTATION MODULE
112a
DEVICE REPUTATION MODULE
120a
110a
LOCAL NETWORK
CLOUD
NETWORK REPUTATION MODULE
118b
106
104
SERVER
NETWORK REPUTATION MODULE
118a
108
NETWORK
ELECTRONIC DEVICE
LOCAL NETWORK REPUTATION MODULE
DEVICE REPUTATION MODULE
112c
120h
102h
110c
LOCAL NETWORK
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
120c
102c
102d
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
120d
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
120f
102f
ELECTRONIC DEVICE
LOCAL NETWORK REPUTATION MODULE
DEVICE REPUTATION MODULE
112b
120e
102e
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
120g
102g
LOCAL NETWORK
110b
ELECTRONIC DEVICE
DEVICE REPUTATION MODULE
120i
102i

FIG. 4

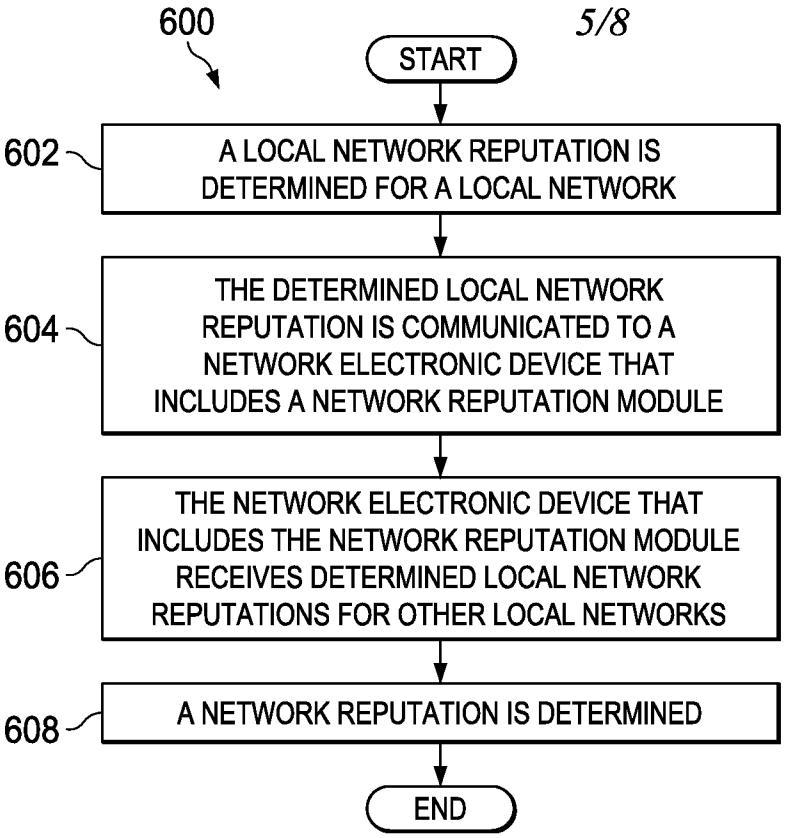

600
START
602
A LOCAL NETWORK REPUTATION IS DETERMINED FOR A LOCAL NETWORK
604
THE DETERMINED LOCAL NETWORK REPUTATION IS COMMUNICATED TO A NETWORK ELECTRONIC DEVICE THAT INCLUDES A NETWORK REPUTATION MODULE
606
THE NETWORK ELECTRONIC DEVICE THAT INCLUDES THE NETWORK REPUTATION MODULE RECEIVES DETERMINED LOCAL NETWORK REPUTATIONS FOR OTHER LOCAL NETWORKS
608
A NETWORK REPUTATION IS DETERMINED
END

FIG. 6

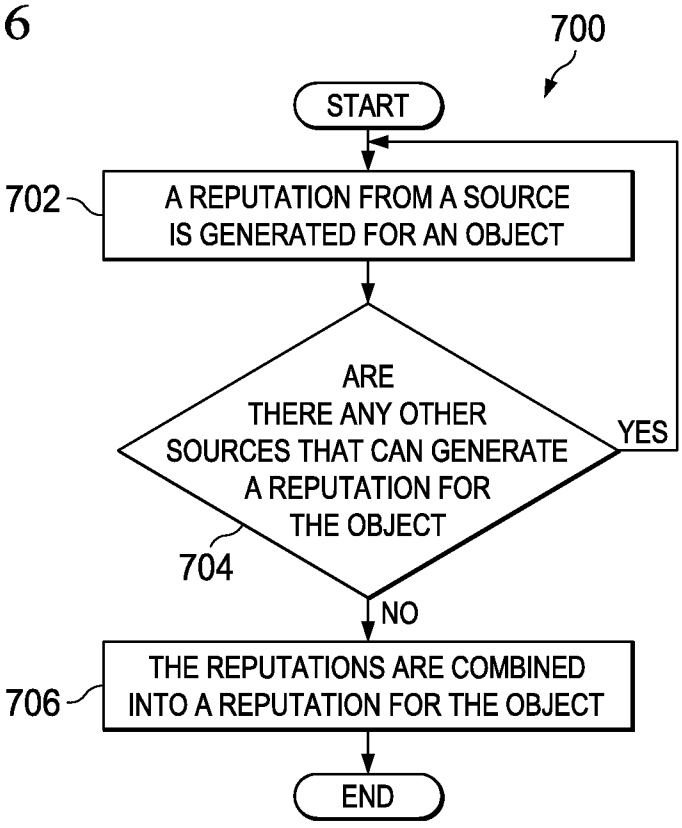

700
START
702
A REPUTATION FROM A SOURCE IS GENERATED FOR AN OBJECT
ARE THERE ANY OTHER SOURCES THAT CAN GENERATE A REPUTATION FOR THE OBJECT
704
YES
NO
706
THE REPUTATIONS ARE COMBINED INTO A REPUTATION FOR THE OBJECT
END

FIG. 7

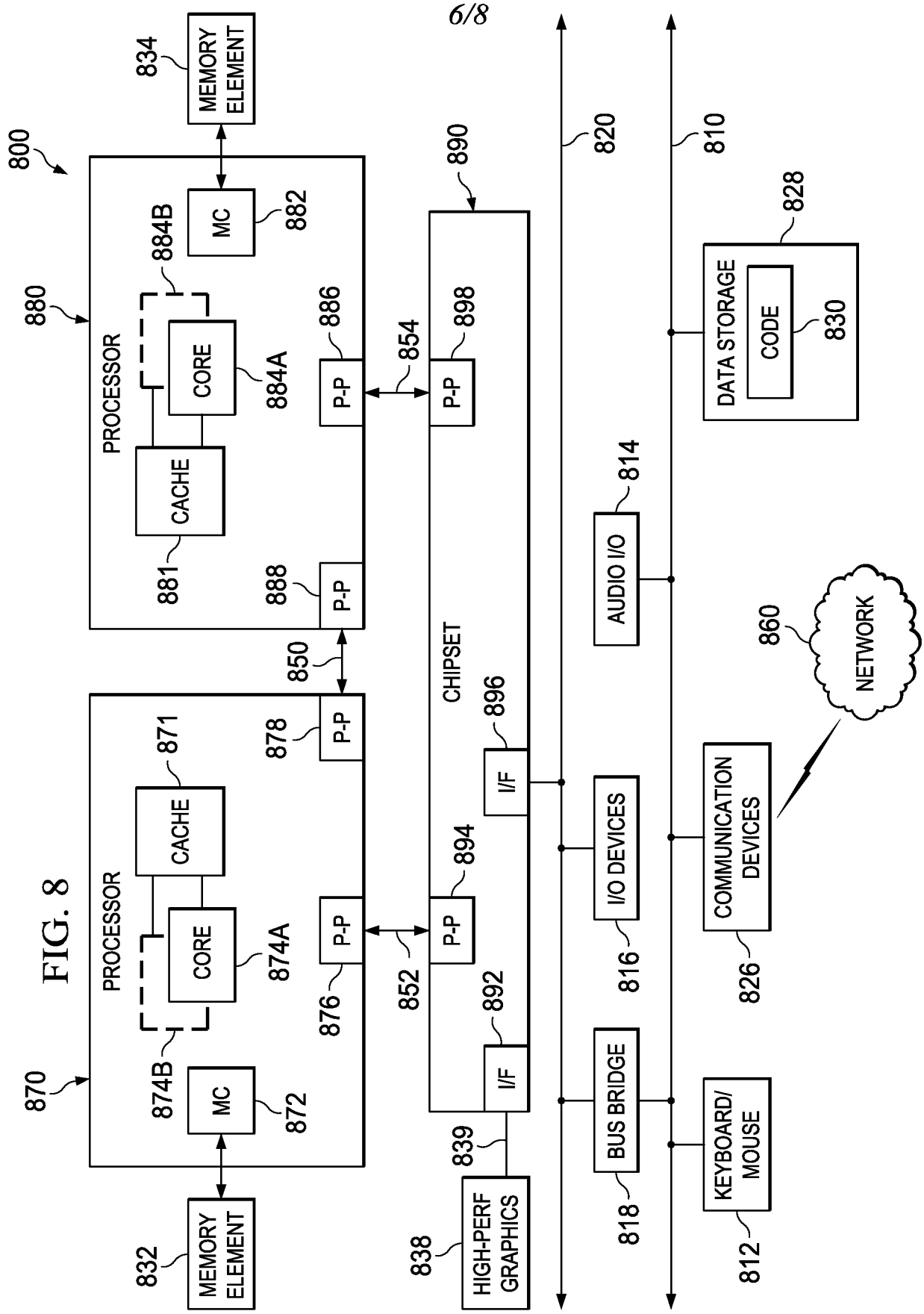
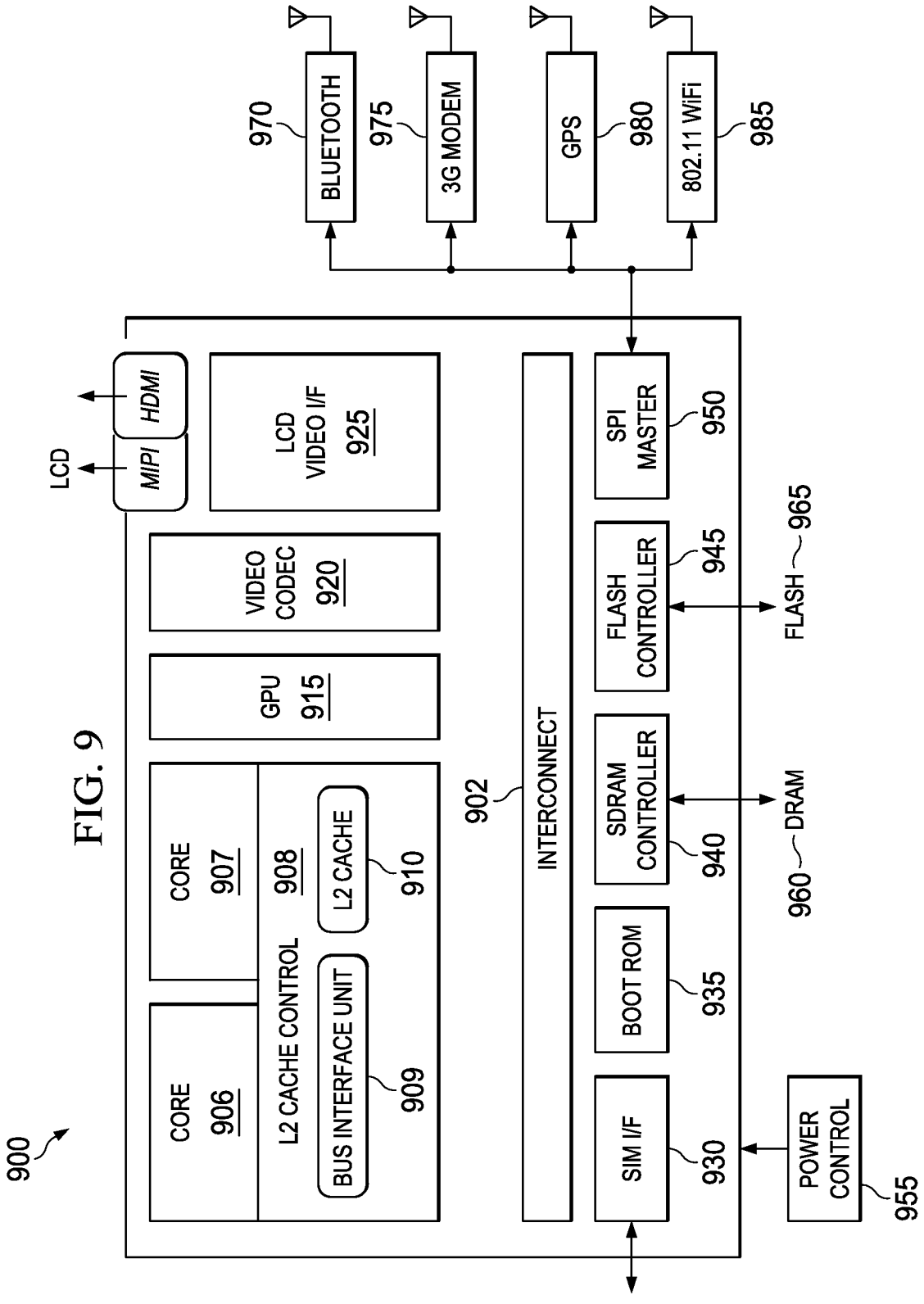

800
834
MEMORY ELEMENT
MC
882
884B
880
PROCESSOR
CORE
884A
CACHE
881
886
P-P
888
P-P
854
890
P-P
898
CHIPSET
850
878
P-P
871
CACHE
PROCESSOR
CORE
874A
874B
MC
872
870
876
P-P
852
894
P-P
896
I/F
892
I/F
839
838
HIGH-PERF GRAPHICS
832
MEMORY ELEMENT
820
810
828
DATA STORAGE
CODE
830
AUDIO I/O
814
860
NETWORK
I/O DEVICES
816
COMMUNICATION DEVICES
826
BUS BRIDGE
818
KEYBOARD/ MOUSE
812

FIG. 8

FIG. 9


900
CORE 906
CORE 907
L2 CACHE CONTROL 908
BUS INTERFACE UNIT 909
L2 CACHE 910
GPU 915
VIDEO CODEC 920
LCD VIDEO I/F 925
LCD
MIPI
HDMI
902
INTERCONNECT
SIM I/F 930
BOOT ROM 935
SDRAM CONTROLLER 940
FLASH CONTROLLER 945
SPI MASTER 950
POWER CONTROL 955
960 DRAM
FLASH 965
970 BLUETOOTH
975 3G MODEM
980 GPS
985 802.11 WiFi

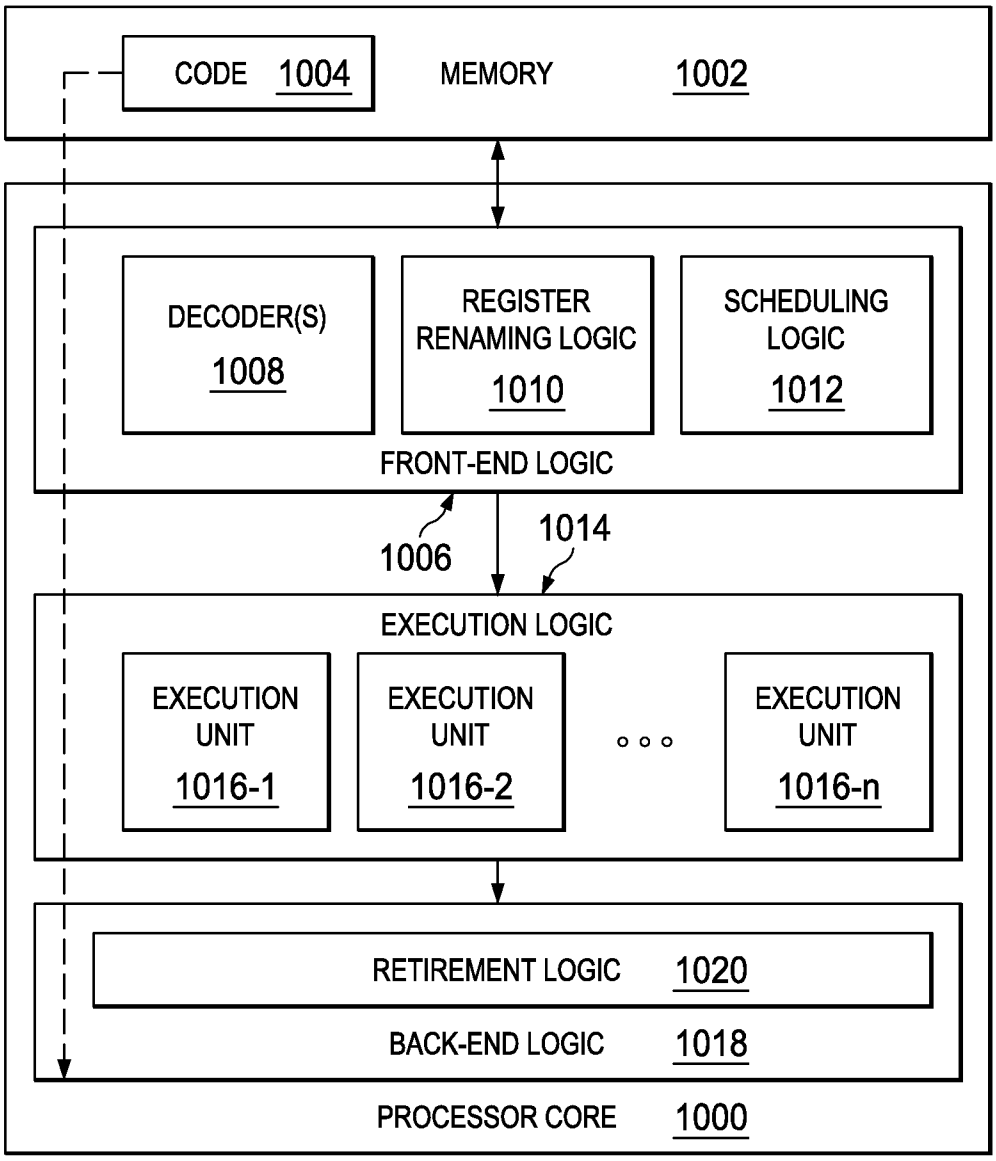

CODE 1004
MEMORY 1002
DECODER(S) 1008
REGISTER RENAMING LOGIC 1010
SCHEDULING LOGIC 1012
FRONT-END LOGIC
1006
1014
EXECUTION LOGIC
EXECUTION UNIT 1016-1
EXECUTION UNIT 1016-2
EXECUTION UNIT 1016-n
RETIREMENT LOGIC 1020
BACK-END LOGIC 1018
PROCESSOR CORE 1000

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/062597

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(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 29/06; G06F 15/16; G06F 17/30; H04L 9/32; G06T 11/20; G06F 21/50

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: plurality, device, process, reputations, object, combine, Bayesian algorithm

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008-0141366 A1 (DAVID CROSS et al.) 12 June 2008 See paragraphs [0013], [0017]; and figure 1.	1-25
Y	US 2012-0284282 A9 (RISHAB AIYER GHOSH et al.) 08 November 2012 See paragraphs [0018], [0026], [0029]-[0032], [0059]; and figure 3.	1-25
Y	US 2011-0040825 A1 (ZULFIKAR RAMZAN et al.) 17 February 2011 See paragraphs [0024], [0059]; and figure 1.	3-5,11-13,19-20,25
A	KR 10-2014-0127178 A (SANG-HO LEE) 03 November 2014 See paragraphs [0065]-[0087]; and figures 8-10.	1-25
A	US 2009-0287819 A1 (KRIS IVERSON) 19 November 2009 See paragraphs [0034], [0037], [0069]-[0072]; and figures 1, 6.	1-25

☐ 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
11 March 2016 (11.03.2016)	**14 March 2016 (14.03.2016)**

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. +82-42-472-7140

Authorized officer
KIM, Seong Woo
Telephone No. +82-42-481-3348

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2015/062597

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0141366 A1	12/06/2008	AU 2007-333444 A1	19/06/2008
		AU 2007-333444 B2	09/02/2012
		BR PI0719035 A2	05/11/2013
		CA 2671031 A1	19/06/2008
		CN 101553833 A	07/10/2009
		EP 2126808 A1	02/12/2009
		EP 2126808 A4	23/11/2011
		JP 2010-512576 A	22/04/2010
		JP 5066578 B2	07/11/2012
		KR 10-2009-0087122 A	14/08/2009
		MX 2009006025 A	16/06/2009
		RU 2009-126155 A	20/01/2011
		RU 2458393 C2	10/08/2012
		TW 200836085 A	01/09/2008
		US 2011-252483 A1	13/10/2011
		US 7991902 B2	02/08/2011
		WO 2008-073647 A1	19/06/2008
US 2012-0284282 A9	08/11/2012	EP 2359276 A1	24/08/2011
		EP 2359276 A4	23/01/2013
		JP 2012-510667 A	10/05/2012
		JP 2015-057718 A	26/03/2015
		JP 5640015 B2	10/12/2014
		US 2010-0153404 A1	17/06/2010
		US 2014-250112 A1	04/09/2014
		US 8688701 B2	01/04/2014
		US 9135294 B2	15/09/2015
		WO 2010-065111 A1	10/06/2010
US 2011-0040825 A1	17/02/2011	CA 2763201 A1	17/02/2011
		CN 102656587 A	05/09/2012
		EP 2465071 A1	20/06/2012
		JP 2013-502009 A	17/01/2013
		JP 5599884 B2	01/10/2014
		US 2015-269379 A1	24/09/2015
		US 9081958 B2	14/07/2015
		WO 2011-019720 A1	17/02/2011
KR 10-2014-0127178 A	03/11/2014	None	
US 2009-0287819 A1	19/11/2009	CN 102100032 A	15/06/2011
		CN 102100032 B	26/03/2014
		US 8266284 B2	11/09/2012
		WO 2009-139950 A1	19/11/2009