



- (51) International Patent Classification:
G06F 17/30 (2006.01) *G06F 21/30* (2013.01)
- (21) International Application Number:
PCT/US2015/022071
- (22) International Filing Date:
23 March 2015 (23.03.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
287/CHE/2015 19 January 2015 (19.01.2015) IN
- (71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).
- (72) Inventors: **PHATAK, Anand Satish**; Sy. No.192, Whitefield Road, Mahadevapura Post, Bangalore, Karnataka 560048 (IN). **SRIVILLIPUTTUR MANNARSWAMY, Sandya**; Sy. No.192, Whitefield Road, Mahadevapura Post, Bangalore, Karnataka 560048 (IN).
- (74) Agents: **ORTEGA, Arthur S.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (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: ACCESS CONTROL TO A PORTION OF A FILE SYSTEM OBJECT

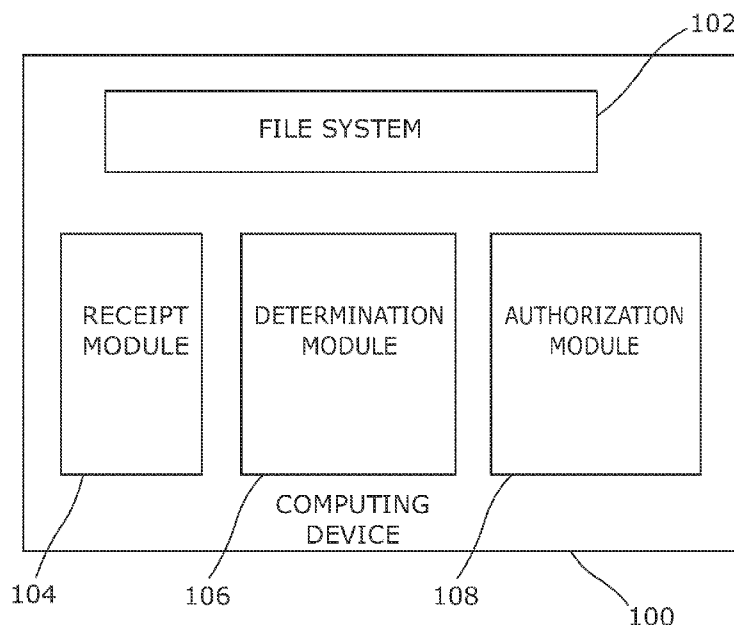


Fig. 1

(57) Abstract: Some examples relate to controlling access to a portion of a file system object. In an example, a request may be received for accessing a portion of a file system object. A determination may be made from an Access Control List (ACL) associated with the file system object whether the request is permitted to access the portion of the file system object, wherein the ACL specifies an access right related to the portion of the file system object. If the request is permitted to access the portion of the file system object, the request may be allowed to access the portion of the file system object.

**Declarations under Rule 4.17:**

- *as to the identity of the inventor (Rule 4.17(i))*
- *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))*

ACCESS CONTROL TO A PORTION OF A FILE SYSTEM OBJECT

Background

[001] File systems typically include methods to assign permissions or access rights to a specific user or group of users. These mechanisms control the ability of the users to perform an action related to the contents of the file system. In other words, they may convey to an operating system what can be done with a file and by whom. Some examples of such actions may include a read, write, execute, delete file, and directory access operation.

Brief Description of the Drawings

[002] For a better understanding of the solution, embodiments will now be described, purely by way of example, with reference to the accompanying drawings, in which:

[003] FIG. 1 is a block diagram of an example computing device for controlling access to a portion of a file system object;

[004] FIG. 2 is a flowchart of an example method of controlling access to a portion of a file system object; and

[005] FIG. 3 is a block diagram of an example computer system for controlling access to a portion of a file system object.

Detailed Description

[006] File system permissions may range from a simple arrangement with one or two basic permissions (such as read and write) to a more detailed classification that describes access rights to a file system object. There may be scenarios where access to an entire file system object may not be

required. Rather, permissions to access or modify a portion of a file system object may be more desirable. To provide an example, a cloud-based content service provider may prefer to provide access to only those portions or segments of a file's content (for example, a video or sound recording) that are paid for by a subscriber (for example, a media house), as against access to an entire file. Likewise, a subscriber may also be reluctant to pay for an entire file's contents. Thus, there may be situations where it may be possible for a single file to hold data that may not be required by all users, or hold data whose parts may be required by different users at the same time. The existing file system permission mechanisms may not authorize a request to access a portion(s) of a file system object.

[007] To address this issue, the present disclosure describes various examples for controlling access to a portion of a file system object. In an example, a request may be received to access a portion of a file system object. Upon receipt of the request, a determination may be made from an Access Control List (ACL) associated with the file system object whether the request is authorized to access the portion of the file system object. If the request is authorized to access the portion of the file system object, the request may be allowed to access the portion of the file system object.

[008] FIG. 1 is a block diagram of an example computing device 100 for controlling access to a portion of a file system object. Computing device 100 may include a file system 102, a receipt module 104, a determination module 106, and an authorization module 108. The term "module" may refer to a software component (machine readable instructions), a hardware component or a combination thereof. A module may include, by way of example, components, such as software components, processes, tasks, co-routines, functions, attributes, procedures, drivers, firmware, data, databases, data structures, Application Specific Integrated Circuits (ASIC) and other computing devices. A module may reside on a volatile or non-

volatile storage medium and configured to interact with a processor of computing device 100.

[009] Computing device 100 generally represents any type of computing system capable of reading machine-executable instructions. Examples of computing device 100 may include, without limitation, a server, a desktop computer, a notebook computer, a tablet computer, a thin client, a mobile device, a personal digital assistant (PDA), a phablet, and the like.

[0010] File system 102 may include one or more file system objects. Some non-limiting examples of a file system object may include a file, a directory, a sub-directory, and the like. In an example, file system 102 may be a local file system. In another example, file system may a scale-out file system such as a shared file system or network file system. Examples of a shared file system may include a Network Attached Storage (NAS) file system or cluster file system. Examples of a network file system may include a distributed file system or distributed parallel file system.

[0011] An access control list (ACL) may be associated with a file system object of the file system 102, wherein the ACL may specify an access right (or permission) related to accessing of a portion of the file system object. The access control list (ACL) may be used to manage file system permissions related to various portions of the file system object. For instance, the access control list may define a list of permissions attached to a portion of a file system object. The ACL may include a set of data (for example, a table) that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific portion of a file system object. The permissions determine specific access rights, such as whether a user can read from, or write to a portion of a file system object. In an instance, such ACL may be termed as a "custom ACL", which may be in addition to or alternative to a default ACL that may be associated with the file system

object. In an example, the custom ACL may be a part of extended file attributes of the associated file system object.

[0012] In an example, the ACL may specify whether a request is authorized to access a portion of an associated file system object. The ACL may also define what operations a request may be allowed to perform on a portion of a file system object. In another example, if the request originates from a computer application or computer process, the ACL may specify which computer application or computer process may be allowed to access a segment of an associated file system object. This may help, for instance, to distinguish between a trusted application and an application that may be suspicious. In the former case, the ACL may allow the request to access the requested part of a file system object. However, in the latter case, the ACL may disallow the request. In this context, the ACL may also define, in addition, whether a user making such a request via the aforementioned computer application or process is allowed to access the requested segment of the file system object.

[0013] In a yet another example, the ACL may specify a computing device(s) that may be allowed to access a portion of an associated file system object. In other words, the ACL may allow a request to access a portion of a file system object only if the request is received from a specified computing device. This may help, for instance, to distinguish between a trusted computing device and a device that may be untrustworthy. In the former case, the ACL may allow the computing device to access the requested part of a file system object. However, in the latter case, the ACL may deny access.

[0014] In a further example, the ACL may specify a computer network(s) that may be allowed to access a portion of an associated file system object. In other words, the ACL may allow a request to access a portion of a file system object only if the request is received from a specified computer

network. This may help, for instance, to distinguish between a trusted computer network and a network that may be untrustworthy. In the former case, the ACL may allow the computer network to access the requested part of a file system object. However, in the latter case, the ACL may not grant access.

[0015] In a still further example, the ACL may specify a geographical location(s) that may be allowed to access a portion of an associated file system object. In other words, the ACL may allow a request to access a portion of a file system object only if the request is received from a specified location. This may help, for instance, to distinguish between a permitted location and a location that may be barred. In the former case, the ACL may allow the location to access the requested part of a file system object. However, in the latter case, the ACL may deny access.

[0016] In a still further example, the ACL may specify a time period during which an access right may remain valid for a portion of a file system object. In other words, the ACL may specify how long a request may be allowed to access a portion of a file system object. In another instance, the ACL may specify a time period for allowing a request to access a portion of a file system object from a particular computer application or process. In another example, the ACL may specify a time period for allowing a request to access a portion of a file system object from a particular computing device or computer network. In a further example, the ACL may specify a time period for allowing a request to access a portion of a file system object from a particular location.

[0017] Receipt module 104 may receive a request to access a portion (or specific part) of a file system object of a file system (for example, 102). In an example, the request may be received from a user. In another example, the request may be received from a computer application or computer process. In a yet another example, the request may be received from another

computing device that may be communicatively coupled to the computing device 100, for example, via a computer network. Such a computer network may be a wireless or wired network. The computer network may include, for example, a Local Area Network (LAN), a Wireless Local Area Network (WAN), a Metropolitan Area Network (MAN), a Storage Area Network (SAN), a Campus Area Network (CAN), or the like. Further, the computer network may be a public network (for example, the Internet) or a private network (for example, an intranet).

[0018] In an example, the “portion” of a file system object, for which a request may be received by the receipt module 104, may be defined using file offsets. For instance, a request may define a portion of a file system object that it requires access to by specifying a “start offset” value and an “end offset” value. In such case, the “portion” may be considered as that segment of the file system object, which may be present between these two offsets (including both start offset and end offset values).

[0019] In an example, a request to access a portion of a file system object of the file system may include a request to perform an operation related to the portion of the file system object. Some non-limiting examples of such operation may include a read, write, and an execute operation.

[0020] Determination module 106 may determine, from an Access Control List (ACL) associated with a file system object, whether a request to access a portion of a file system object is authorized to access the portion of the file system object. In other words, the determination module 106 may refer to the Access Control List (ACL) associated with the file system object to determine whether the request may be allowed to access the requested portion of the file system object. In another example, the determination module 106 may determine, from the Access Control List (ACL) associated with the file system object, if the request is received from a computer application or computer process that is permitted to access the requested

portion of the file system object in the ACL. In a further example, the determination module 106 may determine, from the Access Control List (ACL) associated with the file system object, if the request is received from a computing device that is permitted to access the requested portion of the file system object in the ACL. In a yet another example, the determination module 106 may determine, from the Access Control List (ACL) associated with the file system object, if the request is received from a computer network that is permitted to access the requested portion of the file system object in the ACL. In a still another example, the determination module 106 may determine, from the Access Control List (ACL) associated with the file system object, if the request is received from a geographical location that is permitted to access the requested portion of the file system object in the ACL.

[0021] Authorization module 108 may authorize a request to access a portion of a file system object if the determination module determines that the request is authorized to access the portion of the file system object. In other words, the authorization module 108 may allow the request to manipulate the portion of file system object. The aforementioned manipulation may include, by way of non-limiting examples, a read operation, a write operation, and a delete operation with respect to the requested portion. In an example, the authorization module 108 may authorize a request to access a portion of a file system object if it is determined that the request is received from a computing device that is permitted to access the requested portion of the file system object in the ACL. In a yet another example, the authorization module 108 may authorize a request to access a portion of a file system object if it is determined that the request is received from a computer network that is permitted to access the requested portion of the file system object in the ACL. In a still another example, the authorization module 108 may authorize a request to access a portion of a file system object if it is determined that request is received from a geographical location that is

permitted to access the requested portion of the file system object in the ACL.

[0022] FIG. 2 is a flowchart of an example method of controlling access to a portion of a file system object. The method 200, which is described below, may at least partially be executed on a computing device 100 of FIG. 1. However, other computing devices may be used as well. At block 202, a request may be received (for example, by receipt module 104) for accessing a portion of a file system object of a file system (for example, 102). At block 204, a determination may be made (for example, by determination module 106), from an Access Control List (ACL) associated with the file system object, whether the request is permitted to access the portion of the file system object. In an example, the ACL may specify all access right(s) related to the portion of the file system object. At block 206, if it is determined (for example, by authorization module 108) that the request is permitted to access the portion of the file system object, the request may be permitted to access the portion of the file system object. In an instance, the request may be permitted to access the portion of the file system object only for a time period specified in the ACL. In another instance, the permission to access a portion of the file system object may include a permission to perform an operation related to the portion of the file system object. Some non-limiting examples of such operation may include a read, write, and an execute operation.

[0023] FIG. 3 is a block diagram of an example computer system 300 for controlling access to a portion of a file system object. System 300 includes a processor 302 and a machine-readable storage medium 304 communicatively coupled through a system bus. In an example, system 300 may be analogous to computing device 100 of FIG. 1. Processor 302 may be any type of Central Processing Unit (CPU), microprocessor, or processing logic that interprets and executes machine-readable instructions stored in machine-readable storage medium 304. Machine-readable storage

medium 304 may be a random access memory (RAM) or another type of dynamic storage device that may store information and machine-readable instructions that may be executed by processor 302. For example, machine-readable storage medium 304 may be Synchronous DRAM (SDRAM), Double Data Rate (DDR), Rambus DRAM (RDRAM), Rambus RAM, etc. or a storage memory media such as a floppy disk, a hard disk, a CD-ROM, a DVD, a pen drive, and the like. In an example, machine-readable storage medium 304 may be a non-transitory machine-readable medium. Machine-readable storage medium 304 may store instructions 306, 308, and 310. In an example, instructions 306 may be executed by processor 302 to receive a request to access a portion of a file system object of a file system (for example, 102). Instructions 308 may be executed by processor 302 to determine, from an Access Control List (ACL) associated with the file system object, whether the request is authorized to access the portion of the file system object. In an instance, the ACL may enumerate an authorization related to the portion of the file system object. Instructions 310 may be executed by processor 302 to authorize the request to access the portion of the file system object if the request is authorized to access the portion of the file system object.

[0024] For the purpose of simplicity of explanation, the example method of FIG. 2 is shown as executing serially, however it is to be understood and appreciated that the present and other examples are not limited by the illustrated order. The example systems of FIGS. 1 and 3, and method of FIG. 3 may be implemented in the form of a computer program product including computer-executable instructions, such as program code, which may be run on any suitable computing device in conjunction with a suitable operating system (for example, Microsoft Windows, Linux, UNIX, and the like). Embodiments within the scope of the present solution may also include program products comprising non-transitory computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media

that can be accessed by a general purpose or special purpose computer. By way of example, such computer-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM, magnetic disk storage or other storage devices, or any other medium which can be used to carry or store desired program code in the form of computer-executable instructions and which can be accessed by a general purpose or special purpose computer. The computer readable instructions can also be accessed from memory and executed by a processor.

[0025] It should be noted that the above-described examples of the present solution is for the purpose of illustration only. Although the solution has been described in conjunction with a specific embodiment thereof, numerous modifications may be possible without materially departing from the teachings and advantages of the subject matter described herein. Other substitutions, modifications and changes may be made without departing from the spirit of the present solution. All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Claims:

1. A method of controlling access to a portion of a file system object, comprising:

receiving a request for accessing a portion of a file system object;

determining, from an Access Control List (ACL) associated with the file system object, whether the request is permitted to access the portion of the file system object, wherein the ACL specifies an access right related to the portion of the file system object; and

if the request is permitted to access the portion of the file system object, allowing the request to access the portion of the file system object.

2. The method of claim 1, further comprising allowing the request to access the portion of the file system object only for a time period specified in the ACL.

3. The method of claim 1, wherein the determining comprises determining whether the request is received from a specific application.

4. The method of claim 3, wherein the specific application includes a trusted application.

5. The method of claim 1, further comprising allowing the request to manipulate the portion of the file system object.

6. A system to control access to a portion of a file system object, comprising:

a receipt module to receive a request to access a portion of a file system object;

a determination module to determine, from a custom Access Control List (ACL) associated with the file system object, whether the request is authorized to access the portion of the file system object, wherein the custom ACL specifies an access right related to the portion of the file system object; and

an authorization module to authorize the request to access the portion of the file system object if the determination module determines that the request is authorized to access the portion of the file system object.

7. The system of claim 6, wherein to determine whether the request is authorized to access the portion of the file system object comprises to determine whether the request is received from a specific device.

8. The system of claim 6, wherein the determination whether the request is authorized to access the portion of the file system object comprises to determine whether the request is received from a specific network.

9. The system of claim 6, wherein the determination whether the request is authorized to access the portion of the file system object comprises to determine whether the request is received from a particular location.

10. The system of claim 6, wherein the custom ACL is a part of extended file attributes of the file system object.

11. A non-transitory machine-readable storage medium comprising instructions to control access to a portion of a file system object, the instructions executable by a processor to:

receive a request to access a portion of a file system object;

determine, from an Access Control List (ACL) associated with the file system object, whether the request is authorized to access the portion of the file system object, wherein the ACL enumerates an authorization related to the portion of the file system object; and

authorize the request to access the portion of the file system object if the request is authorized to access the portion of the file system object.

12. The storage medium of claim 11, wherein the request is received from a user.

13. The storage medium of claim 11, wherein the request is received from a computer application or computer process.

14. The storage medium of claim 11, wherein the request to access includes a request to perform an operation related to the portion of the file system object.

15. The storage medium of claim 11, wherein file offsets are used to define the portion of the file system object.

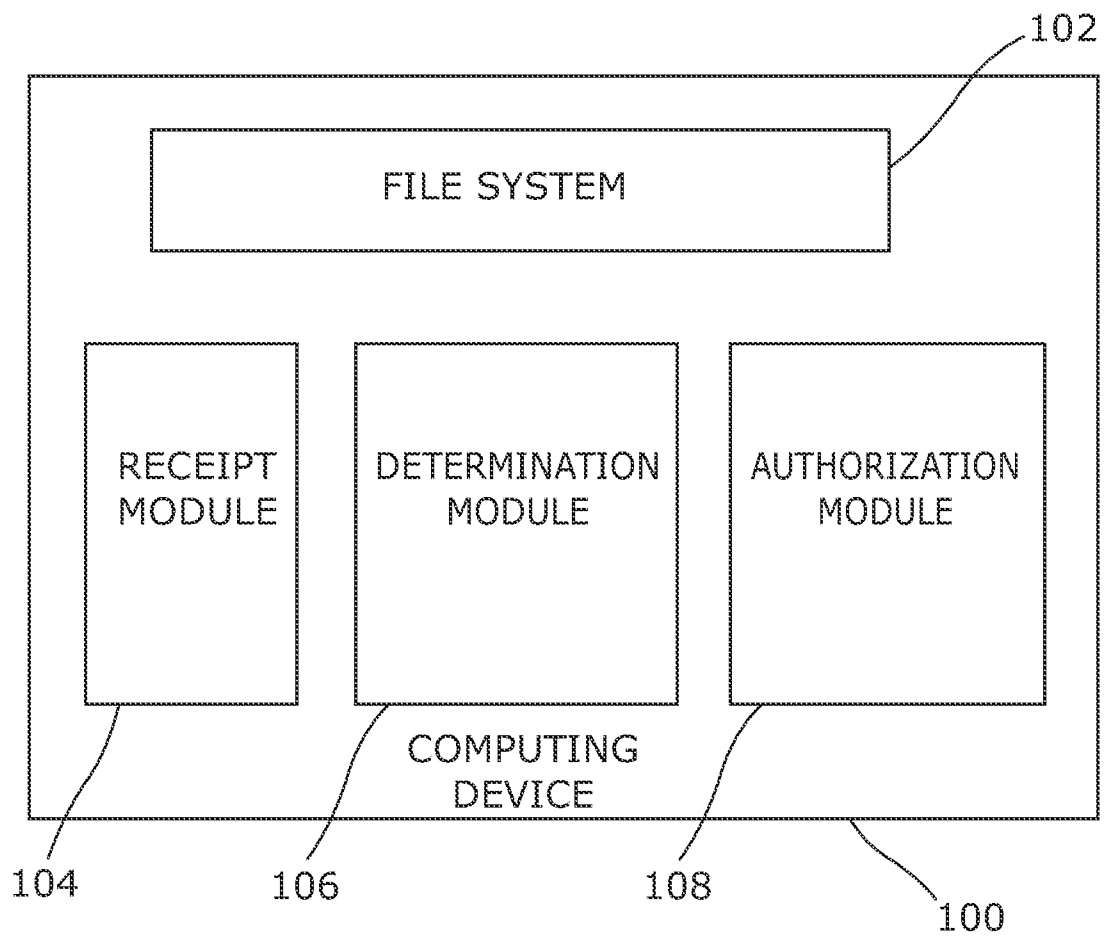


Fig. 1

2/3

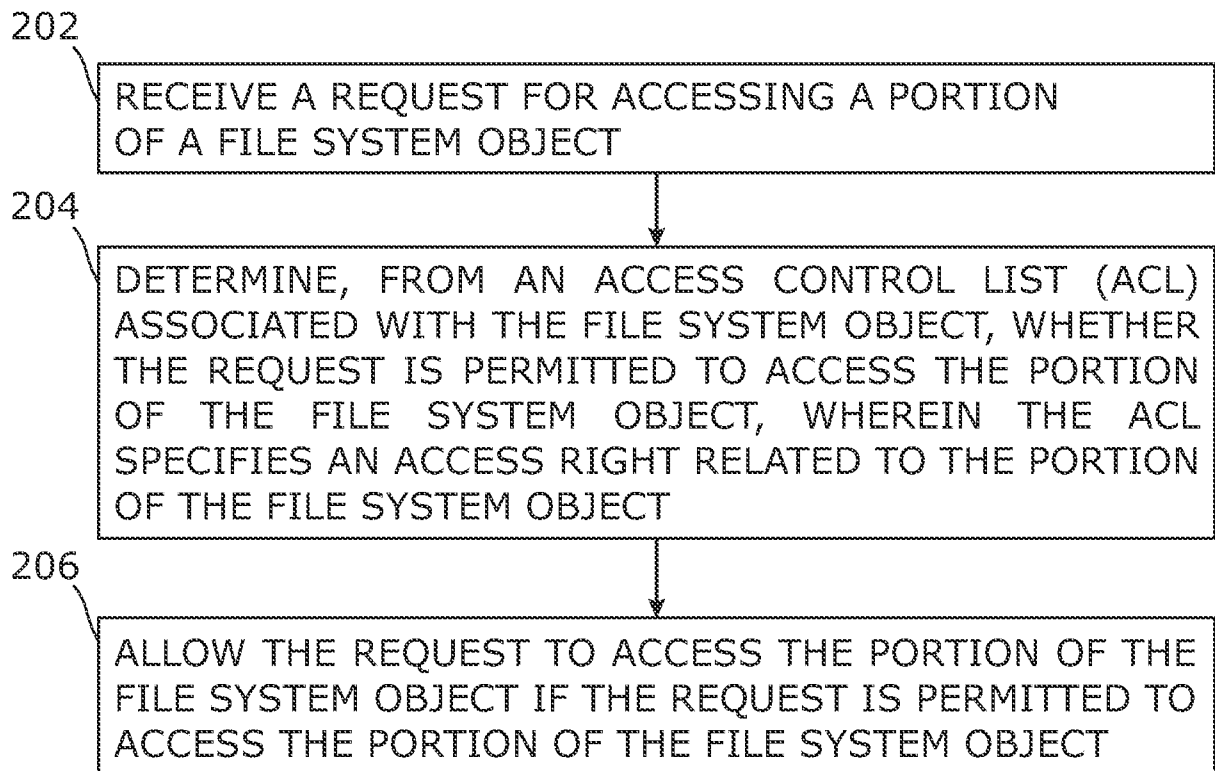
200

Fig. 2

3/3

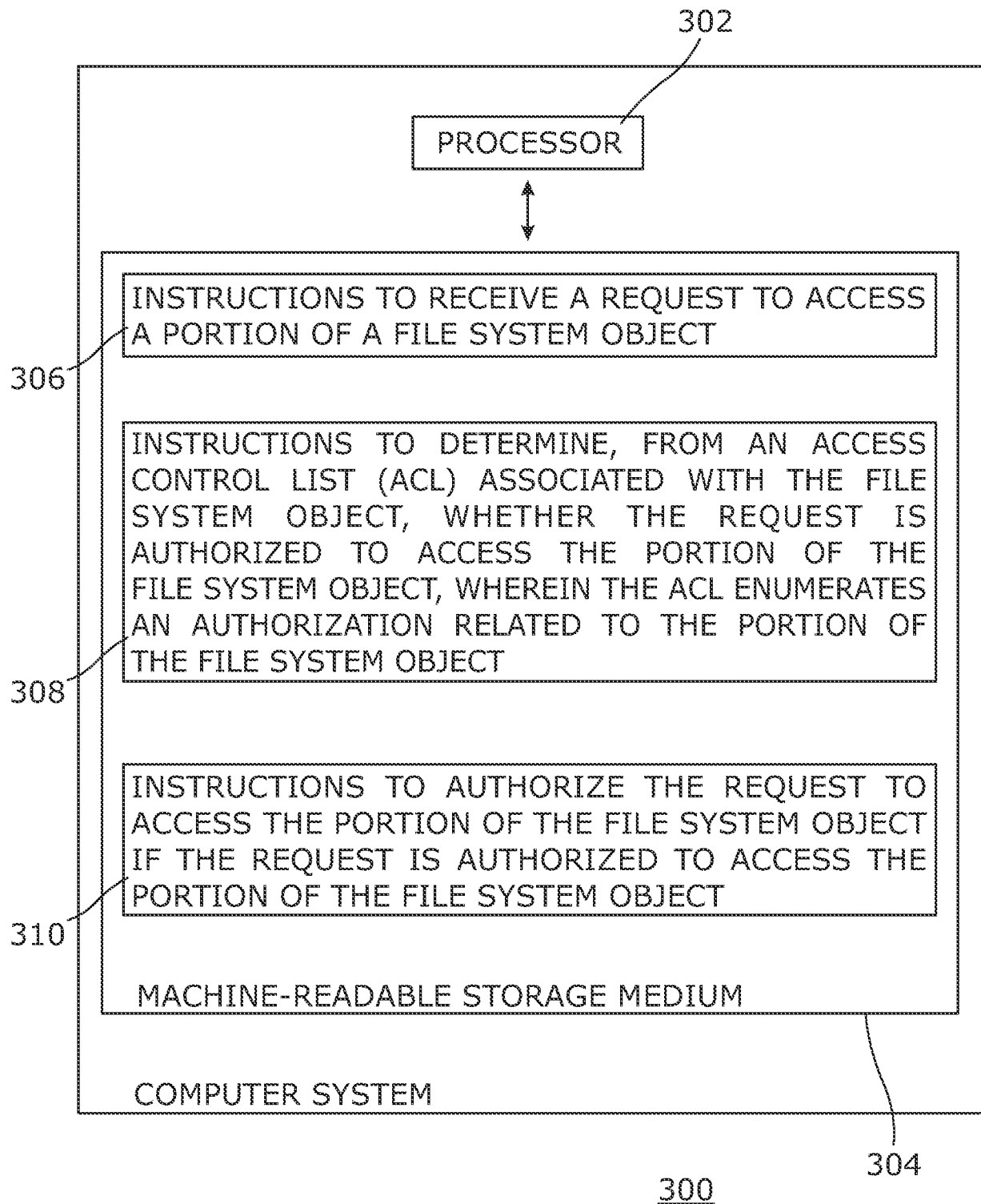


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/022071**A. CLASSIFICATION OF SUBJECT MATTER****G06F 17/30(2006.01)i, G06F 21/30(2013.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHEDMinimum documentation searched (classification system followed by classification symbols)
G06F 11/30; G06F 12/00; G06F 12/14; G06F 15/16; G06F 17/30; G06F 21/30; H04L 9/32Documentation 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 modelsElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: file system object, portion, Access Control List (ACL), permission, and similar terms.**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008-0066185 A1 (LESTER, JAMES et al.) 13 March 2008 See paragraphs [0001], [0016], [0025]-[0026], [0030], [0036]-[0039], [0041], and [0050]-[0053]; claims 1, 4-5, and 7; and figures 1-3 and 5.	1-15
A	US 2014-0149461 A1 (WIJAYARATNE, RAVI et al.) 29 May 2014 See paragraphs [0037]-[0039], [0049], and [0064]-[0066]; and figures 3 and 5.	1-15
A	US 2007-0233957 A1 (LEV-RAN, ETAI et al.) 04 October 2007 See paragraphs [0052]-[0068] and figures 2A-2B.	1-15
A	US 2009-0055921 A1 (FIELD, SCOTT A. et al.) 26 February 2009 See paragraphs [0068]-[0082] and figures 6-8.	1-15
A	US 8,601,283 B2 (JOGAND-COULOMB, FABRICE et al.) 03 December 2013 See column 10, line 7 - column 11, line 57; column 12, lines 9-64; and figures 5-6.	1-15



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

12 June 2015 (12.06.2015)

Date of mailing of the international search report

15 June 2015 (15.06.2015)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

NHO, Ji Myong

Telephone No. +82-42-481-8528



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/022071

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0066185 A1	13/03/2008	CN 101512479 A CN 101512479 B WO 2008-033445 A2 WO 2008-033445 A3	19/08/2009 11/04/2012 20/03/2008 16/10/2008
US 2014-0149461 A1	29/05/2014	None	
US 2007-0233957 A1	04/10/2007	US 7506102 B2	17/03/2009
US 2009-0055921 A1	26/02/2009	US 8214641 B2 WO 2009-026027 A2 WO 2009-026027 A3	03/07/2012 26/02/2009 16/04/2009
US 8601283 B2	03/12/2013	CN 100583117 C CN 101120352 A CN 101120352 B CN 101120353 A CN 101120355 A CN 101120355 B CN 101120356 A CN 101819612 A CN 101819612 B CN 101908106 A CN 101908106 B EP 1836640 A2 EP 1836641 A2 EP 1836642 A2 EP 1836643 A2 EP 2189922 A2 EP 2189922 A3 EP 2284758 A2 EP 2284758 A3 JP 2008-524753 A JP 2008-524755 A JP 2008-524757 A JP 2008-524758 A JP 2010-182322 A JP 4847967 B2 JP 4848039 B2 JP 4857283 B2 JP 4857284 B2 KR 10-1213118 B1 KR 10-1214497 B1 KR 10-1238848 B1 KR 10-2007-0087175 A KR 10-2007-0091349 A TW 200700991 A TW 200700992 A TW 200702997 A	20/01/2010 06/02/2008 06/10/2010 06/02/2008 06/02/2008 26/09/2012 06/02/2008 01/09/2010 25/09/2013 08/12/2010 05/06/2013 26/09/2007 26/09/2007 26/09/2007 26/09/2007 26/05/2010 02/06/2010 16/02/2011 05/10/2011 10/07/2008 10/07/2008 10/07/2008 10/07/2008 19/08/2010 28/12/2011 28/12/2011 18/01/2012 18/01/2012 24/12/2012 24/12/2012 04/03/2013 27/08/2007 10/09/2007 01/01/2007 01/01/2007 16/01/2007

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/022071Patent document
cited in search reportPublication
datePatent family
member(s)Publication
date

TW I388985 B	11/03/2013
US 2006-0242064 A1	26/10/2006
US 2006-0242065 A1	26/10/2006
US 2006-0242066 A1	26/10/2006
US 2006-0242067 A1	26/10/2006
US 2006-0242068 A1	26/10/2006
US 2006-0242150 A1	26/10/2006
US 2006-0242151 A1	26/10/2006
US 2007-0168292 A1	19/07/2007
US 2010-0077214 A1	25/03/2010
US 2014-0115698 A1	24/04/2014
US 8051052 B2	01/11/2011
US 8504849 B2	06/08/2013
WO 2006-069194 A2	29/06/2006
WO 2006-069194 A3	23/11/2006
WO 2006-069274 A2	29/06/2006
WO 2006-069274 A3	26/10/2006
WO 2006-069311 A2	29/06/2006
WO 2006-069311 A3	16/11/2006
WO 2006-069312 A2	29/06/2006
WO 2006-069312 A3	09/11/2006