



- (51) International Patent Classification:
G06F 21/78 (2013.01)
- (21) International Application Number:
PCT/US2014/057070
- (22) International Filing Date:
23 September 2014 (23.09.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
2175/CHE/2014 29 April 2014 (29.04.2014) IN
- (71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive W., Houston, Texas 77070 (US).
- (72) Inventors: **DEY, Biraj**; Sy.No.192, Whitefield Road, Mahadevapura Post, Karnataka, Bangalore 560048 (IN).
JOSHI, Mehul Manharlal; Sy.No.192, Whitefield Road, Mahadevapura Post, Karnataka, Bangalore 560048 (IN).
- (74) Agents: **ORTEGA, Arthur** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 East Harmony Road Mail Stop 35, Fort Collins, Colorado 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,

[Continued on next page]

(54) Title: SECURING DATA IN A FILE SYSTEM

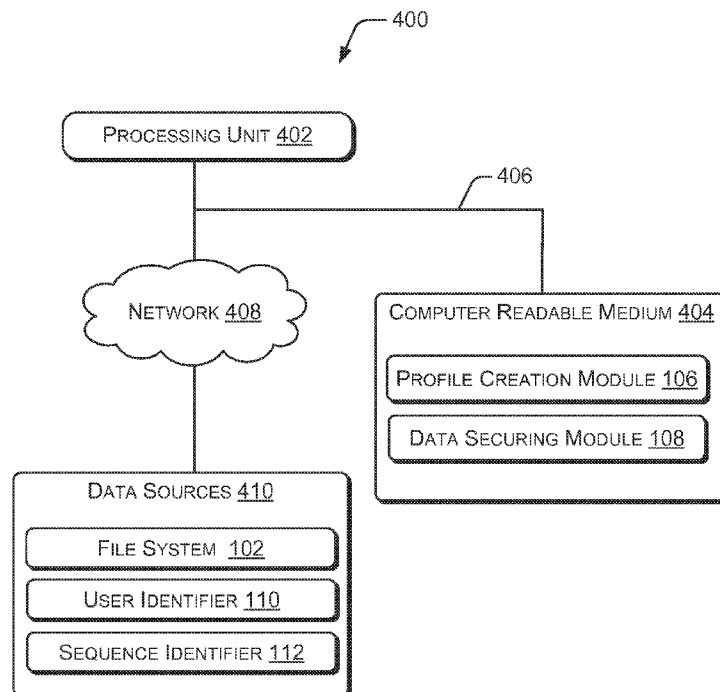


Figure 4

[Continued on next page]



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).

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

Published:

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

Declarations under Rule 4.17:

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

(57) Abstract: The present subject matter relates to securing data in a file system. In one example, the present subject matter includes assigning a user identifier (ID) to a user for creating and storing files having data in the file system. The present subject matter further includes creating a sequence ID for the user, where the sequence ID is created based on whether the user ID is used before, and where each of the files, created and stored by the user, is associated with the user ID and the sequence ID of the user.

BACKGROUND

[0001] In recent years, organizations have become dependent on network-based systems for data storage and data communication. The users may store data, in the form of data files, in a file system which is implemented in a network-based system, such as a server. With the growing number of users accessing the server, the chance of unauthorized access of data has also increased. Exposure of data to an unauthorized user may breach the security of the data. In order to control access to the data in the file system, the organization assigns a unique user identifier (ID) to each user, such that each user can store and access his data using a respective user ID.

BRIEF DESCRIPTION OF DRAWINGS

[0002] The detailed description is described with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to refer like features and components:

[0003] Figure 1(a) illustrates a data securing system, according to an example of the present subject matter.

[0004] Figure 1(b) illustrates a network environment implementing the data securing system, according to an example of the present subject matter.

[0005] Figure 2 illustrates a method for securing data in a file system, according to an example of the present subject matter.

[0006] Figure 3 illustrates a method for securing the data in a file system, according to an example of the present subject matter.

[0007] Figure 4 illustrates a network environment for securing data in a file system, according to an example of the present subject matter.

DETAILED DESCRIPTION

[0008] The present subject matter relates to systems and methods for securing data in a file system. The data may be stored in the form of files, also referred to as data files. The file system is a system that defines the way the files are stored, organized, and accessed. In a network-based implementation,

the file system may be implemented in a device, such as a server, where the data is stored.

[0009] Organizations generally create a profile for each of their users in which a unique user identifier (ID) is assigned to each user. Each user can
5 create files to store data in the file system. The files may be stored through folders or directories in the file system. The files that belong to a particular user are associated with the user ID of the user. The access to files from the file system is granted to a user based on the user ID of the user. As a result, an unauthorized user cannot access files belonging to the particular user.

10 [0010] At the end of a user's employment term, i.e., when a user leaves the organization, his user ID may be deleted from the server; however, the files that belong to that user may be retained. The user ID of a user may be deleted permanently or temporarily from the server. On network-based systems functioning through operating systems (OS), such as Unix®, the deleted user
15 IDs can be recycled. That means, when a user leaves the organization, the user ID of the user may be deleted from the server, and the same user ID may be reassigned to a new user. If the deleted user ID of a previous user is assigned to a new user and if the files belonging to the previous user of that user ID are retained in the file system in the server, then the new user may access the files
20 of the previous user. With this, the data in the files of the previous users is put at risk of being accessible to unauthorized users. The access of the files by the unauthorized users can place sensitive data, such as users' personal information, at a risk of disclosure.

[0011] To avoid this, the ownership of the files may be changed before
25 creating a user ID for a new user. However, with this, the organization may lose track of which files belong to which previous user. Further, in certain scenarios, the user IDs of the users who have left the organization may be disabled instead of being deleted from the server. In such scenarios, the user IDs which are disabled may not be available for reassignment to new users. With this, the
30 organizations may be left with lesser number of user IDs for assignment to the new users.

[0012] Systems and methods for securing data in a file system are described herein. With the systems and the methods of the present subject matter, a new user with a user ID same as a deleted user ID of a previous user cannot gain access to files belonging to the previous user. Therefore, the files
5 associated with the deleted user ID of the previous user are protected or secured from an unauthorized access by a new user.

[0013] In an example implementation, a user ID is assigned to the user for creating and storing files having data in a file system. The user ID can be a new user ID, or can be a deleted user ID which is used before for a previous
10 user who has left the organization. Along with the user ID, a sequence ID is also created for the user. The sequence ID for the user is created based on whether the user ID, which is assigned to the user, is used before. In an example, the sequence ID may be any unique identifier, such as a numeral, based on the number of times the user ID is used before. The combination of the user ID and
15 the sequence ID is unique for each user. The user ID and the sequence ID for the user may be stored in a system database for future reference.

[0014] Further, each of the files within the file system may be further associated with the user ID and the sequence ID of the user who created and stored the respective file in the file system. Based on the user ID and the
20 sequence ID, access of a file within the file system to a user may be controlled.

[0015] With the systems and the methods of the present subject matter, access to data, or files in the file system, belonging to a previous user is not granted to a new user, even if a previously used user ID is assigned to the new user. Thus, the data or the files of the previous user are not put at risk of being
25 accessible to other users. Further, since the ownership of the files may not be changed for securing the data in the file system, the organization can keep track of which files belong to which user. Furthermore, as would be evident, using the sequence IDs along with the user IDs for the user, user IDs, both previously used and new, are available for assignment to the new users.

30 [0016] The above systems and the methods are further described with reference to Figures 1(a) to 4. It should be noted that the description and figures merely illustrate the principles of the present subject matter. It may be

understood that various arrangements may be devised that, although not explicitly described or shown herein, embody the principles of the present subject matter. Further, while aspects of described systems and methods for securing data in a file system can be implemented in any number of different
5 computing systems, environments, and/or implementations, the examples and implementations are described in the context of the following system(s).

[0017] Figure 1(a) illustrates a data securing system 100, according to an example of the present subject matter. In an example, the data securing system 100 may be deployed in an organization having a network-based system for
10 data storage and communication. The data securing system 100 may be a computing device, such as a laptop computer, a desktop computer, a workstation or a server, of the organization. The data securing system 100 enables securing data in a file system 102. The file system 102 is a system that allows the users to create and store files through folders and directories, and
15 defines the way the files are stored, organized, and accessed. The files created by the users may be data files, such as text documents, spreadsheets, images, and videos. In an example, the users may be employees of the organization.

[0018] The data securing system 100 includes processor(s) 104. The processor(s) 104 may be implemented as microprocessors, microcomputers,
20 microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. The functions of various elements shown in Figure 1(a), including a functional block labeled as "processor(s)", may be provided through the use of dedicated hardware as well as hardware capable of executing
25 machine readable instructions.

[0019] The data securing system 100 further includes a profile creation module 106 and a data securing module 108, coupled to the processor 104. The profile creation module 106 and the data securing module 108, amongst other things, may include routines, programs, objects, components, and data
30 structures, which perform particular tasks or implement particular abstract data types. The profile creation module 106 and the data securing module 108 may also be implemented as, signal processor(s), state machine(s), logic circuitries,

and/or any other device or component that manipulates signals based on operational instructions. Further, the profile creation module 106 and the data securing module 108 can be implemented by hardware, by computer-readable instructions executed by a processing unit, or by a combination thereof. The data securing system 100 also includes data comprising user identifier 110 and sequence identifier 112.

[0020] According to an example implementation, the profile creation module 106 creates a profile for each user of the organization, through which each user can create, store, and access files in the file system 102 in a secure manner. In one example, the profile may be created at the time when the user joins the organization. In creating the profile of a user, the profile creation module 106 assigns a user ID to the user, and creates a sequence ID for the user, such that the combination of the user ID and the sequence ID for the user is unique. The user ID can be a new user ID which is not used before for any user, or can be a deleted user ID which is used before for a previous user. In an example, the previous user is a user who has left the organization. The sequence ID for the user is created based on whether the user ID, which is assigned to the user, is a deleted user ID or a new user ID. In an example, the sequence ID may be a numeral, which is set based the number of times the user ID assigned to the user is used before. The user ID for each user may be stored in the user identifier 110, and the sequence ID for each user may be stored in the sequence identifier 112. The assignment of a user ID and the creation of a sequence ID for a user are described in detail later with reference to Figure 1(b).

[0021] Further, for the purpose of securing the data in the file system 102, the data securing module 108 associates each of the files, created and stored by each user, with the user ID and the sequence ID of the respective user. A user may then be granted access of a file from the file system 102 based on comparison of the user ID and the sequence ID associated with the file with the user ID and sequence ID of the user accessing the file. The association of the user IDs and the sequence IDs with files, and the granting of access of files

from the file system 102 to the users are described in detail later with reference to Figure 1(b).

[0022] Figure 1(b) illustrates a network environment 150 implementing the data securing system 100, according to an example of the present subject matter. As shown, apart from the data securing system 100, the network environment 150 includes a plurality of user devices 114-1, 114-2, ..., 114-N, individually referred to a user device 114 and collectively referred to as user devices 114. The user devices 114 are connected to the data securing system 100 through a communication network 116. The user devices 114 may be used by the users to create, store, and access files in the file system 102, over the communication network 116. The user devices 114 may include computing devices, such as a laptop computer, a desktop computer, a notebook, a workstation, a mainframe computer, a mobile phone, and a personal digital assistant.

[0023] The communication network 116 may be a wireless network, a wired network, or a combination thereof. The communication network 116 can also be an individual network or a collection of many such individual networks, interconnected with each other and functioning as a single large network, e.g., the Internet or an intranet. The communication network 116 can be implemented as one of the different types of networks, such as intranet, local area network (LAN), wide area network (WAN), and the internet. The communication network 116 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), and Transmission Control Protocol/Internet Protocol (TCP/IP), to communicate with each other. In an example implementation, the communication network 116 may include a Global System for Mobile Communication (GSM) network, a Universal Mobile Telecommunications System (UMTS) network, or any other communication network that use any of the commonly used protocols, for example, Hypertext Transfer Protocol (HTTP) and Transmission Control Protocol/Internet Protocol (TCP/IP).

[0024] Apart from the processor(s) 104, the data securing system 100 includes interface(s) 118. The interface(s) 118 may include a variety of commercially available interfaces, for example, interfaces for peripheral device(s), such as data input output devices, referred to as I/O devices, storage devices, network device. The I/O device(s) may include Universal Serial Bus (USB) ports, Ethernet ports, host bus adaptors, and their corresponding device drivers. The interface(s) 118 may facilitate the communication of the data securing system 100 with various communication and computing devices and various communication networks, such as networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP) and Transmission Control Protocol/Internet Protocol (TCP/IP).

[0025] The data securing system 100 further includes a memory 120 coupled to the processor(s) 104. Among other capabilities, the processor(s) 104 may fetch and execute computer-readable instructions stored in the memory 120. The memory 120 may include any computer-readable medium known in the art including, for example, volatile memory, such as static random access memory (SRAM) and dynamic random access memory (DRAM), and/or non-volatile memory, such as read only memory (ROM), erasable programmable ROM, and flash memories.

[0026] Further, the data securing system 100 includes module(s) 122 and data 124. The module(s) 122 include the profile creation module 106, the data securing module 108, an access granting module 126, and other module(s) 128. The other module(s) 128 may include programs or coded instructions that supplement applications or functions performed by the data securing system 100.

[0027] The data 124 includes the file system 102, the user identifier 110, the sequence identifier 112, file metadata 130, and other data 132. The other data 132 may include data generated and saved by the modules 122 for providing various functionalities of the data securing system 100. Although the file system 102 is shown internal to the data securing system 100, the file system 102 can also be implemented external to the data securing system 100.

[0028] The description hereinafter describes the procedures of assigning a user ID to a new user, creating a sequence ID for the new user, associating the files created and stored by the new user with the user ID and the sequence ID of the new user, and granting access to a file from the file system 102 to a new user, in accordance with an example implementation of the present subject matter. The description herein is provided with respect to one user; the procedure can be repeated for all the users of the organization, such that the data is secured in the file system 102.

[0029] The profile creation module 106 assigns a user name to a new user, hereinafter referred to as the user. The user may login using the user name through his user device 114 for creating and storing files in the file system 102. The user name may be based on the name of the user. For example, if the name of the user is John Smith, where John is the first name of the user and Smith is the last name of the user, then the profile creation module 106 may assign a user name "John.Smith" to the user.

[0030] The profile creation module 106 also assigns a user ID to the user. The user ID may be a numerical value. In one example, the user ID may be an employee ID of the user. The user ID assigned to the user can be a deleted user ID, which is used before for a previous user who has left the organization. For instance, this may be possible when the previous user has an employee ID, same as that of the new user joining the organization. In an example implementation, the user ID assigned to the user may be stored in the user identifier 110 from where the user ID of the user can be located for reference.

[0031] According to an example implementation, the profile creation module 106 may receive an instruction to create a user name and a user ID for a user. The instruction may be received from a system administrator, when the user joins an organization. In an example, for the creation of the user name, the profile creation module 106 may receive the name of the user from the system administrator, or retrieve the name from a database where details of the user are stored. Further, for the creation of the user ID, the profile creation module 106 may receive the employee ID of the user from the system administrator, or retrieve the employee ID from the database.

[0032] After assigning the user name and the user ID to the user, the profile creation module 106 creates a sequence ID for the user. As mentioned earlier, the sequence ID may be a numeral, which can be used for tracking whether the user ID assigned to the user is being reused, i.e., a deleted user ID, or is new, and is based on the number of times of the user ID is used before. For the creation of the sequence ID, the profile creation module 106 may keep a list of the deleted user IDs and the number of times each deleted user ID is used before. It may be understood that if a user ID is not included in the list, then the user ID is a new user ID.

10 [0033] In an example implementation, the profile creation module 106 may set the sequence ID for the user with a predefined initial value when the user ID assigned to the user is a new user ID. The predefined initial value may be '1'. Further, the profile creation module 106 may set the sequence ID with a value incremented from the predefined initial value when the user ID assigned to the user is a deleted user ID. The value of the sequence ID may be based on a number of times the deleted user ID is used before. In an example, if the deleted user ID was used before once, then the profile creation module 106 increments the predefined initial value by 1, and thus sets the sequence ID as '2'. Further, if the deleted user ID was used before twice, then the profile creation module 106 increments the predefined initial value by 2, and thus sets the sequence ID as '3'.

15 [0034] Thus, no two users, from amongst the new users and the previous users, will have the same sequence IDs. The combination of the user ID and the sequence ID is unique for the user. Further, the sequence ID created for the user may be stored in the sequence identifier 112, from where the sequence ID of the user can be located for reference. In an example, the sequence ID of the user stored in the sequence identifier 112 cannot be altered by unauthorized users.

25 [0035] Once the user ID is assigned to the user and the sequence ID is created for the user, the user can create and store files in the file system 102. The files created by the user may be data files, such as text documents, spreadsheets, images, and videos.

[0036] Further, the data securing module 108 associates each of the files, created and stored by the user, with the user ID and the sequence ID of the user. For this, the data securing module 108 may retrieve the user ID from the user identifier 110 and the sequence ID from the sequence identifier 112. The user ID and the sequence ID of the user may be associated with a file when the file is created by the user. The user can access a file, belonging to him, stored in the file system 102, where the access to the files by the user may be granted based on the user ID and the sequence ID of the user and the user ID and the sequence ID associated with the file. The procedure of accessing a file is described later in the description.

[0037] In an example, for the data securing system 100 operating on a Unix[®] based operating system, each file which is created by the user has an inode associated with it. An inode for a file includes metadata for the file, which may include the information to access a file in a file system. In an example implementation, the user ID and sequence ID associated with the file is included as the metadata in the inode of the file. In an example, in addition to the user ID and the sequence ID, other information, such as file creation, access and modification time, file size, file type, permissions (read, write, execute permissions) and the like, may also be included in the metadata in the inode. The data securing module 108 may store the metadata, or the inodes, of the files in the file metadata 130.

[0038] Further, for accessing a file from the file system 102, the user may login using his user name through his user device 114. As the user attempts to access a file from the file system 102, the access granting module 126 may receive a request from the user. In an example, the request may be received as an indication when the user interacts using an input device to attempt an access of the file. The interaction to attempt an access of the file may include, clicking on a file using a mouse to open the file, scrolling on the file using a mouse to read the file, or typing using a keyboard to write text in the file.

[0039] Based on the request from the user, the access granting module 126 retrieves the metadata of the file from the file metadata 130. As mentioned above, the metadata of the file may include the user ID and the sequence ID

associated with the file. In an example, the metadata may be retrieved from the inode of the file. In addition to the metadata of the file, the access granting module 126 retrieves the user ID and the sequence ID of the user who has attempted to access the file. For this, the access granting module 126 may
5 identify the user through his login details, and may then retrieve the user ID and the sequence ID of the identified user from the user identifier 110 and the sequence identifier 112, respectively.

[0040] Thereafter, for the purpose of granting the access to the file, the access granting module 126 determines whether the user ID associated with the
10 file, to be accessed by the user, and the user ID of the user, who has performed the operation, are same. In case the user ID associated with the file matches with the user ID of the user, the access granting module 126 compares the sequence ID associated with the file, to be accessed by the user, with the sequence ID of the user. If the sequence ID associated with the file matches
15 with the sequence ID of the user, the access granting module 126 grants the access of the file from the file system 102 to the user. Therefore, if both the user ID and the sequence ID associated with the file match with those of the user, then the access granting module 126 grants the access to the file to the user.

[0041] Figure 2 illustrates a method 200 for securing data in a file system,
20 according to an example of the present subject matter. The order in which method 200 is described is not intended to be construed as a limitation, and some of the described method blocks can be combined in a different order to implement the method 200, or an alternative method. Furthermore, the method 200 may be implemented in any suitable hardware, computer-readable
25 instructions, or combination thereof.

[0042] The steps of the method 200 may be performed by either a computing device under the instruction of machine executable instructions stored on a non-transitory computer readable medium or by dedicated hardware circuits, microcontrollers, or logic circuits. Herein, some examples are also
30 intended to cover computer readable medium, for example, digital data storage media, which are machine or computer readable and encode machine-

executable or computer-executable instructions, where said instructions perform some or all of the steps of the described method 200.

[0043] With reference to method 200 as depicted in Figure 2, at block 202, the method 200 includes assigning a user ID to a user for creating and storing files having data in a file system. In an example, the user may be an employee of an organization. The user ID of the user may be a numerical value. For instance, the user ID of the user may be based on the employee ID of the user. Further, the user ID may be a deleted user ID or a new user ID. In an example, the profile creation module 106 of the data securing system 100 assigns the user ID to the user.

[0044] At block 204, the method 200 includes creating a sequence ID for the user, where the sequence ID is created based on whether the user ID is used before, and where each of the files, created and stored by the user, is associated with the user ID and the sequence ID of the user. The sequence ID may be any unique identifier, such as a numeral, which can be used for tracking whether the user ID which is assigned to the user is being reused or is new, and is based on the number of times the user ID is used before. In an example, the sequence ID is set with a predefined initial value when the user ID assigned to the user is the new user ID, and the sequence ID is set with a value incremented from the predefined initial value when the user ID assigned to the user is the deleted user ID. The value may be based on a number of times the deleted user ID is used before. In an example, the profile creation module 106 creates the sequence ID for the user.

[0045] Figure 3 illustrates a method 300 for securing the data in a file system, according to an example of the present subject matter. The order in which method 300 is described is not intended to be construed as a limitation, and some of the described method blocks can be combined in a different order to implement the method 300, or an alternative method. Furthermore, the method 300 may be implemented in any suitable hardware, computer-readable instructions, or combination thereof.

[0046] The steps of the method 300 may be performed by either a computing device under the instruction of machine executable instructions

stored on a non-transitory computer readable medium or by dedicated hardware circuits, microcontrollers, or logic circuits. Herein, some examples are also intended to cover computer readable medium, for example, digital data storage media, which are machine or computer readable and encode machine-executable or computer-executable instructions, where said instructions perform
5 some or all of the steps of the described method 300.

[0047] With reference to method 300 as depicted in Figure 3, at block 302, the method 300 includes assigning a user ID to a user for creating and storing files having data in a file system. In an example, the user ID may be
10 assigned to the user by the profile creation module 106 of the data securing system 100 in a manner as described earlier in the description. In addition to the user ID, a user name is assigned to the user. The user can login using the user name through his user device 114 for creating, storing, and accessing files from the file system 102.

15 [0048] At block 304, the method 300 includes creating a sequence ID for the user, where the sequence ID is created based on whether the user ID is used before, and where each of the files, created and stored by the user is associated with the user ID and the sequence ID of the user. In an example, the sequence ID may be created for the user by the profile creation module 106 of
20 the data securing system 100 in a manner as described earlier in the description. Further, each of the files, created and stored by the user, is associated with the user ID and the sequence ID of the user.

[0049] At block 306, the method 300 includes receiving a request from the user to access a file stored in the file system. In an example, the request
25 from the user may be received, whenever the user performs any of read, write, and access operation on the file. In an example, the access granting module 126 of the data securing system 100 receives a request from the user to access the file stored in the file system 102.

[0050] At block 308, the method 300 includes retrieving metadata of the
30 file to be accessed by the user, where the metadata comprises the user ID and the sequence ID associated with the file. The metadata may also include other information of the file, such as file creation, access and modification time, file

size, file type, permissions (read, write, execute permissions) and the like. In an example, the access granting module 126 retrieves the metadata of the file to be accessed by the user from the file metadata 130.

5 [0051] Further, at block 310, the method 300 includes determining, based on the metadata, whether the user ID associated with the file, to be accessed by the user, and the user ID of the user are same. In an example, the access granting module 126 determines whether the user ID associated with the file and the user ID of the user are same.

10 [0052] At block 312, the method 300 includes comparing, based on the metadata, the sequence ID associated with the file with the sequence ID of the user, when the user ID associated with the file matches with the user ID of the user. In an example, the access granting module 126 compares the sequence ID associated with the file with the sequence ID of the user.

15 [0053] At block 314, the method 300 includes granting the access of the file from the file system to the user when the sequence ID associated with the file matches with the sequence ID of the user. Therefore, if both the user ID and the sequence ID associated with the file match with the user ID and the sequence ID of the user, then the access to the data in the file is granted to the user. In an example, the access granting module 126 grants the access of the
20 file from the file system 102 to the user when the sequence ID associated with the file matches with the sequence ID of the user.

[0054] Figure 4 illustrates a system environment 400 for securing data in a file system 102, according to an example of the present subject matter. The system environment 400 includes a processing unit 402 communicatively
25 coupled to a non-transitory computer readable medium 404 through a communication link 406. In one implementation, the processing unit 402 can be a computing device, such as the data securing system 100, which utilized the non-transitory computer readable medium 404 for securing data in the file system 102.

30 [0055] The non- transitory computer readable medium 404 may be, for example, an internal memory device or an external memory device. In one implementation, the communication link 406 may be a direct communication

link, such as any memory read/write interface. In another implementation, the communication link 406 may be an indirect communication link, such as a network interface. In such a case, the processing unit 402 may access the non-transitory computer readable medium 404 through a network 408. The network
5 408 may be a single network or a combination of multiple networks and may use a variety of different communication protocols.

[0056] The processing unit 402 and the non-transitory computer readable medium 404 may also be communicating with data sources 410 over the network 408. The data sources 410 have applications that communicate with
10 the processing unit 402, for securing data in the file system 102, in accordance with the present subject matter. The data sources 410 may include, for example, the file system 102, user identifier 110, and sequence identifier 112.

[0057] In one implementation, the non-transitory computer readable medium 404 includes a set of computer readable instructions, such as the
15 profile creation module 106 and the data securing module 108. The set of computer readable instructions, referred to as instructions hereinafter, can be accessed by the processing unit 402 through the communication link 406 and subsequently executed to perform acts for securing data in the file system 102.

[0058] For discussion purposes, the execution of the instructions by the
20 processing unit 402 has been described with reference to various components introduced earlier with reference to description of Figures 1(a) and 1(b).

[0059] On execution by the processing unit 402, the profile creation module 106 assigns a user ID to the user for creating and storing files in the file system 102. The user ID may be assigned in a manner as described earlier in
25 the description. In an example implementation, the profile creation module 106 stores the user ID assigned to the user in the user identifier 110. Further, the profile creation module 106 creates a sequence ID for the user based on whether the user ID is one of a deleted user ID and a new user ID. The sequence ID may be assigned in a manner as described earlier in the
30 description. The profile creation module 106 stores the sequence ID created for the user in the sequence identifier 112. Further, the data securing module 108 associates each of the files, created and stored by the user, with the user ID

and the sequence ID of the user, so that a user can be granted access based on comparison and matching of the user ID and the sequence ID of the user with the user ID and the sequence ID associated with the file to be accessed.

- [0060] Although implementations of securing data in a file system have
5 been described in language specific to structural features and/or methods, it is to be understood that the present subject matter is not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed and explained in the context of a few implementations for securing data in a file system.

I/We claim:

1. A data securing system for securing data in a file system, the data securing system comprising:
 - a processor;
 - 5 a profile creation module coupled to the processor to:
 - assign a user identifier (ID) to a user for creating and storing files having data in the file system; and
 - create a sequence ID for the user based on whether the user ID is one of a deleted user ID and a new user ID;
 - 10 a data securing module coupled to the processor to associate each of the files, created and stored by the user, with the user ID and the sequence ID of the user.
2. The data securing system as claimed in claim 1, wherein the profile creation module is to set the sequence ID with a predefined initial value on determining the user ID assigned to the user to be the new user ID.
3. The data securing system as claimed in claim 1, wherein the profile creation module is to set the sequence ID with a value incremented from a predefined initial value on determining the user ID assigned to the user to be the deleted user ID, and wherein the value is based on a number of times the deleted user ID is used before.
4. The data securing system as claimed in claim 1 further comprising:
 - 25 an access granting module coupled to the processor to:
 - receive a request from the user to access a file stored in the file system;
 - determine whether the user ID associated with the file, to be accessed by the user, and the user ID of the user are same;

when the user ID associated with the file matches with the user ID of the user, compare the sequence ID associated with the file, to be accessed by the user, with the sequence ID of the user; and

- 5 grant the access of the file from the file system to the user when the sequence ID associated with the file matches with the sequence ID of the user.

- 10 5. The data securing system as claimed in claim 4, wherein the access granting module is to retrieve metadata of the file to be accessed by the user, and wherein the metadata comprises the user ID and the sequence ID associated with the file, wherein the determination and the comparison are based on the metadata.

- 15 6. A method for securing data in a file system, the method comprising:
 assigning, by a processor, a user identifier (ID) to a user for creating and storing files having data in the file system; and
 creating, by the processor, a sequence ID for the user, wherein the sequence ID is created based on whether the user ID is used before,
20 and wherein each of the files, created and stored by the user, is associated with the user ID and the sequence ID of the user.

7. The method as claimed in claim 6, wherein the user ID is a deleted user ID.

- 25 8. The method as claimed in claim 6, wherein, when the user ID assigned to the user is not used before, the sequence ID for the user is set with a predefined initial value.

- 30 9. The method as claimed in claim 6, wherein, when the user ID assigned to the user is used before, the sequence ID for the user is set with a value

incremented from a predefined initial value, and wherein the value is based on a number of times the user ID is used before.

10. The method as claimed in claim 6 further comprising:
- 5 receiving a request from the user to access a file stored in the file system;
- determining whether the user ID associated with the file, to be accessed by the user, and the user ID of the user are same;
- when the user ID associated with the file matches with the user ID
- 10 of the user, comparing the sequence ID associated with the file, to be accessed by the user, with the sequence ID of the user; and
- granting the access of the file from the file system to the user when the sequence ID associated with the file matches with the sequence ID of the user.

15

11. The method as claimed in claim 10 further comprising:
- retrieving metadata of the file to be accessed by the user, wherein the metadata comprises the user ID and the sequence ID associated with the file, wherein the determining and the comparing are based on the
- 20 metadata.

12. A non-transitory computer-readable medium having a set of computer readable instructions that, when executed, cause a data securing system to:
- assign a user identifier (ID) to a user for creating and storing files
- 25 having data in a file system;
- create a sequence ID for the user based on whether the user ID is used before; and
- associate each of the files, created and stored by the user, with the user ID and the sequence ID of the user.

30

13. The non-transitory computer-readable medium as claimed in claim 12, wherein the user ID is a deleted user ID.

14. The non-transitory computer-readable medium as claimed in claim 12
5 further comprising computer readable instructions to:

receive a request from the user to access a file stored in the file system;

determine whether the user ID associated with the file, to be accessed by the user, and the user ID of the user are same;

10 when the user ID associated with the file matches with the user ID of the user, compare the sequence ID associated with the file, to be accessed by the user, with the sequence ID of the user; and

grant the access of the file from the file system to the user when the sequence ID associated with the file matches with the sequence ID of the user.
15

15. The non-transitory computer-readable medium as claimed in claim 14 further comprising computer readable instructions to:

20 retrieve metadata of the file to be accessed by the user, wherein the metadata comprises the user ID and the sequence ID associated with the file, and wherein the determination of whether the user ID associated with the file, to be accessed by the user, and the user ID of the user are same and the comparison of the sequence ID associated with the file, to be accessed by the user, with the sequence ID of the user are based on the
25 metadata.

1/6

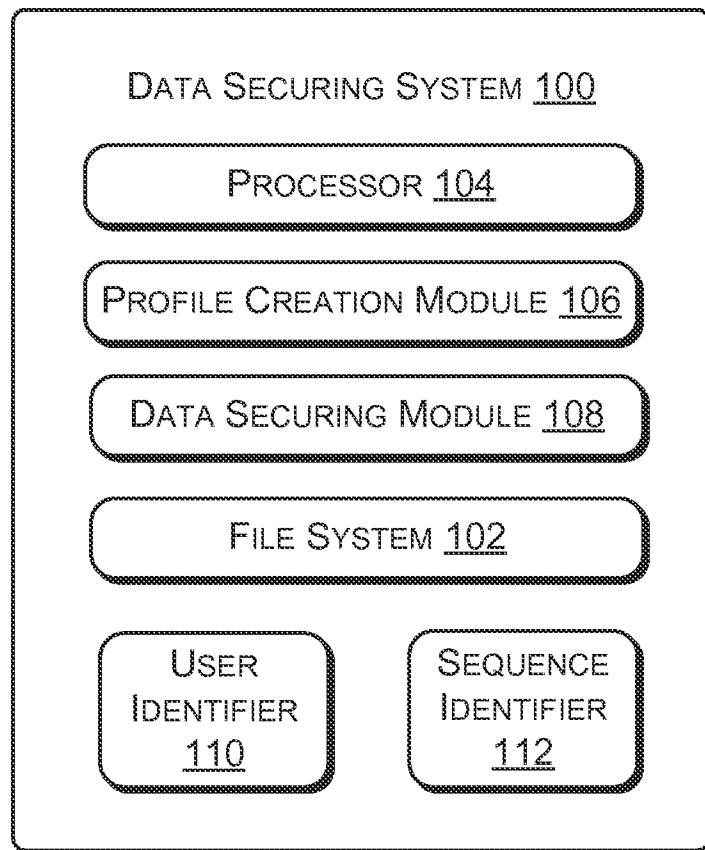
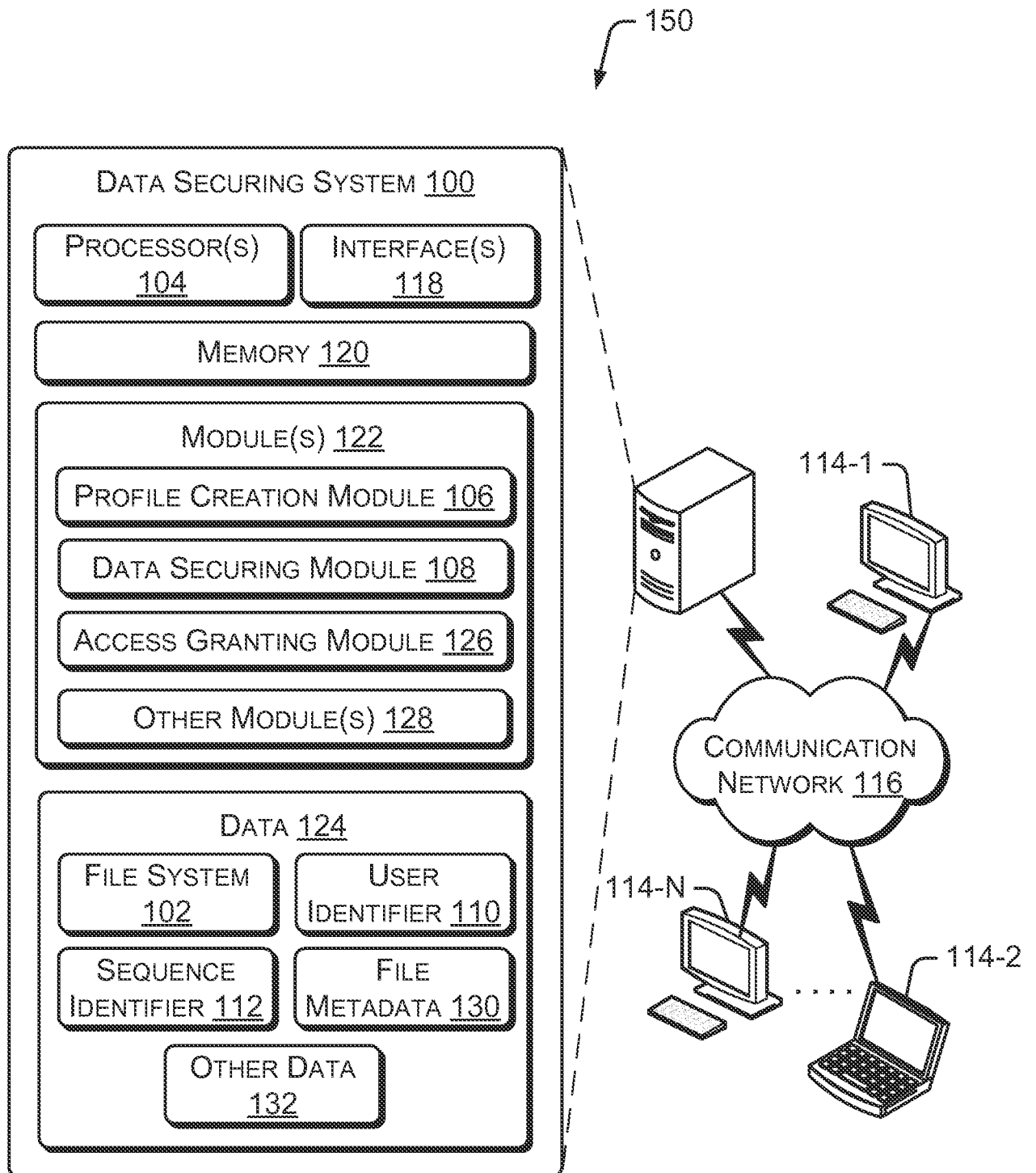


Figure 1(a)

2/6

**Figure 1(b)**

3/6

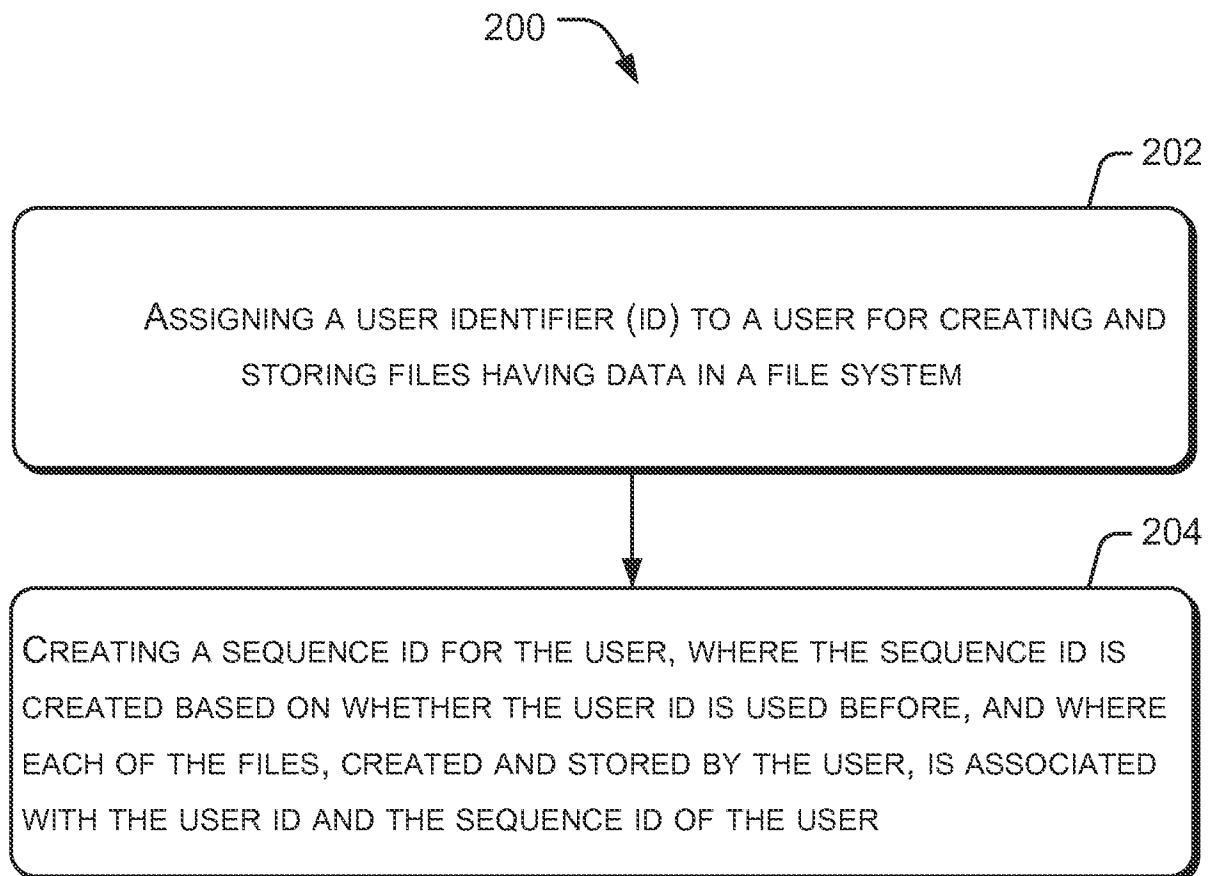
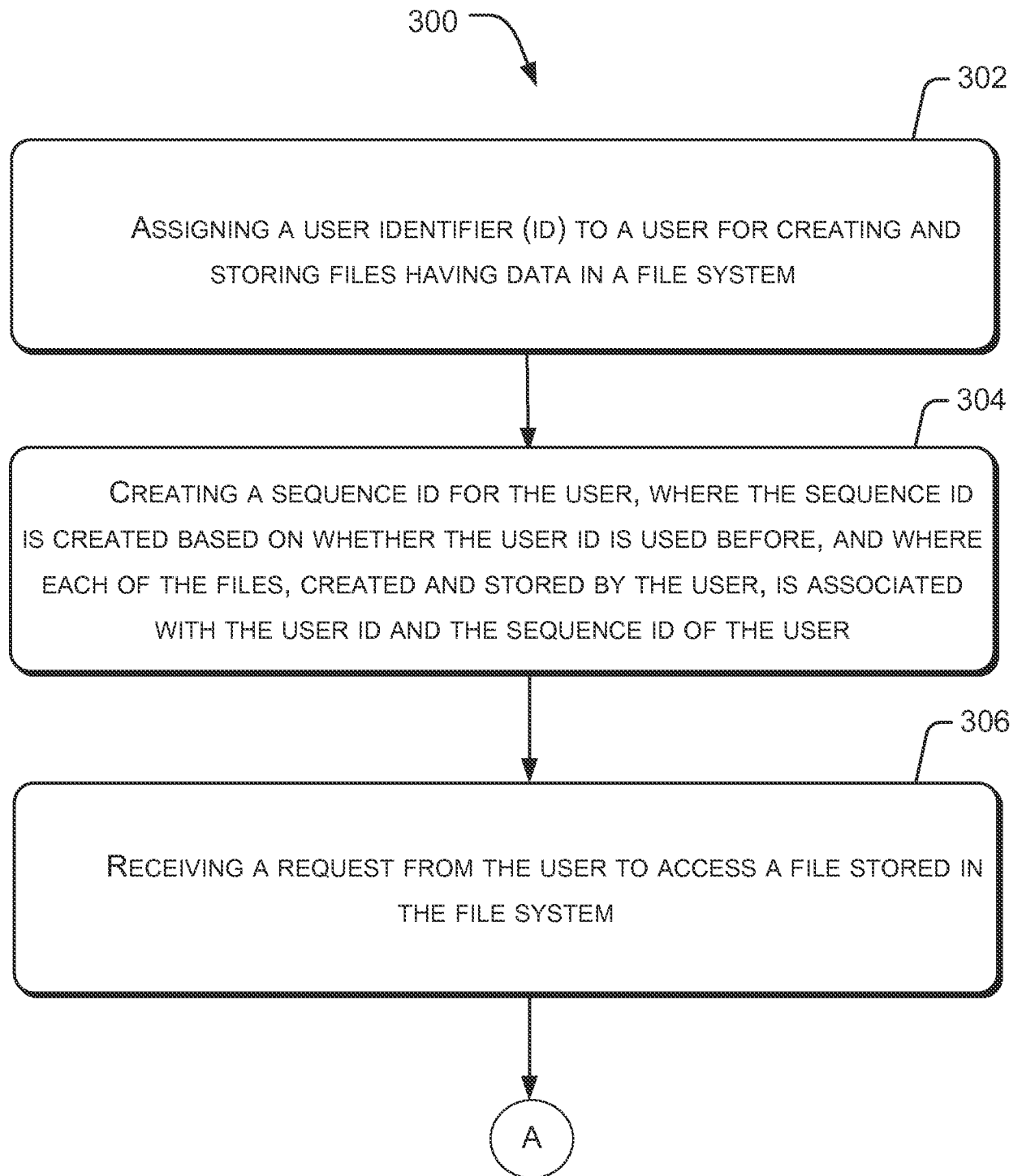
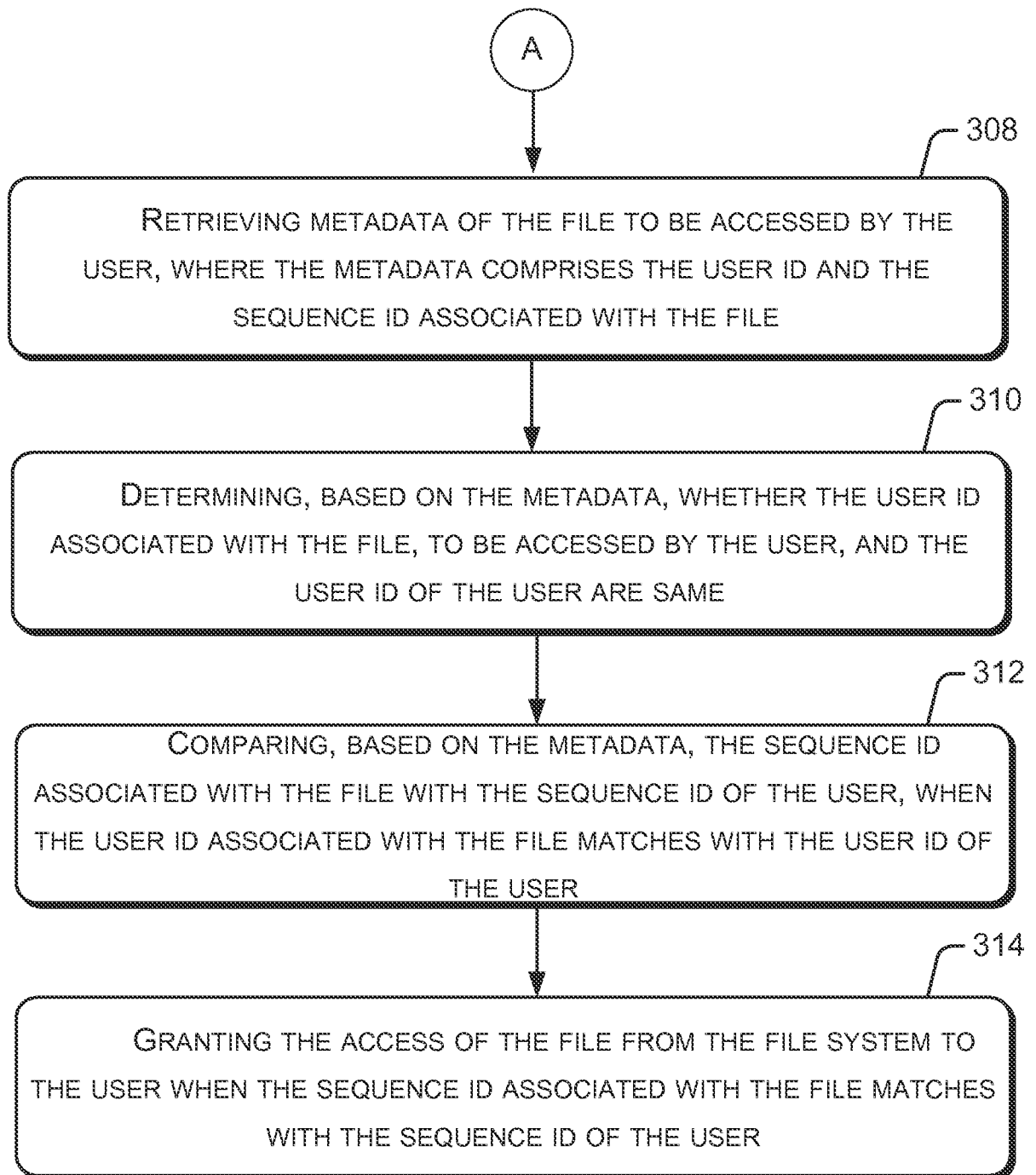


Figure 2

4/6

**Figure 3**

5/6



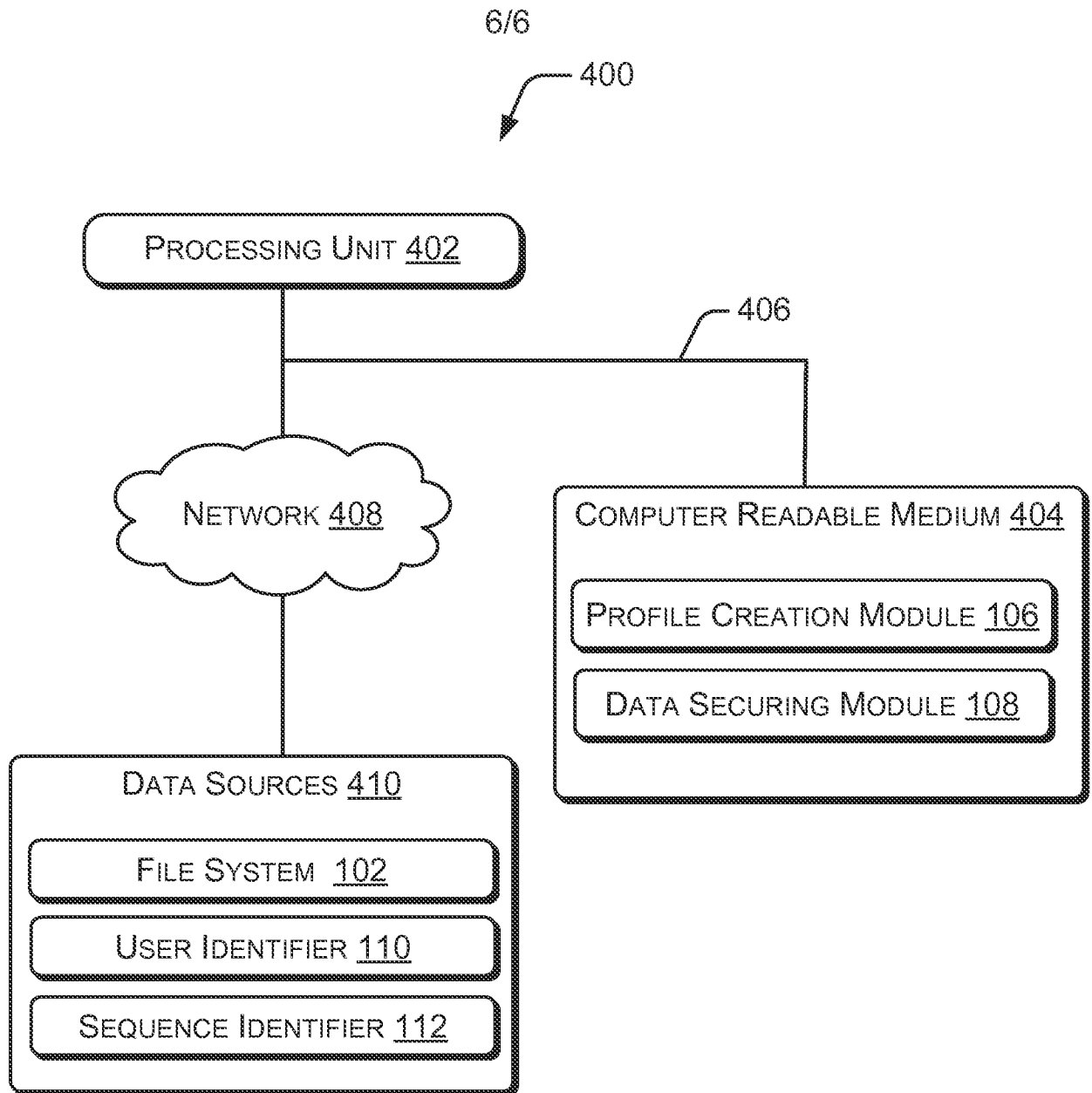


Figure 4

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/78(2013.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/78; G06F 17/22; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: new user, identical ID, sequence ID, protect, private information

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2000-0072017 A (JOO, SUNG-GOO) 05 December 2000	1, 4-6, 10-12, 14-15
Y	See page 1; and claims 1-2.	7, 13
A		2-3, 8-9
Y	KOREA INTERNET & SECURITY AGENCY, 'Website Withdrawal Function Implementation Guide', October 2009 (http://www.kisa.or.kr/public/laws/laws3.jsp)	7, 13
	See page 10.	
A	WO 99-34551 A1 (BARKAN, MORDHAI) 08 July 1999	1-15
	See claim 1; and figure 1.	
A	KR 10-2001-0087510 A (SPEED NET CO., LTD.) 21 September 2001	1-15
	See page 4, lines 22-26.	
A	CIVIL ACTION, 'Private Information Policy Change', 16 July 2004 (http://action.or.kr/?mid=inforight_news&page=25&sort_index=regdate&order_type=asc&document_srl=76847)	1-15
	See page 1.	

☐ 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

17 December 2014 (17.12.2014)

Date of mailing of the international search report

18 December 2014 (18.12.2014)

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

AHN, Jeong Hwan

Telephone No. +82-42-481-8440



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/057070Patent document
cited in search reportPublication
datePatent family
member(s)Publication
date

KR 10-2000-0072017 A

05/12/2000

None

WO 99-34551 A1

08/07/1999

AU 4119399 A
EP 1173950 A119/07/1999
23/01/2002

KR 10-2001-0087510 A

21/09/2001

None