



- (51) **International Patent Classification:**
G06F 17/00 (2006.01) *G06F 17/30* (2006.01)
- (21) **International Application Number:**
PCT/US2014/032167
- (22) **International Filing Date:**
28 March 2014 (28.03.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/806,079 28 March 2013 (28.03.2013) US
- (71) **Applicant:** GOOGLE INC. [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).
- (72) **Inventors:** VONGSOUVANH, Alain; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). JORGENSEN, Russell, Blaine; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). WYRICK, Robert, Eugene; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). HICKS, Justin, Lee; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US). CLARK, Stephen, Nowland; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).
- (74) **Agents:** INGERMAN, Jeffrey, H. et al.; Ropes & Gray LLP, 1211 Avenue of the Americas, New York, NY 10036 (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, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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).

Published:

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

[Continued on next page]

(54) **Title:** SYSTEM AND METHOD TO STORE THIRD-PARTY METADATA IN A CLOUD STORAGE SYSTEM

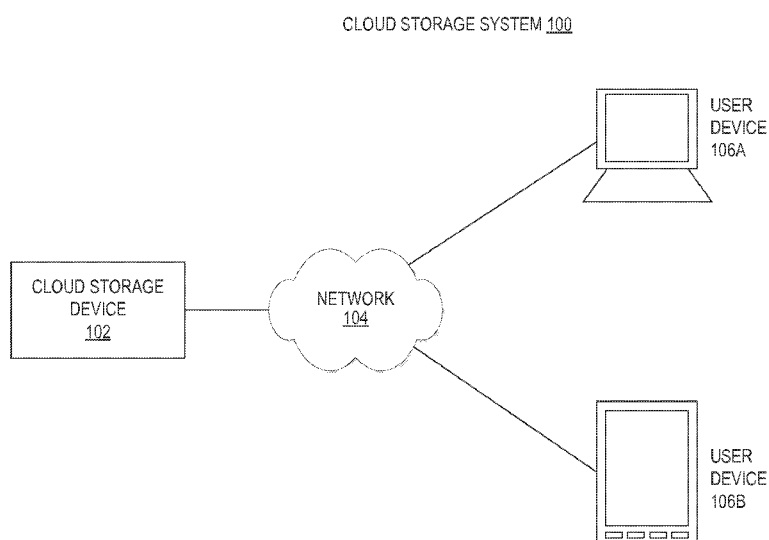


Fig. 1

(57) **Abstract:** A cloud storage system identifies and creates metadata associated with a stored file. On receiving a request to access the file with an application, the cloud storage system generates a metadata category associated only with the application, and creates metadata associated with the generated metadata category and corresponding to the file. On receiving a request to access file metadata, the cloud storage system identifies an application associated with the metadata access request, identifies a set of metadata categories associated with the identified application, filters metadata associated with the file based on the identified set of metadata categories, and provides the filtered metadata to the application.





-
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

System and Method to Store Third-Party Metadata in a Cloud Storage System

Cross-Reference to Related Applications

[0001] This application claims priority to U.S. Provisional Application Serial No. 61/806,079, filed on March 28, 2013, entitled "System and Method to Store Third-Party Metadata in a Cloud Storage System," the entire contents of which are hereby incorporated by reference.

Background

[0002] Personal computers traditionally store files locally on a medium directly accessed by the computer generating or editing the files. As network access has become more widespread, it has become feasible to store files on a remote network. Storing files on a remote network, also referred to as cloud storage, allows a user to access the files using any device that can access the network. Such cloud storage systems reduce the user's need for local storage capacity and assure the user that, regardless of which device is accessing a file, an up-to-date copy of the file is being accessed.

[0003] Existing cloud storage systems limit the metadata associated with the files they store. Such systems may record information corresponding to different metadata categories, such as a name of the file, a creation date of the file, the last time the contents of the file were modified, or other suitable information that is typically limited to a set of predetermined categories of metadata. Applications interacting with the files stored in existing cloud storage systems are therefore restricted to either using the predetermined metadata categories or relying on a second storage system to keep track of metadata that the cloud storage system does not store.

Summary

[0004] Thus there exists a need in the art to allow applications to generate and interact with alternative metadata categories. The systems and methods described herein allow a cloud storage system to store third-party-generated metadata that is associated with a file but may not be associated with a predefined metadata category. The systems and methods described herein further allow a cloud storage system to identify files to third-party applications based on one or more metadata elements.

[0005] In certain aspects, the systems and methods described herein relate to providing metadata associated with a file stored on a cloud storage system to an application. Metadata may include a text string, a numerical value, a date or time, or other suitable information, and in some implementations some metadata may change as a predetermined function of time. The cloud storage system may include a communication processor that receives a request to access metadata associated with the file. The communication processor identifies a first application associated with the request, and identifies a first set of metadata categories associated with the first application. The communication processor filters metadata associated with the file based on the first set of metadata categories, and provides the filtered metadata to the application. In some implementations, the communication processor also identifies whether a user is associated with a metadata category and which user is associated with the request, and such information may also be used to filter metadata associated with the file. In some implementations, the communication processor also generates both metadata categories in the first set of metadata categories and metadata in such categories. In some such implementations, the communication processor also deletes such metadata categories when a user revokes permission of their associated application to access the file.

[0006] In certain aspects, the systems and methods described herein relate to creating metadata associated with a file stored on a cloud storage system. The cloud storage system

may include a communication processor that receives a request to access the file with an application. The communication processor identifies the application and generates a metadata category associated only with the identified application. The communication processor creates metadata associated with the generated metadata category and

5 corresponding to the file. In some implementations, the communication processor deletes the metadata category in response to a user revoking permission of the application to access the file.

Brief Description of the Drawings

[0007] The systems and methods described herein are set forth in the appended claims.

10 However, for the purpose of explanation, several embodiments are set forth in the following drawings.

[0008] FIG. 1 is a block diagram of a cloud storage system, according to an illustrative implementation;

[0009] FIG. 2 is a block diagram of a cloud storage engine, according to an illustrative
15 implementation;

[0010] FIG. 3 is a table depicting an exemplary file database storing the contents of and metadata associated with files, according to an illustrative implementation;

[0011] FIG. 4 is a flow chart of a process for searching for files on a cloud storage system based on metadata associated with the files, according to an illustrative implementation;

20 [0012] FIG. 5 is a flow chart of a process for providing access to metadata associated with a file on a cloud storage system, according to an illustrative implementation;

[0013] FIG. 6 is a flow chart of a process for editing metadata associated with a file stored on a cloud storage system, according to an illustrative implementation; and

[0014] FIG. 7 is a block diagram of a computing device for performing any of the processes
25 described herein, according to an illustrative implementation.

Detailed Description

[0015] In the following description, numerous details are set forth for the purpose of explanation. However, one of ordinary skill in the art will realize that the implementations described herein may be practiced without the use of these specific details and that the implementations described herein may be modified, supplemented, or otherwise altered without departing from the scope of the systems and methods described herein.

[0016] The systems and methods described herein relate to accessing and editing metadata associated with a file stored on a cloud storage system. The cloud storage system may allow applications to create application-specific metadata for a file, and may further identify files based on general or application-specific metadata. The cloud storage system may restrict which users or which applications may access or alter metadata associated with certain metadata categories.

[0017] Figure 1 is an illustrative block diagram of a cloud storage system 100, which provides remote storage of and access to computer files. Computer files may include text, pictures, audio files, video files, presentation files, spreadsheets, binary data files, computer instructions, HyperText Markup Language (HTML) files, or other suitable files. Files are stored on cloud storage device 102, which may include a server, a personal computer, a mainframe, a cluster of computing devices, or some other suitable computing device, and which is described in more detail in relation to FIG. 2. Files may be uploaded to or accessed from cloud storage device 102 via network 104. Network 104 is a computer network, and in certain implementations may be the Internet. As depicted, user devices 106A and 106B (collectively user devices 106) may interact with cloud storage device 102 through network 104.

[0018] A user device 106 is a computing device that may be used to access cloud storage device 102, and may be a personal laptop computer, a personal desktop computer, a tablet

computer, a smartphone, or some other suitable computing device. User device 106 may include installed applications, or may have access to applications that are capable of accessing or altering files stored on cloud storage device 102. In certain implementations, user device 106 may store information regarding one or more users, the data processing capacity of user device 106, a list of installed applications, a list of file types accessible by each installed application, the categories of metadata used by each installed application, or other suitable information regarding the capability of user device 106 to access files stored on cloud storage device 102. In such implementations, user device 106 may be configured to transmit a portion or the whole of such information upon first connecting to cloud storage device 102, in response to a query by cloud storage device 102, or under other suitable circumstances.

[0019] Cloud storage system 100 stores computer files and allows a user to access the files with a remote user device 106. A user device 106 connects to cloud storage device 102 through network 104. An application on user device 106 may generate, access, edit, or delete metadata associated with a file stored on cloud storage device 102.

[0020] Figure 2 is an illustrative block diagram of a cloud storage engine 200, which may act as the cloud storage device 102 of FIG. 1. Cloud storage engine 200 allows user device 106 to access files over network 104. Cloud storage engine 200 transmits and receives data through communication port 202. Communication processor 204 identifies user instructions received through communication port 202 and stores or transmits information based on the received instructions. The content and metadata of files may be stored in file database 206, user information may be stored in user database 208, and information regarding applications may be stored in application database 210. Authentication processor 212 may verify that a request to access or edit information associated with cloud storage engine 200 is authorized.

[0021] The depicted communication port 202 is a network port which receives user commands via network 104 and transmits information sent by cloud storage engine 200. Communication port 202 may include a 100BASE-TX port, a 1000BASE-T port, a 10GBASE-T port, a Wi-Fi antenna, a cellular antenna, or other suitable network ports. In certain implementations, there may be a different number of ports than are depicted. In certain implementations, communication port 202 may provide secure communications, such as by using the Secure Sockets Layer (SSL) protocol, the Transport Layer Security (TLS) protocol, or other suitable protocol.

[0022] Communication processor 204 may be a computer processor which identifies instructions received through communication port 202 and may store or transmit information in response. Upon a user connecting to cloud storage engine 200, communication processor 204 may identify the user, in certain implementations by comparing login information provided by the user to information stored in user database 208. Communication processor 204 may further identify the user device 106 or an application thereon from packet headers identifying the source of data received from the user, by querying the user device 106, from information provided by the user device 106 at login, or through some other suitable method of identifying the user device or an application thereon. Communication processor 204 may respond to a user command by identifying files having metadata that meets criteria provided in the user command, by transmitting metadata associated with one or more files to a user, by editing metadata associated with a file, or by some other suitable measure according to the command. Communication processor 204 may also provide access to or edit content of a file according to a user command, which in some implementations may also cause communication processor 204 to edit metadata associated with the file. As an illustrative example of such implementations, upon implementing a user edit to the content of a file,

communication processor 204 may also adjust metadata indicating the last time the file was edited.

[0023] File database 206 may be a computer-readable and -writable medium storing at least one file associated with a cloud storage system 100. In some implementations, a portion of file database 206 may be accessed through a remote network. Such a portion may be a third-party database. Files stored on file database 206 may include text, images, audio files, video files, spreadsheets, presentation files, HTML files, or other suitable computer files. File database 206 may also store metadata associated with each file. Each item of metadata may correspond to a metadata category, such as a Multipurpose Internet Mail Extensions (MIME) type of the file, the time at which the file was generated, or other suitable metadata category. A metadata category may be associated with every file in file database 206 or with only a portion of the files in file database 206. As an illustrative example, each file in file database 206 may have a file identifier, while only files associated with a particular application may be associated with a metadata category unique to the application. In certain implementations, metadata may be stored in a database separate from file database 206.

[0024] Each category of metadata may be general or application-specific. General metadata may be accessible to any application associated with the file, and in some implementations any application associated with the file may edit general metadata. Application-specific metadata may be accessible to and edited by a single application. In some implementations, application-specific metadata may be accessible to a set of applications. In some such implementations, a subset of the applications may edit the application-specific metadata. File database 206 may store information indicating whether a category of metadata is general or application-specific, and with which application or set of applications an application-specific category of metadata is associated. In some implementations, any application may generate general metadata categories. In some

implementations, information about whether metadata is general or application-specific may be stored in application database 210.

[0025] Each category of metadata may also be public or private. Public metadata may be accessed by any user with permission to access the file, while private metadata may only be
5 accessed by an owner of the metadata or a user that the owner authorized to access the private metadata. As an illustrative example, a filename may be public metadata, while metadata indicating the stage of a document within a workflow may be private metadata. File database 206 may store information indicating whether a category of metadata is public or private, and which user or set of users may access or edit public or private metadata. In some
10 implementations, information about whether metadata is public or private may be stored in user database 208.

[0026] In some implementations, a metadata category may be associated with another metadata category. As an illustrative example of such implementations, a first metadata category may indicate a document priority, while a second metadata category may indicate a
15 deadline after which the document priority will change.

[0027] User database 208 may be a computer-readable and -writable medium storing information associated with at least one user of cloud storage engine 200. The information may include one or more of a username and password associated with a user, a list of the files associated with each user, a list of at least one user device 106 associated with the user, a list
20 of applications available to a user, a list of each application the user has authorized to access each file or file type represented in the user's files, user-specified preferences, or other suitable user information.

[0028] Application database 210 may be a computer-readable and -writable medium storing information regarding applications associated with cloud storage engine 200. Application
25 database 210 may store metadata associated with an application, which may include metadata

categories visible to the application, metadata categories that may be edited by the application, file types the application is capable of opening, the users authorized to use the application, or other suitable information. In some implementations, application database 210 may include compiled or uncompiled computer instructions comprising an application, a link to access a cloud application, a link to download a native application, an icon associated with the application, a description of the application, or other suitable information regarding an application. In some implementations, some applications may be stored as computer instructions that may be performed by a web browser run on a user device 106, which may be written in HTML, JavaScript, Asynchronous JavaScript and XML (Ajax), or another suitable computer language. In some such implementations, a stored application may be executed by cloud storage engine 200 and one or more outputs from the application may be transmitted to a user device 106.

[0029] Authentication processor 212 may be a computer processor that blocks unauthorized access or editing of information associated with cloud storage engine 200. Unauthorized access may be detected by comparing one or more of a username and password combination, information identifying a user device 106, geographic information associated with the user device 106, or other suitable information with information stored in user database 208. If a request to access or edit information is not successfully verified, authentication processor 212 may transmit a message to the user or a system administrator, block user device 106, temporarily lock the user account, or take some other predetermined action. In certain implementations, if a user device 106 has not previously been connected to cloud storage engine 200, authentication processor 212 may require the user to provide identification information, which may include a username and password combination, an identification number provided to the user by a voice or text message sent to a telephone number previously provided by the user, or other predetermined identification information. In certain

implementations, authentication processor 212 may verify that an application may be allowed to access or edit contents or metadata of a file by searching file database 206, user database 208, and application database 210 to determine whether the application is associated with the user who generated the request, whether the user is permitted to access or alter the file, whether the application is associated with the category of metadata being accessed or edited, whether the user has authorized the application to access the file or the file type, or other suitable verification information. In some such implementations, authentication processor 212 may verify a security token provided by the application against information stored in one or more of file database 206, user database 208, or application database 210. If an application is not authorized to access information, authentication processor 212 may prevent the application from accessing the information, transmit a message to the user or a system administrator, or take some other suitable action. In certain implementations, such a message to the user may ask if the user wishes to authorize the application to access the information. In certain implementations, authentication processor 212 may establish a secure connection with user device 106 using a protocol such as the SSL or TLS protocols.

[0030] Cloud storage engine 200 receives transmissions from user device 106 at communication port 202 via network 104. Communication processor 204 may identify an account associated with a user upon the establishment of a connection with a user device 106, and authentication processor 212 may compare information provided by user device 106 with information stored in user database 208 to verify that the user has access to the account. Communication processor 204 may identify files based on metadata associated with the file. Authentication processor 212 may verify that requests to access or edit one or more metadata categories associated with a file were generated by a user and an application authorized to access or edit the metadata categories, and, if the request is successfully verified, communication processor 204 may implement the request.

[0031] Figure 3 is an illustrative table depicting a file database 300, such as the file database 206 described in relation to FIG. 2. As depicted, file database 300 stores files 302A, 302B, and 302C, collectively files 302. For each file 302, file database 300 records the content 304 of the file as well as three categories of metadata describing each file. Metadata category 306 is a public, general category, and indicates the name of the file 302. Metadata category 308 is a public, general category, and indicates the type of the file 302. Metadata category 310 is a private, application-specific category, and indicates which user is next in line to approve the associated file 302. Thus, an authorized search for files with “Kate” as their metadata in metadata category 310 would return files 302A and 302B, while a similar search for image files named “Lorem” would return no files. The metadata categories here depicted may vary in number, whether they are public or private, whether they are general or application-specific, and in the information they record. Likewise, the number, content, and associated metadata of files 302 may vary from how they are here depicted. As an illustrative example, file 302A may be associated with application-specific metadata associated with metadata category 310, while file 302B may not be associated with any application-specific metadata at all. In some implementations, metadata in a metadata category may vary with time. As an illustrative example of such implementations, a metadata category may indicate the priority of a document, which may increase with time.

[0032] Figure 4 is an illustrative flow chart of a metadata search process 400. Metadata search process 400 identifies one or more files matching criteria provided by a user or an application. Referring also to FIG. 2, metadata search process 400 begins with step 401, in which communication processor 204 receives a request to identify one or more files based on metadata criteria. The request may be generated by a user through an application run on or provided to user device 106, and the application may be an operating system, a web browser, a document editing application, or some other suitable application. Metadata criteria may

include one or more of a text string associated with a metadata category, a range of numerical values associated with a metadata category, a range of dates and times associated with a metadata category, the absence of a text string associated with a metadata category, or other suitable criteria.

5 **[0033]** In step 402, communication processor 204 identifies the user and the application associated with the request based on the source of the request, a token associated with the request, or some other suitable indicator. In step 403, authentication processor 212 verifies that both the user and the application generating the request are authorized to access the metadata categories associated with the request made in step 401. If the request is made by
10 an unauthorized user or application, metadata search process 400 ends with communication processor 204 taking remedial action in step 404. The remedial action may include indicating that there are no files meeting the criteria of step 401, blocking the application from accessing cloud storage engine 200, alerting the user or a system administrator, transmitting a message to the user informing them how they may gain access to the file, or some other appropriate
15 action. If authentication processor 212 instead verifies that the user and the application are authorized to access the varieties of metadata indicated in the search of step 401, metadata search process 400 continues to step 405.

[0034] In step 405, communication processor 204 determines which files are available to the user identified in step 402. The determination may be based on user-related metadata
20 stored in file database 206 or in a listing of files associated with a user stored in user database 208. In step 406, communication processor 204 then identifies which of the available files meet the requested metadata criteria. This information may be provided to a user or to an application as a list of filenames or other file identifiers. In some implementations, the list may also provide information such as the metadata associated with the criteria of step 401.

[0035] Figure 5 is an illustrative flow chart of a metadata access process 500. Metadata access process 500 provides metadata associated with one or more files. Referring also to FIG. 2, metadata access process 500 begins with step 501, in which communication processor 204 receives a request for access to metadata associated with a file. The request may be generated by a user through an application run on or provided to user device 106, and the application may be an operating system, a web browser, a document editing application, or some other suitable application.

[0036] In step 502, communication processor 204 identifies the user and the application associated with the request based on the source of the request, a token associated with the request, or some other suitable indicator. In step 503, authentication processor 212 verifies that both the user and the application generating the request are authorized to access the metadata requested in step 501. If the request is made by an unauthorized user or application, metadata search process 500 ends with communication processor 204 taking remedial action in step 504. The remedial action may include indicating that the requested metadata is not available, blocking the application from accessing cloud storage engine 200, alerting the user or a system administrator, transmitting a message to the user informing them how they may gain access to the metadata, or some other appropriate action. If authentication processor 212 instead verifies that the user and the application are authorized to access the metadata requested in step 501, metadata search process 500 ends with step 505, in which communication processor 204 retrieves the requested metadata from file database 206 and provides it to the user through the application used to generate the request.

[0037] Figure 6 is an illustrative flow chart of a metadata edit process 600. Metadata edit process 600 edits metadata associated with a file. Referring also to FIG. 2, metadata edit process 600 begins with step 601, in which communication processor 204 receives a request to edit metadata associated with a file. The request may be generated by a user through an

application run on or provided to user device 106, and the application may be an operating system, a web browser, a document editing application, or some other suitable application.

[0038] In step 602, communication processor 204 identifies the user and the application associated with the request based on the source of the request, a token associated with the request, or some other suitable indicator. In step 603, authentication processor 212 verifies that both the user and the application generating the request are authorized to make the edit requested in step 601. If the request is made by an unauthorized user or application, metadata edit process 600 may end with communication processor 204 taking remedial action in step 604. The remedial action may include blocking the application from accessing cloud storage engine 200, alerting the user or a system administrator, transmitting a message to the user informing them how they may gain access to the file, or some other appropriate action. If authentication processor 212 instead verifies that the user and the application are authorized to make the edit requested in step 601, metadata edit process 600 continues to step 605.

[0039] In step 605, communication processor 204 determines whether the file is associated with the metadata category associated with the request of step 601. If so, metadata edit process 600 ends with step 606, in which communication processor 204 edits the metadata according to the request of step 601. If not, metadata process 600 continues to step 607, in which communication processor 204 determines whether the metadata quota associated with the file has been reached. A metadata quota may restrict the number of metadata categories associated with a file, the number of an application's application-specific metadata categories associated with a file, or otherwise restrict the metadata that may be associated with a file. As an illustrative example of a metadata quota, a file may be restricted to having one hundred metadata categories, with a maximum of thirty application-specific metadata categories associated with any one application. If there is space to store the metadata category, metadata edit process 600 ends with step 608, in which communication processor 204

generates the metadata category for the file and stores the requested metadata therein. Thus, the metadata stored in cloud storage engine 200 is not limited to a hardcoded set of metadata categories, but may accept arbitrary metadata categories generated by applications accessing cloud storage engine 200. In some implementations, there may be no quota, in which case
5 step 607 would always be followed by step 608. Otherwise, if storing the metadata would cause the metadata quota to be exceeded, metadata edit process ends with step 609, in which the request is denied. In step 609, communication processor 204 may transmit an error code to user device 106, generate a message indicating what metadata may be deleted to allow the request to be fulfilled, or generate some other suitable message to user device 106.

10 [0040] In some implementations, a metadata quota may also or alternatively limit the size of metadata associated with a file, such as the amount of memory available for a metadata category, the amount of memory available for all metadata associated with a file, or some other suitable limit. In such implementations, step 605 or step 607 may be followed by step 609 if the requested edit would cause the metadata quota to be exceeded.

15 [0041] Figure 7 is a block diagram of a computing device that can be used to implement or support any of the components of the system of FIG. 1 or 2, and for performing any of the processes described herein. Cloud storage engine 200 may be implemented on one or more computing devices 700 having suitable circuitry, and user device 106 may communicate with cloud storage device 102 through one or more computing devices 700 having suitable
20 circuitry. In certain aspects, a plurality of the components of cloud storage system 100 may be included within one computing device 700. In certain implementations, a component and a storage device may be implemented across several computing devices 700.

[0042] The computing device 700 comprises at least one communications interface unit, an input/output controller 710, system memory, and one or more data storage devices. This can
25 support a network connection such as a connection to network 104 in FIG. 1. The system

memory includes at least one random access memory (RAM 702) and at least one read-only memory (ROM 704). RAM 702 can support the file database 206 of FIG. 2, for example. All of these elements are in communication with a central processing unit (CPU 706) to facilitate the operation of the computing device 700. The computing device 700 may be
5 configured in many different ways. For example, the computing device 700 may be a conventional standalone computer or alternatively, the functions of computing device 700 may be distributed across multiple computer systems and architectures. In FIG. 7, the computing device 700 may be linked, via network or local network, to other servers or systems.

10 [0043] The computing device 700 may be configured in a distributed architecture, wherein databases and processors are housed in separate units or locations. Some units perform primary processing functions and contain, at a minimum, a general controller or a processor and a system memory. In distributed architecture implementations, each of these units may be attached via the communications interface unit 708 to a communications hub or port (not
15 shown) that serves as a primary communication link with other servers, client or user computers, and other related devices. The communications hub or port may have minimal processing capability itself, serving primarily as a communications router. A variety of communications protocols may be part of the system, including, but not limited to: Ethernet, SAP, SAS™, ATP, BLUETOOTH™, GSM, and TCP/IP.

20 [0044] The CPU 706 comprises a processor, such as one or more conventional microprocessors and one or more supplementary co-processors such as math co-processors for offloading workload from the CPU 706. The CPU 706 is in communication with the communications interface unit 708 and the input/output controller 710, through which the CPU 706 communicates with other devices such as other servers, user terminals, or devices.
25 The communications interface unit 708 and the input/output controller 710 may include

multiple communication channels for simultaneous communication with, for example, other processors, servers, or client terminals.

[0045] The CPU 706 is also in communication with the data storage device. The data storage device may comprise an appropriate combination of magnetic, optical, or semiconductor memory, and may include, for example, RAM 702, ROM 704, flash drive, an optical disc such as a compact disc, or a hard disk or drive. The CPU 706 and the data storage device each may be, for example, located entirely within a single computer or other computing device; or connected to each other by a communication medium, such as a USB port, serial port cable, a coaxial cable, an Ethernet cable, a telephone line, a radio frequency transceiver, or other similar wireless or wired medium or combination of the foregoing. For example, the CPU 706 may be connected to the data storage device via the communications interface unit 708. The CPU 706 may be configured to perform one or more particular processing functions.

[0046] The data storage device may store, for example, (i) an operating system 712 for the computing device 700; (ii) one or more applications 714 (e.g., computer program code or a computer program product) adapted to direct the CPU 706 in accordance with the systems and methods described here, and particularly in accordance with the processes described in detail with regard to the CPU 706; or (iii) database(s) 716 adapted to store information that may be utilized to store information required by the program. The depicted database 716 can be any suitable database system, and can be a local or distributed database system.

[0047] The operating system 712 and applications 714 may be stored, for example, in a compressed, an uncompiled and an encrypted format, and may include computer program code. The instructions of the program may be read into a main memory of the processor from a computer-readable medium other than the data storage device, such as from the ROM 704 or from the RAM 702, or from a computer data signal embodied in a carrier wave, such as

that found within the well-known Web pages transferred among devices connected to the Internet. While execution of sequences of instructions in the program causes the CPU 706 to perform the process steps described herein, hard-wired circuitry may be used in place of, or in combination with, software instructions for implementation of the processes of the present disclosure. Thus, the systems and methods described are not limited to any specific combination of hardware and software.

[0048] Suitable computer program code may be provided for performing one or more functions in relation to a cloud storage system as described herein. The program also may include program elements such as an operating system 712, a database management system, and "device drivers" that allow the processor to interface with computer peripheral devices (*e.g.*, a video display, a keyboard, a computer mouse, *etc.*) via the input/output controller 710.

[0049] The term "computer-readable medium" as used herein refers to any non-transitory medium that provides or participates in providing instructions to the processor of the computing device 700 (or any other processor of a device described herein) for execution.

Such a medium may take many forms, including but not limited to, non-volatile media and volatile media. Non-volatile media include, for example, optical, magnetic, or opto-magnetic disks, or integrated circuit memory, such as flash memory. Volatile media include dynamic random access memory (DRAM), which typically constitutes the main memory. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM or EEPROM (electronically erasable programmable read-only memory), a FLASH-EEPROM, any other memory chip or cartridge, or any other non-transitory medium from which a computer can read.

[0050] Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to the CPU 706 (or any other processor of a device described herein) for execution. For example, the instructions may initially be borne on a magnetic disk of a remote computer (not shown). The remote computer can load the
5 instructions into its dynamic memory and send the instructions over an Ethernet connection, cable line, or even telephone line using a modem. A communications device local to a computing device 700 (e.g., a server) can receive the data on the respective communications line and place the data on a system bus for the processor. The system bus carries the data to main memory, from which the processor retrieves and executes the instructions. The
10 instructions received by main memory may optionally be stored in memory either before or after execution by the processor. In addition, instructions may be received via a communication port as electrical, electromagnetic, or optical signals, which are exemplary forms of wireless communications or data streams that carry various types of information.

[0051] Some implementations of the above described may be implemented by the
15 preparation of application-specific integrated circuits or by interconnecting an appropriate network of conventional component circuits, as will be apparent to those skilled in the art. Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, requests, information, signals, bits, symbols, and chips that may be referenced
20 throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0052] While various embodiments of the present disclosure have been shown and described herein, it will be obvious to those skilled in the art that such embodiments are provided by way of example only. Numerous variations, changes, and substitutions will now
25 occur to those skilled in the art without departing from the disclosure. For example, users

may have metadata quotas rather than individual files, uninstalling an application or revoking its access to a file may delete application-specific metadata associated with the application, or changing metadata associated with a folder of the computer system may change corresponding metadata of the files contained within the folder. It should be understood that various alternatives to the embodiments of the disclosure described herein may be employed in practicing the disclosure. Elements of an implementation of the systems and methods described herein may be independently implemented or combined with other implementations. It is intended that the following claims define the scope of the disclosure and that methods and structures within the scope of these claims and their equivalents be covered thereby.

CLAIMS

We claim:

1. A computer-implemented method of providing metadata associated with a file stored on a cloud storage system to a first application, comprising:
 - 5 receiving a request to access metadata associated with the file;
 - identifying the first application, wherein the first application is associated with the request;
 - identifying a first set of metadata categories, wherein the first set of metadata categories is associated with the first application;
 - 10 filtering metadata associated with the file based on the first set of metadata categories; and
 - providing the filtered metadata to the first application.
2. The method of claim 1, further comprising:
 - generating the first set of metadata categories and a second set of metadata categories,
 - 15 wherein the second set of metadata categories is not associated with the first application;
 - and
 - generating metadata associated with the first application, wherein the generated metadata is in a metadata category in the first set of metadata categories.
3. The method of claim 1, wherein at least one metadata category in the first set of metadata categories is only associated with the first application.
- 20 4. The method of claim 1, wherein at least one metadata category in the first set of metadata categories is associated with a second application.
5. The method of claim 1, wherein at least one metadata category in the first set of metadata categories is associated with a first user.
- 25 6. The method of claim 5, further comprising:

identifying a second user associated with the request;
determining whether the second user is associated with the file; and
in response to determining that the second user is associated with the file,
providing the filtered metadata to the first application.

- 5 7. The method of claim 1, wherein metadata associated with at least one metadata category
in the first set of metadata categories is a predetermined function of time.
8. The method of claim 1, wherein metadata includes a text string.
9. The method of claim 1, wherein metadata includes a numerical value.
10. The method of claim 1, wherein metadata includes a date and time.
- 10 11. The method of claim 1, wherein a first metadata category in the first set of metadata
categories is associated with a second metadata category in the first set of metadata
categories.
12. The method of claim 1, further comprising verifying that the first application is
authorized to access the file.
- 15 13. A computer-implemented method of creating metadata associated with a file stored on a
cloud storage system, comprising:
receiving a request to access the file with an application;
identifying the application;
generating a metadata category associated only with the application; and
20 creating metadata associated with the metadata category and corresponding to the
file.
14. The method of claim 13, wherein the file is associated with a first user and the application
is associated with a second user.
15. The method of claim 14, wherein the second user is not allowed to edit any content
25 associated with the file.

16. The method of claim 13, wherein the metadata is based on a folder containing the file.
17. The method of claim 13, further comprising deleting the metadata category in response to a user revoking permission of the application to access the file.
18. A cloud storage system, comprising:
- 5 a communication processor in communication with:
- a file database for storing a plurality of files and metadata associated with each of the plurality of files; and
- a user database for storing information associating at least one user with at least one file,
- 10 wherein the communication processor is configured to:
- receive a request to access metadata associated with a file in the plurality of files;
- identify a first application associated with the request;
- identify a first set of metadata categories, wherein the first set of metadata
- 15 categories is associated with the first application;
- filter metadata associated with the file based on the first set of metadata categories; and
- provide the filtered metadata to the first application.
19. The system of claim 18, wherein the communication processor is further configured to
- 20 generate a metadata category in the first set of metadata categories.
20. The system of claim 19, wherein the communication processor is further configured to delete the metadata category in response to a user revoking permission of the first application to access the file.

21. The system of claim 19, wherein the communication processor is further configured to generate a second set of metadata categories, wherein the second set of metadata categories is not associated with the first application.
22. The system of claim 18, wherein at least one metadata category in the first set of metadata categories is only associated with the first application.
23. The system of claim 18, wherein at least one metadata category in the first set of metadata categories is associated with a second application.
24. The system of claim 18, wherein at least one metadata category in the first set of metadata categories is associated with a first user.
25. The system of claim 24, wherein the communication processor is further configured to:
identify a second user associated with the request;
determine whether the second user is associated with the file; and
provide the filtered metadata to the first application in response to determining that the second user is associated with the file.
26. The system of claim 18, wherein the communication processor is further configured to edit metadata associated with the file in response to the request.
27. The system of claim 18, wherein metadata associated with at least one metadata category in the first set of metadata categories is a predetermined function of time.
28. The system of claim 18, wherein metadata includes a text string.
29. The system of claim 18, wherein metadata includes a numerical value.
30. The system of claim 18, wherein metadata includes a date and time.
31. The system of claim 18, wherein a first metadata category in the first set of metadata categories is associated with a second metadata category in the first set of metadata categories.
32. The system of claim 18, wherein:

the file database is further configured for storing a folder associated with one or more files and metadata associated with the folder, and

the communication processor is further configured to edit one or more metadata categories based on metadata associated with the folder.

- 5 33. The system of claim 18, wherein the communication processor is further configured to verify that the first application is authorized to access the file.

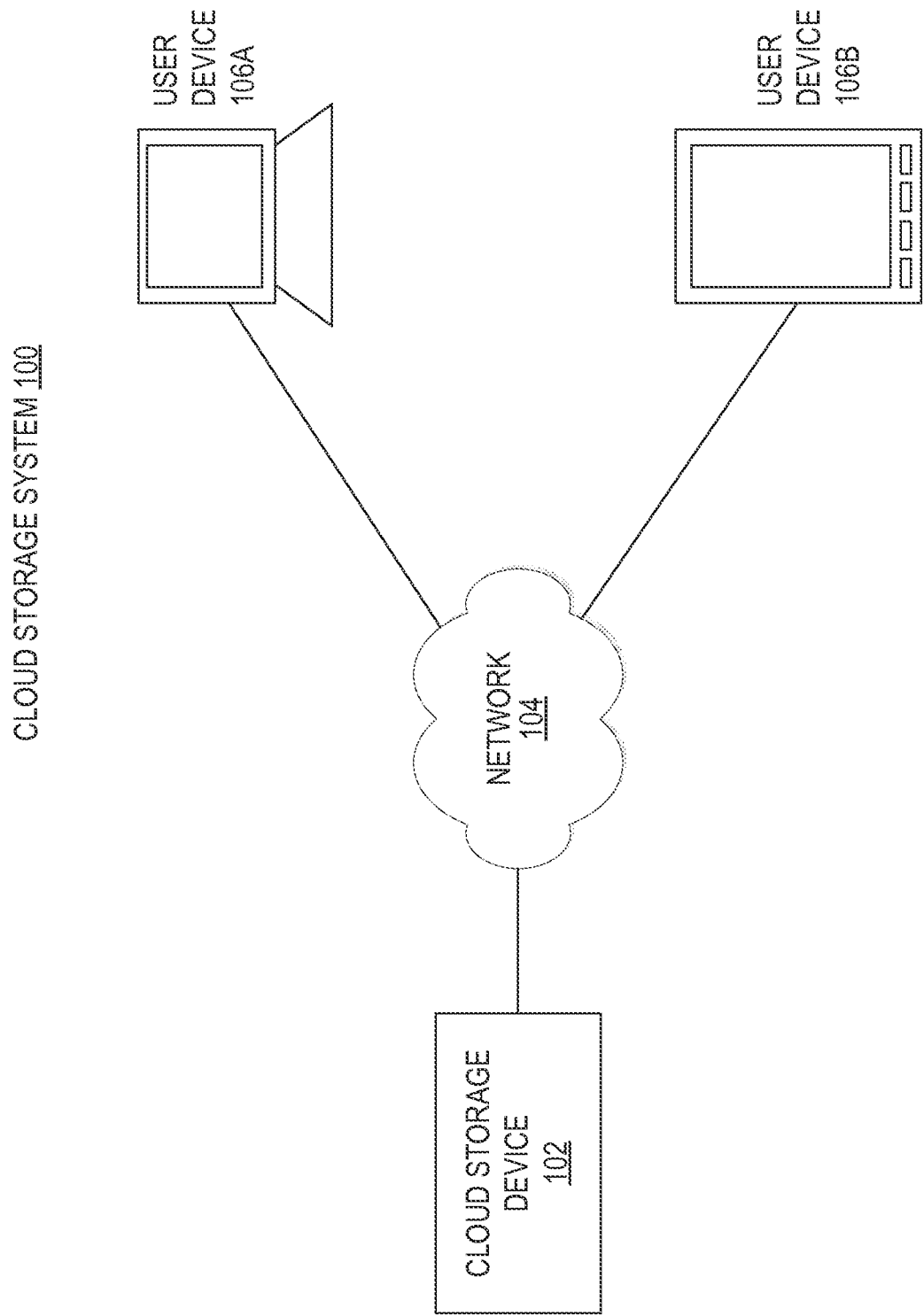


Fig. 1

CLOUD STORAGE ENGINE 200

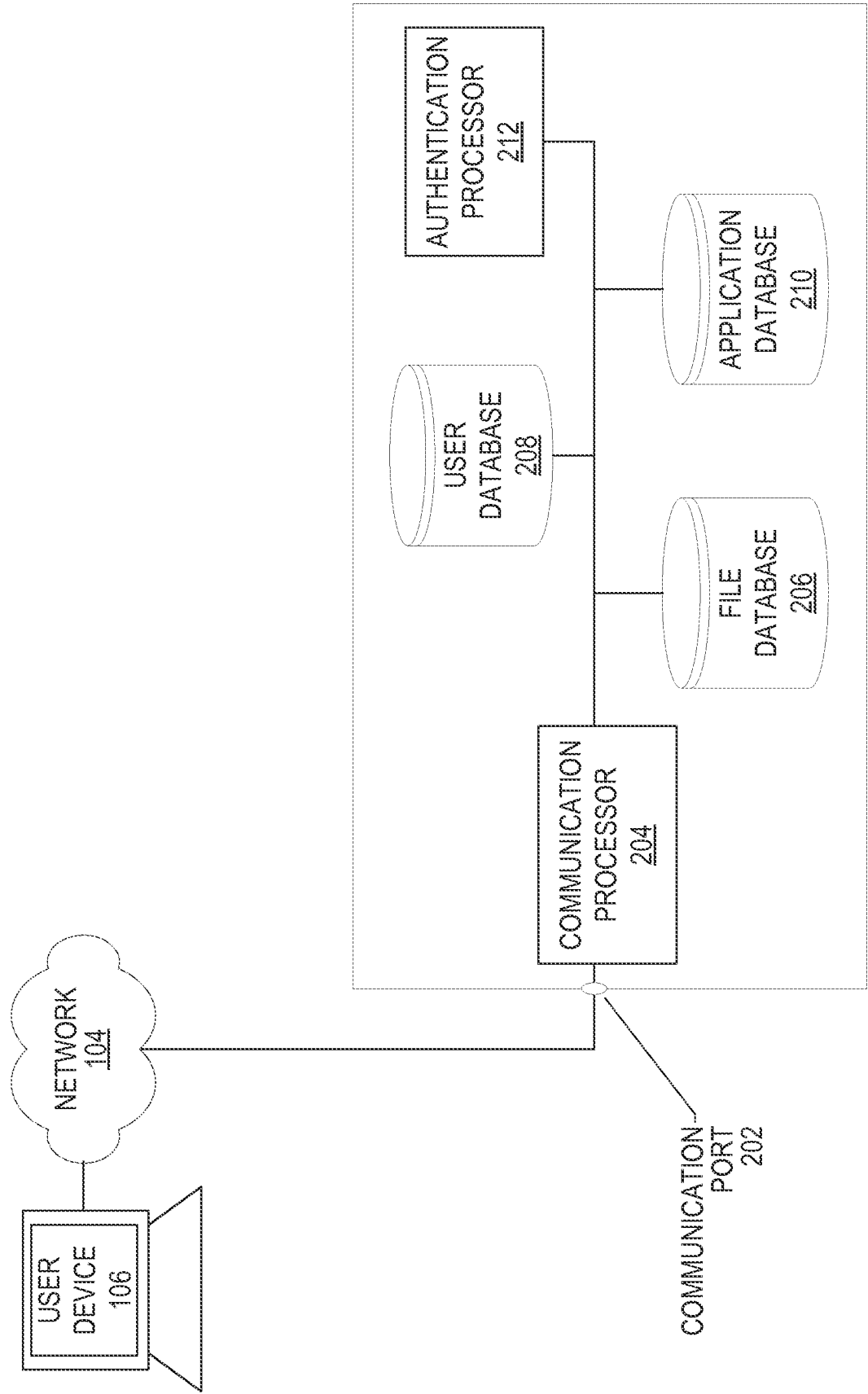


Fig. 2

FILE DATABASE 300

<u>304</u> CONTENT	<u>306</u> PUBLIC: GENERAL: NAME	<u>308</u> PUBLIC: GENERAL: TYPE	<u>310</u> PRIVATE: APPLICATION-SPECIFIC: NEXTAPPROVAL
#####	LOREM	TEXT	KATE
#####	IPSUM	IMAGE	KATE
#####	DOLOR	AUDIO	PAT

FILE 302A
FILE 302B
FILE 302C

Fig. 3

METADATA SEARCH PROCESS 400

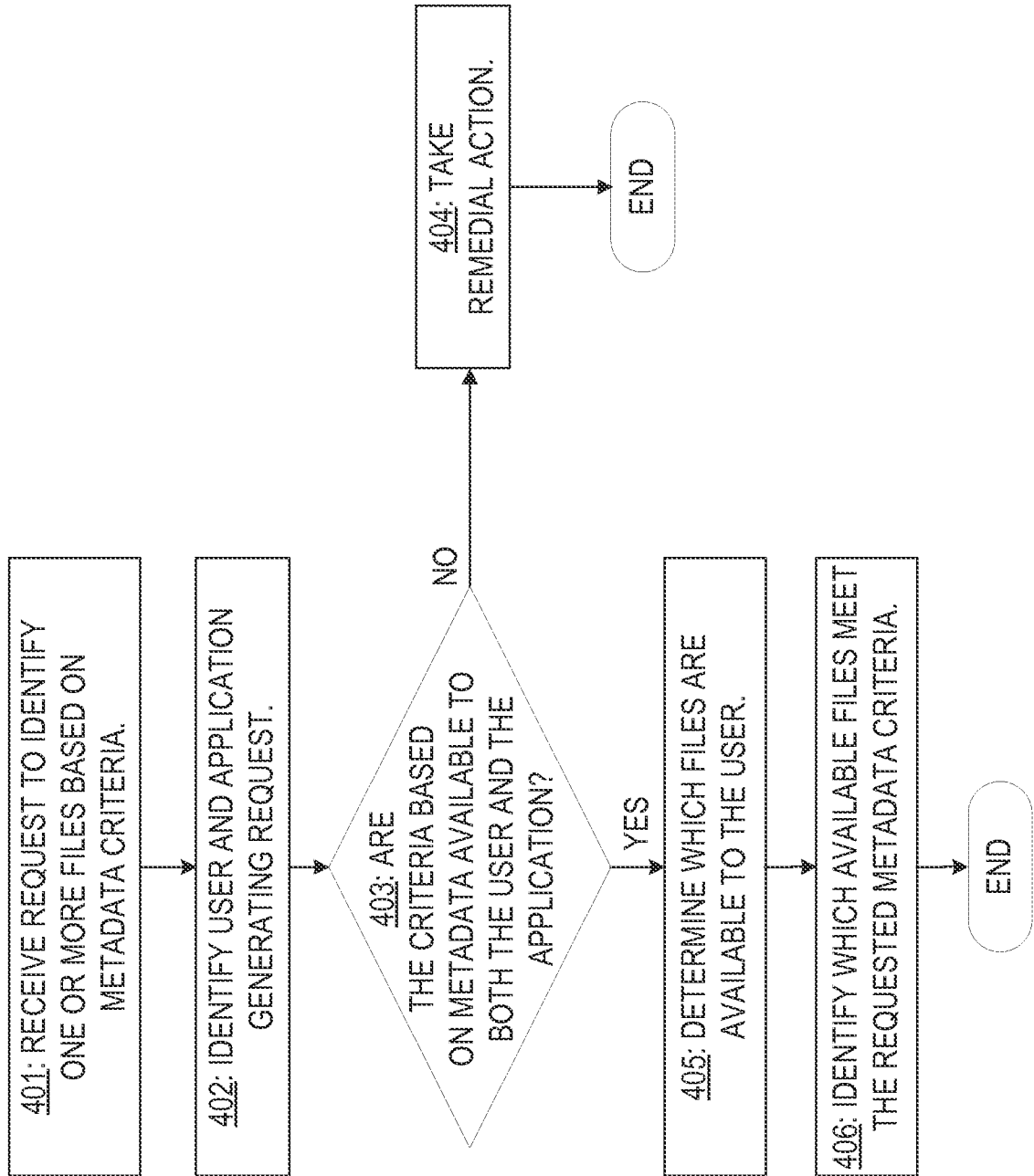


Fig. 4

METADATA ACCESS PROCESS 500

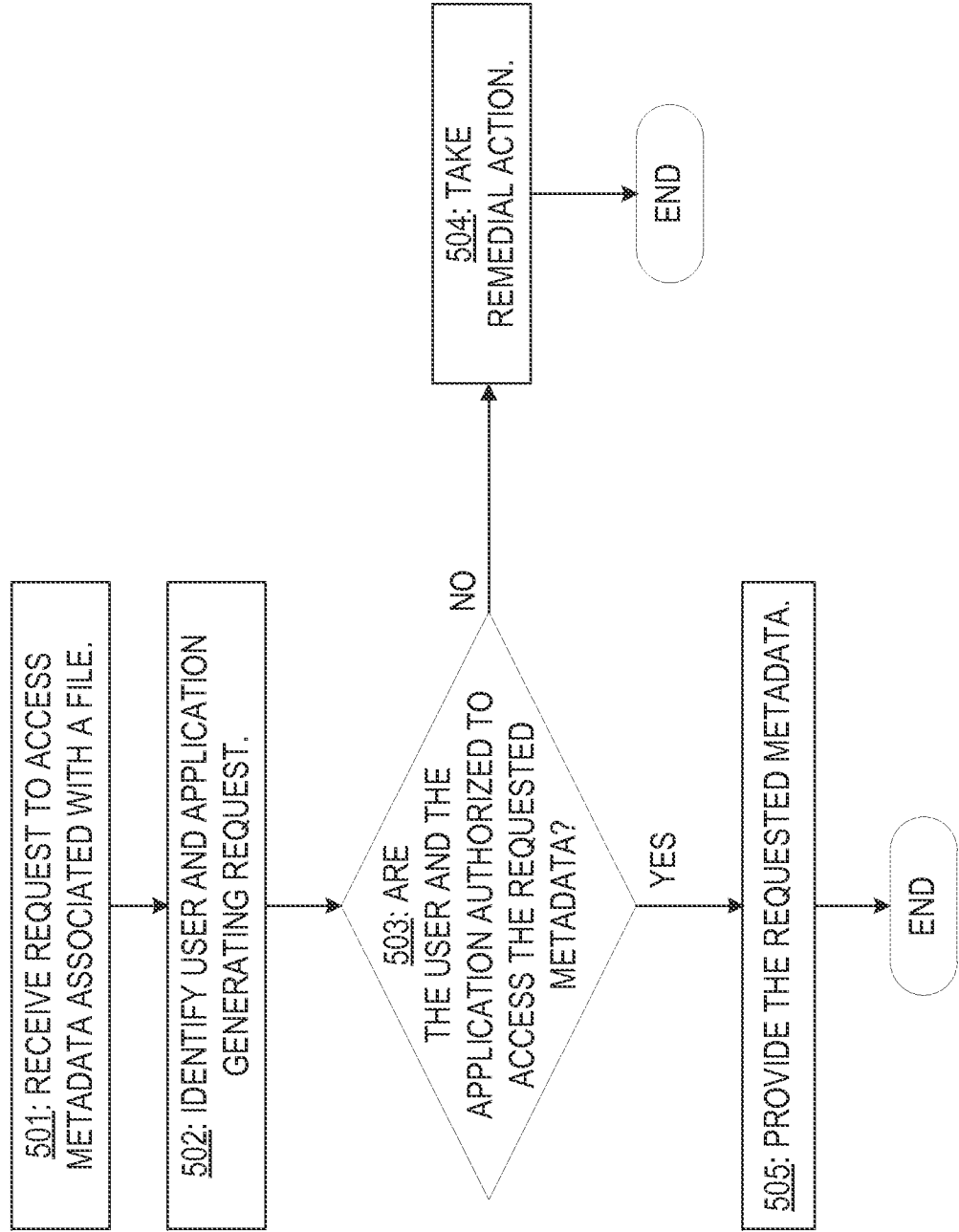


Fig. 5

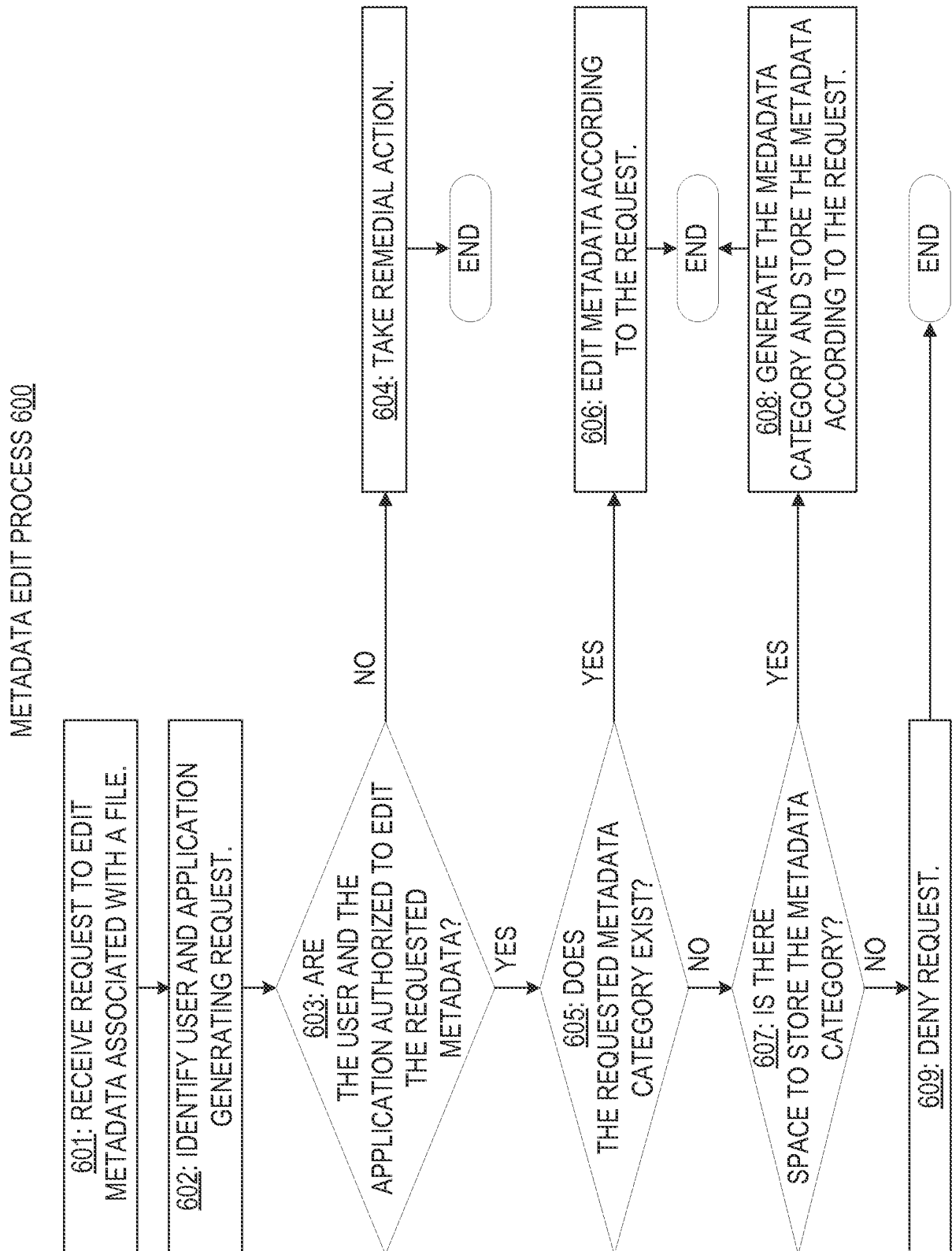


Fig. 6

700

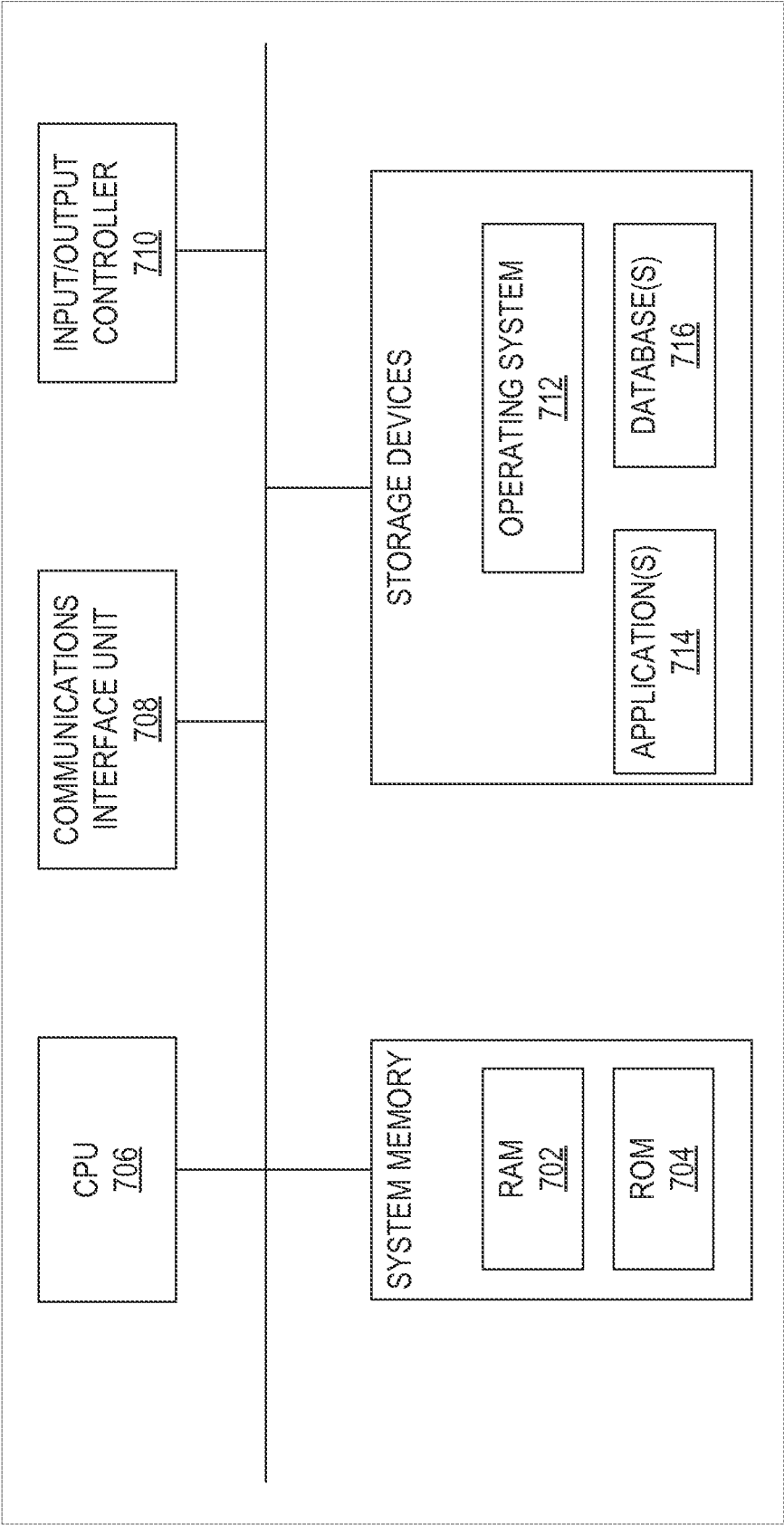


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/032167**A. CLASSIFICATION OF SUBJECT MATTER****G06F 17/00(2006.01)i, G06F 17/30(2006.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 17/00; G06F 15/16; G06F 21/24; G06F 15/173; G06F 9/44; G06F 9/06; G06F 17/30

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: metadata, cloud storage system, application, category, 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.
Y	US 2010-0325199 A1 (PARK, SEONG-YEOL et al.) 23 December 2010 See paragraphs [0042], [0058]-[0059], [0064]-[0065], and [0069]-[0071]; claims 9-10; and figures 2-5.	1,5-10,12-13,18 ,24-25,27-30,33
A		2-4,11,14-17,19-23 ,26,31-32
Y	US 2011-0209045 A1 (GHOSH, DIPANJAN et al.) 25 August 2011 See paragraphs [0006], [0067], and [0074]; and figure 5.	1,5-10,12-13,18 ,24-25,27-30,33
A	KR 10-2013-0007459 A (SAMSUNG ELECTRONICS CO., LTD.) 18 January 2013 See paragraphs [0041]-[0048]; claims 1-2; and figures 1-3.	1-33
A	US 2011-0247074 A1 (MANRING, BRADLEY A.C. et al.) 06 October 2011 See paragraphs [0062]-[0065] and figures 2-3.	1-33
A	KR 10-2012-0065072 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 20 June 2012 See paragraphs [0045]-[0048] and figure 2.	1-33



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

29 July 2014 (29.07.2014)

Date of mailing of the international search report

30 July 2014 (30.07.2014)

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

YU, JAE CHON

Telephone No. +82-42-481-8647



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/032167

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0325199 A1	23/12/2010	CN 101930449 A EP 2284725 A1 JP 2011-003187A KR 10-2010-0137323 A US 8762480 B2	29/12/2010 16/02/2011 06/01/2011 30/12/2010 24/06/2014
US 2011-0209045 A1	25/08/2011	CA 2788119 A1 CA 2788282 A1 CN 102763126 A CN 102763127 A CN 102770877 A EP 2539858 A2 EP 2539859 A2 EP 2539860 A2 US 2011-0208786 A1 US 2011-0209049 A1 WO 2011-106150 A2 WO 2011-106150 A3 WO 2011-106279 A2 WO 2011-106279 A3 WO 2011-106280 A2 WO 2011-106280 A3	01/09/2011 01/09/2011 31/10/2012 31/10/2012 07/11/2012 02/01/2013 02/01/2013 02/01/2013 25/08/2011 25/08/2011 01/09/2011 10/11/2011 01/09/2011 10/11/2011 01/09/2011 10/11/2011
KR 10-2013-0007459 A	18/01/2013	US 2012-0331521 A1	27/12/2012
US 2011-0247074 A1	06/10/2011	None	
KR 10-2012-0065072 A	20/06/2012	US 2012-0150930 A1	14/06/2012