

(51) International Patent Classification:
G06F 17/30 (2006.01)(21) International Application Number:
PCT/US2015/013987(22) International Filing Date:
30 January 2015 (30.01.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).(72) Inventor: **MILLER, Joseph A.**; 705 Taconic Trail, Petersburg, New York 12138 (US).(74) Agents: **FEBBO, Michael A.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (US).(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

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

(54) Title: MULTIPLE USER DATA STORAGE AND SEPARATION

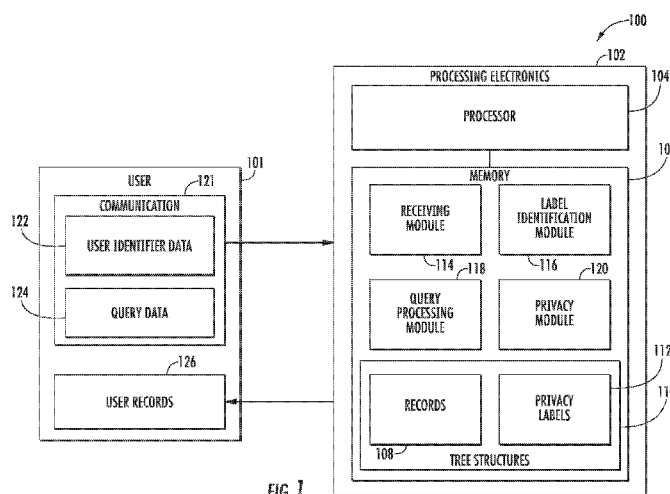


FIG. 1

(57) Abstract: A multiple user data storage and separation apparatus includes memory and records stored in the memory, the records defined by correlated tree structures having schema such that the records are unrestricted by relational table structures. The records include user data items associated with multiple different users. Privacy labels are stored in the memory and correlated with each of the records using privacy label tree structures. The privacy labels distinguish among the users. Instructions are stored in the memory that, when executed, cause a processor to receive a communication including user identifier data and query data, to identify a set of the privacy labels based on the user identifier data; to identify a set of the records based on the query data, and to return, in response to the communication, only records from the identified set of records that are associated with the set of the privacy labels.



MULTIPLE USER DATA STORAGE AND SEPARATION

BACKGROUND

[0001] Providers of cloud computing services may deploy multiple different business applications, such as email applications and case management systems. Each of these business applications may have multiple different clients. In some instances, client personnel may utilize shared business applications. In order to deploy multiple different business applications for multiple different clients, providers of cloud computing services typically deploy multiple servers with each server having multiple database instances. For example, a provider of cloud computing services may deploy 10 different business applications, with each business application having 10 clients for a total of 100 different service instances. The service provider may deploy, for example, 10 different servers, with each server having multiple database instances. Such databases are typically relational databases that enforce relational table structures, such as a column and row structure, to correlate and store data. As such, the service provider may deploy a separate relational database instance for each client on each of the different servers in order to provide appropriate data separation among clients.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Figure 1 is a schematic illustration of an example multiple user data storage and separation apparatus.

[0003] Figure 2 is a diagram illustrating example tree structures for facilitating the multiple user data storage and separation functionality of the apparatus of Figure 1.

[0004] Figure 3A is a Venn diagram illustrating an example relationship between receipts and labels defined by the tree structures of Figure 2.

[0005] Figure 3B is a Venn diagram illustrating an example relationship between receipts and nodes defined by the tree structures of Figure 2.

[0006] Figure 3C is a Venn diagram illustrating an example relationship among nodes, receipts, and labels defined by the tree structures of Figure 2.

[0007] Figure 4 is a diagram illustrating an example implementation of the tree structures of Figure 2.

[0008] Figure 5 is a flow diagram of an example process that may be carried out by the multiple user data storage and separation apparatus of Figure 1.

DETAILED DESCRIPTION OF EXAMPLES

[0009] Examples of apparatus, systems, and methods having multiple user data storage and separation functionality are disclosed herein. Multiple user data storage and separation functionality is of increasing interest to providers of cloud computing services. In particular, the use of virtualization as opposed to server hardware duplication is increasing. Business applications, however, are currently developed from the ground up, often using available off-the-shelf applications, and have a typically large system footprint due in part to the limitations and complexities of relational database technologies used for data storage. These limitations and complexities may lead to, for example, the need for separate database instances for multiple different system users in order to ensure appropriate data separation is maintained. This may in turn lead to high licensing and maintenance costs for deployment of business applications.

[00010] The apparatus, systems, and methods having multiple user data storage and separation functionality disclosed herein may facilitate the implementation of a single computing system or virtualized operating system having a single database instance that stores and separates data for multiple users without resulting in bleeding or unauthorized disclosure of data from one user to another. In particular, the apparatus, systems, and methods having multiple user data storage and

separation functionality disclosed herein may utilize data records defined by correlated tree structures having schema such that the records are unrestricted by relational table structures, such as columns and rows. Privacy labels distinguishing among multiple users may be correlated with each of the records using privacy label tree structures. The use of such tree structures may impose fewer limitations on and provide greater flexibility of the structure of each record while at the same time maintaining appropriate data separation.

[00011] Figure 1 schematically illustrates an example multiple user data storage and separation apparatus 100. As will be described hereafter, apparatus 100 may include multiple user data storage and separation functionality. Apparatus 100 may be, for example, a component of a cloud computing system used to provide multiple different business applications, such as email applications and case management systems, to multiple different users 101. In particular, apparatus 100 may provide a single database instance that stores and separates data for multiple users 101 without resulting in bleeding or unauthorized disclosure of data from one user to another.

[00012] Apparatus 100 may include processing electronics 102. Processing electronics 102 may include, for example, a processor 104 configured to execute logic in the form of instruction modules contained in a memory 106. For purposes of this application, the term “processor” shall mean a presently developed or future developed processor 104 that executes sequences of instructions contained in memory 106. In general, upon executing instructions contained in the memory, processor 104 may provide multiple user data storage and separation functionality in apparatus 100. The instructions may be loaded in a random access memory (RAM) for execution by the processor 102 from a read only memory (ROM), a mass storage device, or some other persistent storage. In some examples, hardwired circuitry modules may be used in processing electronics 102 in place of, or in combination with, processor 104 and/or instruction modules stored in memory 106 to implement the multiple user data storage and separation functionality described herein. For example, the multiple user data storage and separation functionality of apparatus 100 may be implemented

entirely or in part by logic contained in an application-specific integrated circuit (ASIC). Unless otherwise specifically noted, processing electronics 102 is not limited to any specific combination of hardware circuitry modules and instruction modules, nor to any particular source for instructions executed by processor 104.

[00013] Memory 106 may include a non-transitory computer-readable medium. The term “non-transitory computer-readable medium” as used herein includes any computer readable medium, excluding only transitory propagating signals per se. Memory 104 may include, for example any non-volatile or volatile memory such as DRAM, RAM, ROM, register memory, or some combination of these; for example a hard disk combined with RAM. Memory 106 may store software instruction modules for execution by processor 104. In some examples, memory 106 may further store data for use by processor 104. Memory 106 may store various software instruction modules that direct processor 104 to carry out various interrelated actions, such as the multiple user data storage and separation functionality of apparatus 100.

[00014] As shown in Figure 1, memory 106 may include records 108 stored therein. Records 108 may be, for example, individual user data items or groupings of associated user data items. For example, apparatus 100 may be a component of a cloud computing system that provides an email application, and memory 106 may store email records. Such records 108 may be comprised of associated user data items such as “Subject” data from the subject lines of emails, “Message” data including the text of emails, “To” data including the identity of message recipients, and “From” data including the identity of message senders. Memory 106 may store data items for multiple different users 101. The term “user” as used herein may refer to single individuals (e.g., clients or employees) or entities (e.g., companies or corporate entities) or grouping or subgroupings of individuals and/or entities (e.g., an employer entity, an IT department subgroup entity, and subgroups of individual employees).

[00015] Records 108 may be defined by and stored using correlated tree structures 110. For example, records 108 may be defined by node-based binary tree structures used for data storage and searching, such as self-balancing binary tree structures. In particular, tree structures 110 may have schema definitions such that

stored records 108 are unrestricted by the rigid relational table structures required between instances of stored data in relational databases, such as rows and columns. In some examples, the structures of two different records 108 may not be the same. For example, continuing with the email example from above, some records 108 may be structured and stored by associating “Subject”, “Message”, “To”, and “From” user data items, while some records 108 may be structured and stored by associating only “Subject”, “Message”, “To” user data items. In this example, the schema defined by tree structures 110 may not require null or placeholder “From” data for those records 108 that are structured to exclude it, as opposed to a relational table structure, which would require null “From” values in each record 108.

[00016] Memory 106 may also include privacy labels 112. Privacy labels 112 may distinguish among multiple different users 101. Each privacy label 112 may include a unique identification mapping to a user 101. In some examples, privacy label 112 may include a number of tokens (e.g., unique randomly generated cryptographically entropic values having a predetermined number of bytes, etc.) that are uniquely provisioned to user 101. For example, multiple different users 101 may include a manager who shares a subset of records 108 with an employee. The manager may be provisioned a privacy label 112 having a particular set of N tokens. The employee may be provisioned with a privacy label 112 having, for example, a subset of the N tokens.

[00017] Privacy labels 112 may be correlated with records 108 whenever user data items associated as records 108 are written to memory 106. For example, the manager’s privacy label 112 including the full set of N tokens may be correlated with all records 108 written to memory 106 by the manager. A different privacy label 112 containing a subset of the N tokens may be correlated with all records 108 written to memory 106 by the employee.

[00018] Once privacy labels 112 are correlated with records 108, they may be compared with user identifier data provided by users 101 requesting records 108 from memory 106 in order to ensure that only records 108 associated with a particular user 101 are accessed by that user 101. For example, the manager may provide user

identifier data including the full set of N tokens along with query data to apparatus 100. The full set of N tokens in the user identifier data may be compared with privacy labels 112 correlated with records 108 in order to ensure that only records 108 with correlated privacy labels 112 including the full set of N tokens provisioned to the manager, and records 108 with correlated privacy labels 112 including the subset of N tokens provisioned to the employee are returned to the manager. Even if the user identifier data provided by the manager includes the full set of N tokens, the manager may still access records 108 having fewer than N correlated tokens, provided that all tokens for a record 108 are included in the full set of N tokens provided by the manager. Similarly, the employee may provide user identifier data including the subset of N tokens along with query data to apparatus 100. The subset of N tokens in the user identifier data may be compared with privacy labels 112 in order to ensure that only records 108 correlated with the subset of N tokens provisioned to the employee are returned to the employee. The employee may not access records 108 for which there are a greater number of correlated tokens than those provided by the employee. Other provisioning schemes for privacy labels 112 are contemplated as well.

[00019] Privacy labels 112 may be correlated with each of records 108 using privacy label tree structures included in tree structures 110. The privacy label tree structures defining privacy labels 112 may have schema definitions similar to other tree structures 110. That is, privacy labels 112 may be structured and stored without being restricted by the rigid relational table structures required between instances of stored data in relational databases, such as rows and columns.

[00020] By way of example, Figure 2 is a diagram illustrating example tree structures 200 for facilitating the multiple user data storage and separation functionality of apparatus 100. As shown in Figure 2, the tree structures 200 defining records may include segment trees 202 and receipt trees 204. Segment trees 202 may include a number of correlated trees corresponding to segments 206. Segments 206 may correspond to, for example, a particular type or grouping of user data items. For example, as shown in Figure 2, segments 206 may include a segment 206a for

“Subject” data from the subject lines of emails, a segment 206b for “Message” data including the text of emails, a segment 206c for “To” data including the identity of message recipients, and a segment 206d for “From” data including the identity of message senders. Each tree structure corresponding to a segment 206 may include a number of nodes 208. Each node 208 may in turn be an individual node, may be a parent node having a number of child nodes, or may be a child node depending from a parent node. Each node 208 may contain a user data item or a reference to a user data item (e.g., if a user data item is stored in a location other than memory 106). For example, node 208a may include particular “Subject” data for an email, node 208b may include particular “Message” data for an email, node 208c may include particular “To” data for an email, and node 208d may include particular “From” data for an email. Each node 208 may also contain a reference to a number N of receipts 210. That is, each of the nodes 208 in a segment tree 206 has a corresponding receipt tree 204 to define a respective set of records 108 stored in memory 106 in which that respective node 208 is included.

[00021] Receipt trees 204 may include a number of correlated trees corresponding to receipts 206. Each receipt 206 may correspond to and define a respective set of N associated nodes 208, where each of the nodes 208 contains a reference to the respective receipt 210. Accordingly, each node 208 may list a number N of receipts 210, and each receipt 210 may list an unrelated number N of nodes 208. The set of N associated nodes for a particular receipt 210 may define a record 108. For example, each of nodes 208a, 208b, 208c, and 208d may contain a reference to a receipt 210a. Figure 2 illustrates an example reference to a receipt 210a for node 208c. In turn, receipt 210a may contain references to each of nodes 208a, 208b, 208c, and 208d. Figure 2 illustrates an example reference to node 208c for receipt 210a. As such, receipt 210a may define a record that includes each of nodes 208a, 208b, 208c, and 208d. It will be appreciated that the additional receipt references for node 208c shown in Figure 2 may represent the inclusion of node 208c in N-1 other records 108 that may contain additional, fewer, or different nodes 208 than those for record 108a defined by receipt 210a.

[00022] As shown in Figure 2, tree structures 200 may also include privacy label trees 212. Privacy label trees 212 may include a number of correlated trees corresponding to privacy labels 214. Privacy labels 214 are correlated with receipts 210 in receipt trees 204 to define respective sets of records 208 associated with respective different users 101. In particular, each privacy label 214 may correspond to and define a respective set of N associated receipts 210, where each of the receipts 210 contains a reference to the respective privacy label 214. Accordingly, each privacy label 214 may list a number N of receipts 210, and each receipt 210 may list an unrelated number N of privacy labels 214. In some examples, for each privacy label 214, there may or may not be a corresponding receipt 210, but for each receipt 210, there must be at least one privacy label 214. The set of N associated receipts 210 for a particular privacy label 214 may define a set of records 108 for which a particular user 101 may gain access, provided that particular privacy label 214 has been provisioned to that particular user 101.

[00023] As will be appreciated, each node 208 may have a number N of corresponding receipts 210, which may, in turn, have a number N of corresponding privacy labels 214, which may provide a theoretically unbounded storage capability, limited only by the details of the particular practical implementation. As may also be appreciated, segments 206 and their corresponding nodes 208 may be grouped according to any particular attribute and are not limited in structure by the rigid relational table structures required between instances of stored data in relational databases, such as rows and columns. As such, segments 206 and their corresponding nodes 208 may be easily repurposed and/or reused simply by addition, deletion, or modification of corresponding receipts 210.

[00024] Figures 3A, 3B, and 3C are Venn diagrams providing an alternative representation of the relationships among tree structures 200 shown in Figure 2. In Figures 3A, 3B, and 3C, set L is the set of all receipts for all privacy labels, set R is the set of all receipts, and set K is the set of all receipts for a given node in a segment tree. Each privacy label may have many corresponding receipts. Each receipt may have many corresponding nodes. Each node may have a corresponding receipt tree of

receipts. For purposes of Figures 3A, 3B, and 3C, it may be assumed that, for each privacy label, there may or may not be a corresponding receipt, but for each receipt, there must be at least one privacy label. Under this assumption, while all members of set R must correspond to one or more members (i.e., lists of corresponding receipts) of set L, not all members in set L will correspond to elements of set R. $L \cap R$ must always equal R, and therefore $R \subseteq L$ as shown in Figure 3A.

[00025] Referring now to Figures 3B and 3C, set S is the set of all nodes having an associated binary receipt tree, and $S_0, S_1, \dots, S_n$ are all binary trees. Assuming each receipt tree has multiple corresponding nodes, for each $x \in S_n$, K is the set of receipts for each node x. $\forall x \in S_n: \forall y \in K \cap R$ where K is not $\{\}$ and K is the set of receipts for node x as shown in Fig. 3B. Thus, each node is directly correlated with a privacy label upon assignment of a receipt. Each receipt may reference up to S_n nodes. Each privacy label may reference up to N receipts. Accordingly, the total set of all nodes corresponding to a given privacy label is the intersection of nodes in the sets of S, for nodes corresponding to a receipt in K, by which there is a corresponding privacy label set in R, as shown in Figure 3C.

[00026] Figure 4 is a diagram illustrating an example implementation 400 of tree structures 200. Implementation 400 includes correlated binary tree structures corresponding to segments 402, receipts 404, and privacy labels 406. The three possible segments are segment 402a, corresponding to “Name” data, segment 402b, corresponding to “Age”, and a segment 402c, corresponding to “Favorite Day” data. Figure 4 illustrates three specific examples. In the first example, a record that uses only one of three possible segments 402 is illustrated. In particular, segment 402a is used, and a node 408a is assigned to Name data “Bob”. Node 408a has a corresponding receipt 410a. In the second example, a record that uses two of three possible segments 402 is illustrated. In particular, segments 402a and 402b are used, and nodes 408b and 408c are assigned to Name data “Joe” and Age data “21” respectively. Nodes 408b and 408c both correspond to receipt 410b. In the third

example, a record that uses all three possible segments 402 is illustrated. In particular, segments 402a, 402b, and 402c are used. Node 402d is assigned to Name data “Ted”. Node 402e is assigned to Favorite Day data “Tuesday”. Node 408c is reused. Nodes 402c, 402d, and 402e correspond to receipt 410c. The records for Bob and Ted share the same privacy label 412a (e.g., the records for Bob and Ted were created by the same user), while the record for Joe is correlated with privacy label 412b.

[00027] Referring again to Figure 1, memory 106 may include receiving module 114, label identification module 116, query processing module 118, and privacy module 120. Modules 114, 116, 118 and 120 may cooperate to cause processing electronics 102 to carry out the process 500 set forth by the flow diagram of Figure 5. As indicated by a step 502, receiving module 114 may receive a communication 121 including user identifier data 122 and query data 124. For example, each privacy label 112 may include a unique identification mapping to a user 101. In some examples, privacy label 112 may include a number of tokens that are uniquely provisioned to user 101. User 101 may send a communication 121 including user identifier data 122 that includes a set of N tokens along with a query to apparatus 100.

[00028] In some examples, user identifier data 122 is out of band data with respect to query data 124. That is, user identification data 122 may be received by receiving module 114 in the same communication as query data 124, but may be kept separate from query data 124 by a conceptually independent data channel provided as an inherent characteristic of the communication channel and transmission protocol, as opposed to requiring a separate communication channel and endpoints to be established at apparatus 100. In this way, user 101 need not be aware of and is not required to enter user identification data 122, and user identifier 124 may be processed independent of query data 124 by label identification module 116 and privacy module 120. Query data 124 may be, for example, a select statement or other type of query that defines the scope of a data request. For example, query data 124

may include a request to retrieve all emails from person X having Y in the subject line. Other types of query data 124 are contemplated as well.

[00029] At a step 504, label identification module 116 may identify a set of privacy labels 112 based on user identifier data 122. In some examples, label identification module 116 identifies the set of the privacy labels 112 by comparing tokens in the user identifier data 122 with tokens in privacy labels 112 stored in memory 106. In some examples, if tokens in the user identifier data 122 do not match tokens in any privacy labels 112, user 101 is informed that no data exists. In some examples, label identification module 116 communicates with a privacy label mapping service to obtain the actual tokens for the ones the user is providing (e.g., user 101 is not provided with the actual tokens used by apparatus 100, but rather reference tokens).

[00030] At a step 506, query processing module 118 may identify a set of records 108 based on query data 124. In some examples, query processing module 118 may identify the set of records 108 using tree structures such as those described with reference to Figure 2. For example, query processing module 118 may identify segment tree nodes associated with query data 124, and further identify receipts correlated with the segment tree nodes associated with the query data using receipt trees correlated with the segment trees. By way of example, query data 124 may include a request to retrieve all emails from person X having Y in the subject line. Query processing module 118 may search segment trees for segments corresponding to “From” and “Subject” in order to identify nodes matching X and Y. Query processing module 118 may then identify receipts correlated with nodes matching X and Y. The identified set of receipts may correspond to a set of records 108 meeting the requirements of query data 124.

[00031] At a step 508, privacy module 120 may return, in response to communication 121, only records 126 from the set of records 108 identified by query processing module 118 that are associated with the set of the privacy labels 112 identified by label identification module 116. In some examples, privacy module 120 may identify the appropriate records 108 using tree structures such as those described

with reference to Figure 2. For example, privacy module 120 may identify privacy labels 112 correlated with the receipts that correspond to a set of records 108 meeting the requirements of query data 124. Privacy module 120 may then compare the resulting set of privacy labels 112 with the set of the privacy labels 112 identified by label identification module 116. Privacy module 120 may then return only those records 108 for which the set of privacy labels 112 identified by privacy module 120 match those identified by label identification module 116. If there are no matching privacy labels 112, then privacy module 120 may respond to the communication indicating no data exists.

[00032] Although the present disclosure has been described with reference to example embodiments, workers skilled in the art will recognize that changes may be made in form and detail without departing from the spirit and scope of the claimed subject matter. For example, although different example embodiments may have been described as including one or more features providing one or more benefits, it is contemplated that the described features may be interchanged with one another or alternatively be combined with one another in the described example embodiments or in other alternative embodiments. Because the technology of the present disclosure is relatively complex, not all changes in the technology are foreseeable. The present disclosure described with reference to the example embodiments and set forth in the following claims is manifestly intended to be as broad as possible. For example, unless specifically otherwise noted, the claims reciting a single particular element also encompass a plurality of such particular elements.

WHAT IS CLAIMED IS:

- 1 1. A multiple user data storage and separation apparatus, comprising:
2 memory;
3 records stored in the memory, the records defined by correlated tree
4 structures having schema such that the records are unrestricted by relational table
5 structures, the records including user data items associated with multiple different users;
6 privacy labels stored in the memory and correlated with each of the
7 records using privacy label tree structures; wherein the privacy labels distinguish among
8 the users; and
9 instructions stored in the memory, the instructions, when executed,
10 causing a processor to
11 receive a communication including user identifier data and query
12 data;
13 identify a set of the privacy labels based on the user identifier data;
14 identify a set of the records based on the query data; and
15 return, in response to the communication, only records from the
16 identified set of records that are associated with the set of the privacy labels.
- 1 2. The apparatus of claim 1, wherein the tree structures defining the records include
2 segment trees, the segment trees including nodes corresponding to the user data items,
3 and wherein the tree structures defining the records stored in the memory further include
4 receipt trees, the receipt trees including receipts that define respective sets of segment
5 tree nodes included in each of the respective records stored in the memory, and wherein
6 each of the nodes in the segment trees has a corresponding one of the receipt trees to
7 define a respective set of the records stored in the memory in which that respective
8 segment tree node is included.

1 3. The apparatus of claim 2, wherein the instructions, when executed, cause
2 the processor to identify the set of the records based on the query data by identifying
3 segment tree nodes associated with the query data, and by identifying receipts correlated
4 with the segment tree nodes associated with the query data using the receipt trees.

1 4. The apparatus of claim 2, wherein the privacy labels are correlated with
2 the receipt trees to define respective sets of the records associated with each of the
3 respective multiple users.

1 5. The apparatus of claim 1, wherein the user identifier data is out of band
2 data with respect to the query data, wherein the privacy labels and the user identifier data
3 include tokens, and wherein the instructions, when executed, cause the processor to
4 identify the set of the privacy labels by comparing the tokens in the user identifier data
5 with the tokens in the privacy labels stored in the memory.

1 6. A method of multiple user data storage and separation, comprising:
2 receiving, by an apparatus, a communication including user identifier data
3 and query data, the apparatus including records defined by correlated tree structures
4 having schema such that the records are unrestricted by relational table structures, the
5 records including user data items associated with multiple different users, the apparatus
6 also including privacy labels correlated with each of the records using privacy label tree
7 structures, wherein the privacy labels distinguish among the users;
8 identifying a set of the privacy labels based on the user identifier data;
9 identifying a set of the records based on the query data; and
10 returning, in response to the communication, only records from the
11 identified set of records that are associated with the set of the privacy labels.

1 7. The method of claim 6, wherein the tree structures defining the records
2 include segment trees, the segment trees including nodes corresponding to the user data
3 items, and wherein the tree structures defining the records stored in the memory further
4 include receipt trees, the receipt trees including receipts that define respective sets of

5 segment tree nodes included in each of the respective records stored in the memory, and
6 wherein each of the nodes in the segment trees has a corresponding one of the receipt
7 trees to define a respective set of the records stored in the memory in which that
8 respective segment tree node is included.

1 8. The method of claim 7, further comprising identifying segment tree nodes
2 associated with the query data, and identifying receipts correlated with the segment tree
3 nodes associated with the query data using the receipt trees in order to identify the set of
4 the records based on the query data.

1 9. The method of claim 7, wherein the privacy labels are correlated with the
2 receipt trees to define respective sets of the records associated with each of the respective
3 multiple users.

1 10. The method of claim 6, wherein the user identifier data is out of band data
2 with respect to the query data, and wherein the privacy labels and the user identifier
3 include tokens, the method further comprising comparing the tokens in the user identifier
4 data with the tokens in the privacy labels stored in the memory in order to identify the set
5 of the privacy labels.

1 11. A multiple user data storage and separation system, comprising:
2 a processor;
3 memory in communication with the processor and including records
4 defined by correlated tree structures having schema such that the records are unrestricted
5 by relational table structures, the records including user data items associated with
6 multiple different users, the memory also including privacy labels stored in the memory
7 and correlated with each of the records using privacy label tree structures, wherein the
8 privacy labels distinguish among the users; and
9 instructions stored in the memory for directing the processor, the
10 instructions including

11 a receiving module to receive a communication including user
12 identifier data and query data;
13 a label identification module to identify a set of the privacy labels
14 based on the user identifier data;
15 a query processing module to identify a set of the records based on
16 the query data; and
17 a privacy module to return, in response to the communication, only
18 records from the identified set of records that are associated with the set of the
19 privacy labels.

1 12. The system of claim 11, wherein the tree structures defining the records
2 include segment trees, the segment trees including nodes corresponding to the user data
3 items, and wherein the tree structures defining the records stored in the memory further
4 include receipt trees, the receipt trees including receipts that define respective sets of
5 segment tree nodes included in each of the respective records stored in the memory, and
6 wherein each of the nodes in the segment trees has a corresponding one of the receipt
7 trees to define a respective set of the records stored in the memory in which that
8 respective segment tree node is included.

1 13. The system of claim 12, wherein the query processing module identifies
2 the set of the records based on the query data by identifying segment tree nodes
3 associated with the query data, and by identifying receipts correlated with the segment
4 tree nodes associated with the query data using the receipt trees.

1 14. The system of claim 12, wherein the privacy labels are correlated with the
2 receipt trees to define respective sets of the records associated with each of the respective
3 multiple users.

1 15. The printing system of claim 11, wherein the user identifier data is out of
2 band data with respect to the query data, wherein the privacy labels and the user identifier

- 3 data include tokens, and wherein the label identification module identifies the set of the
4 privacy labels by comparing the tokens in the user identifier data with the tokens in the
5 privacy labels stored in the memory.

1/5

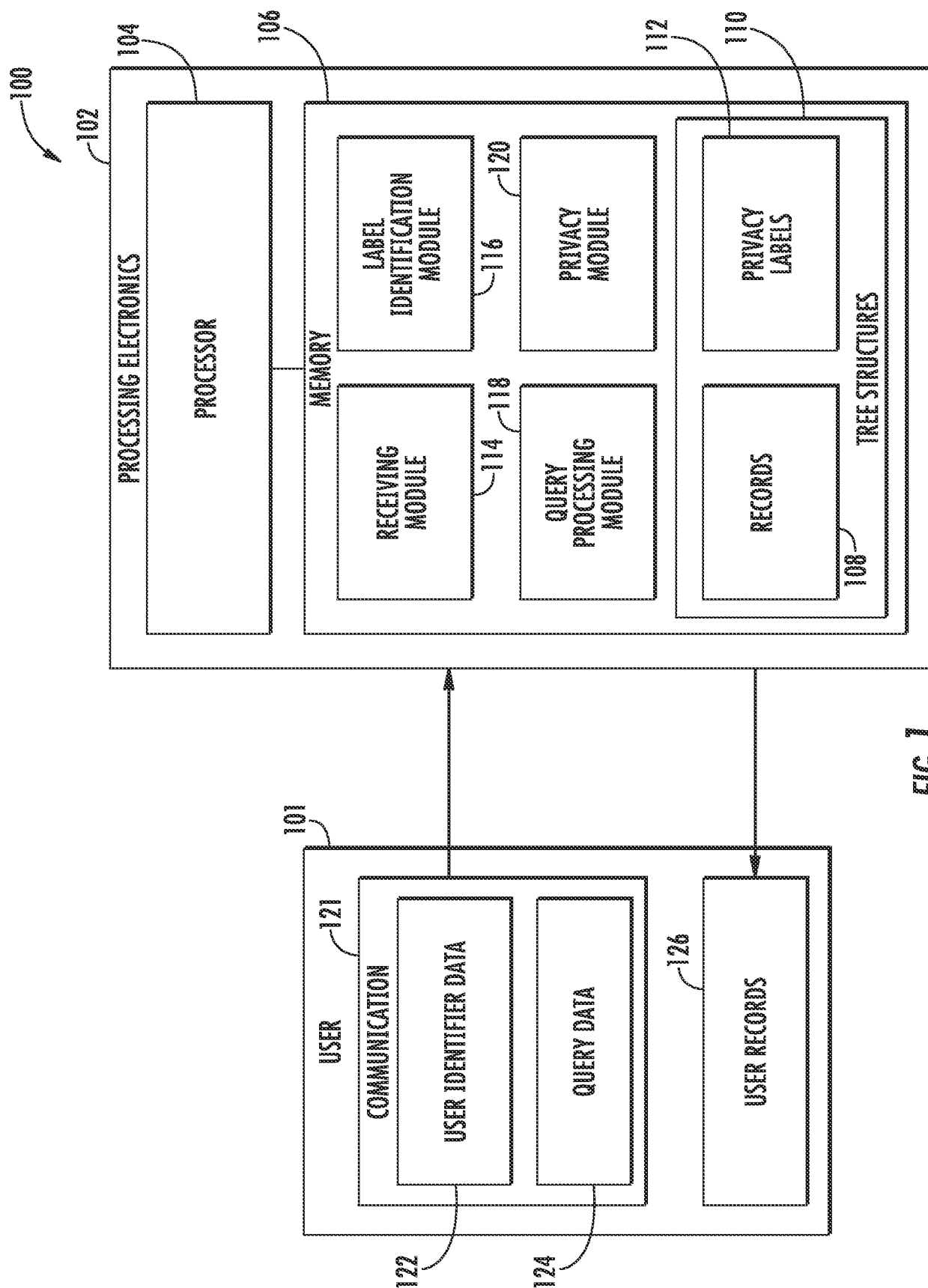


FIG. 1

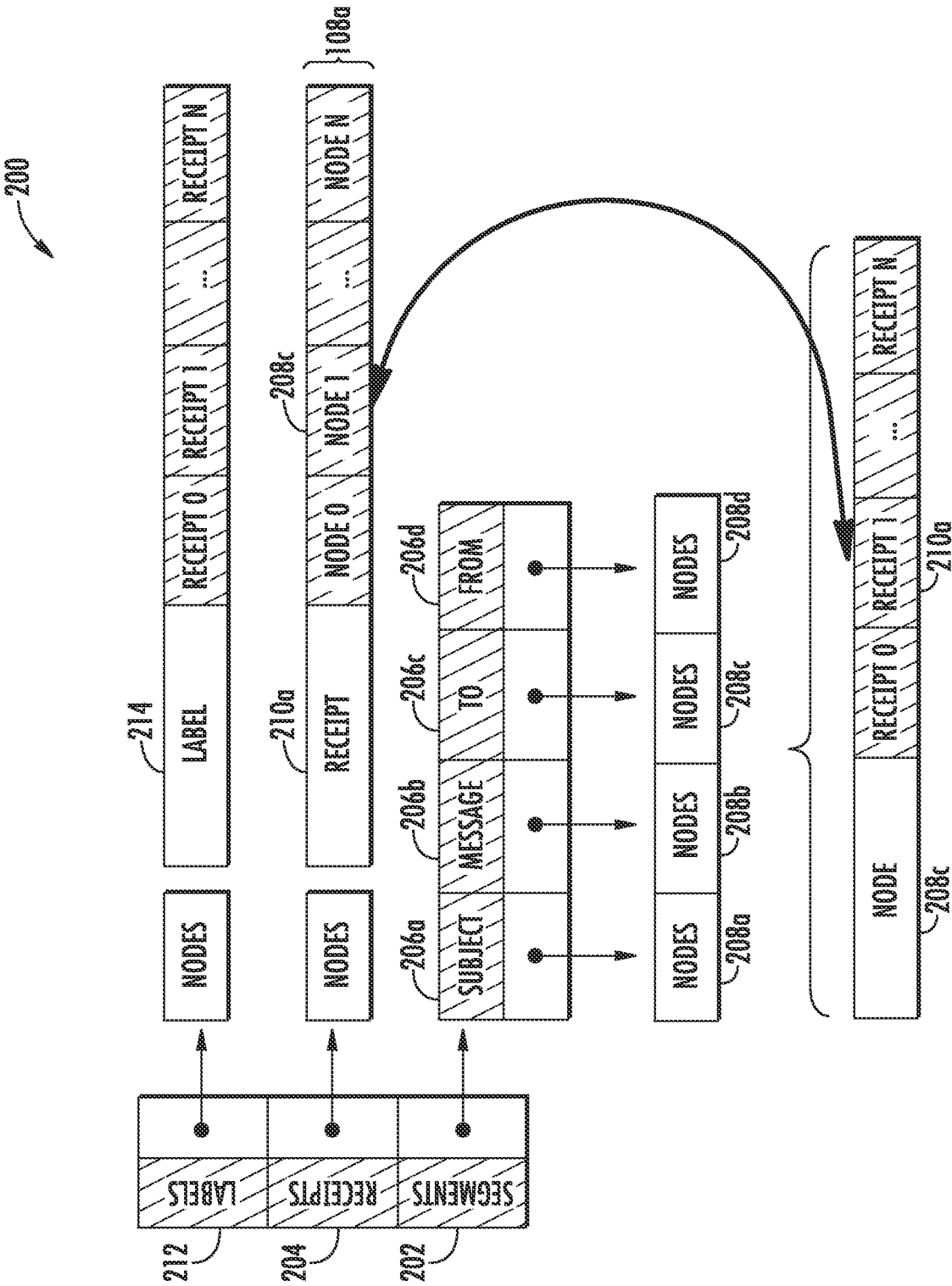


FIG. 2

3/5

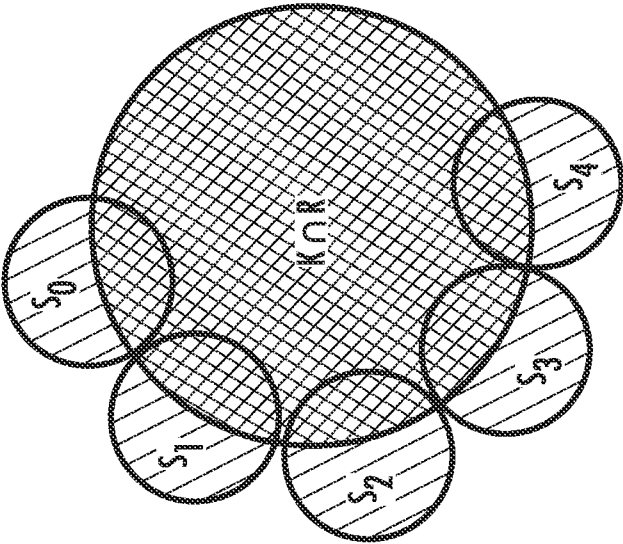


FIG. 3C

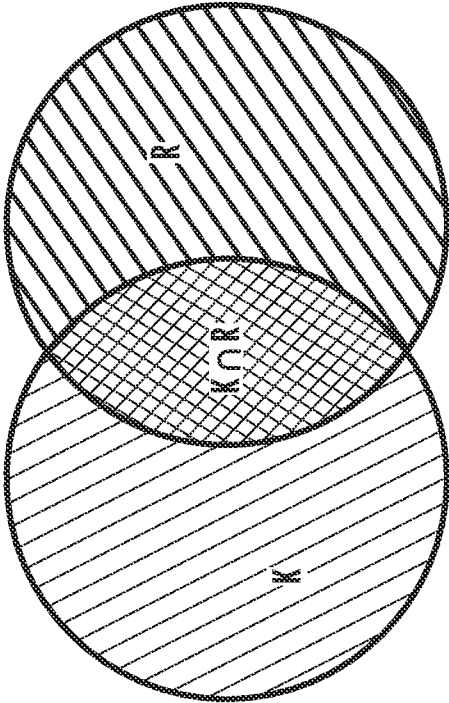


FIG. 3B

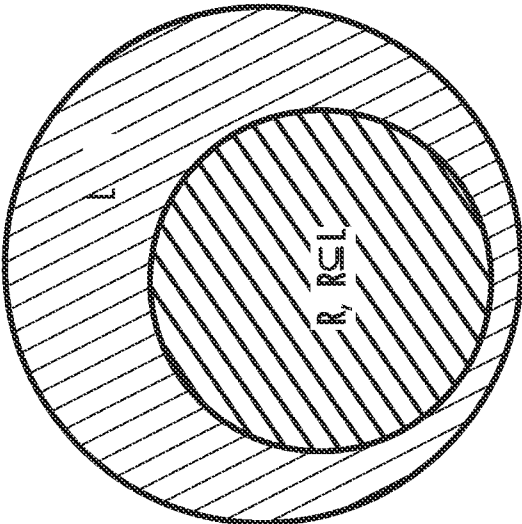


FIG. 3A

4/5

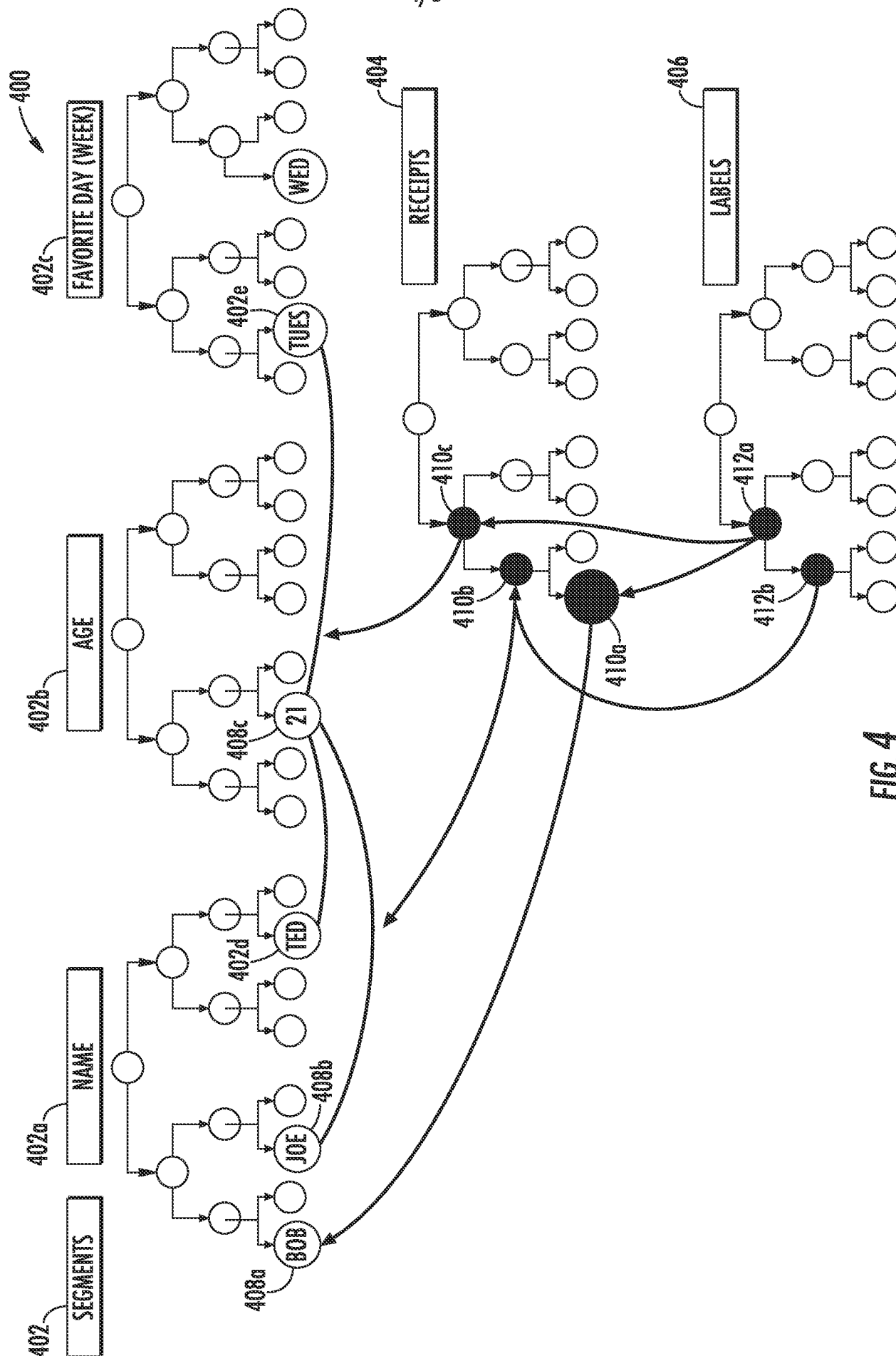


FIG. 4

5/5

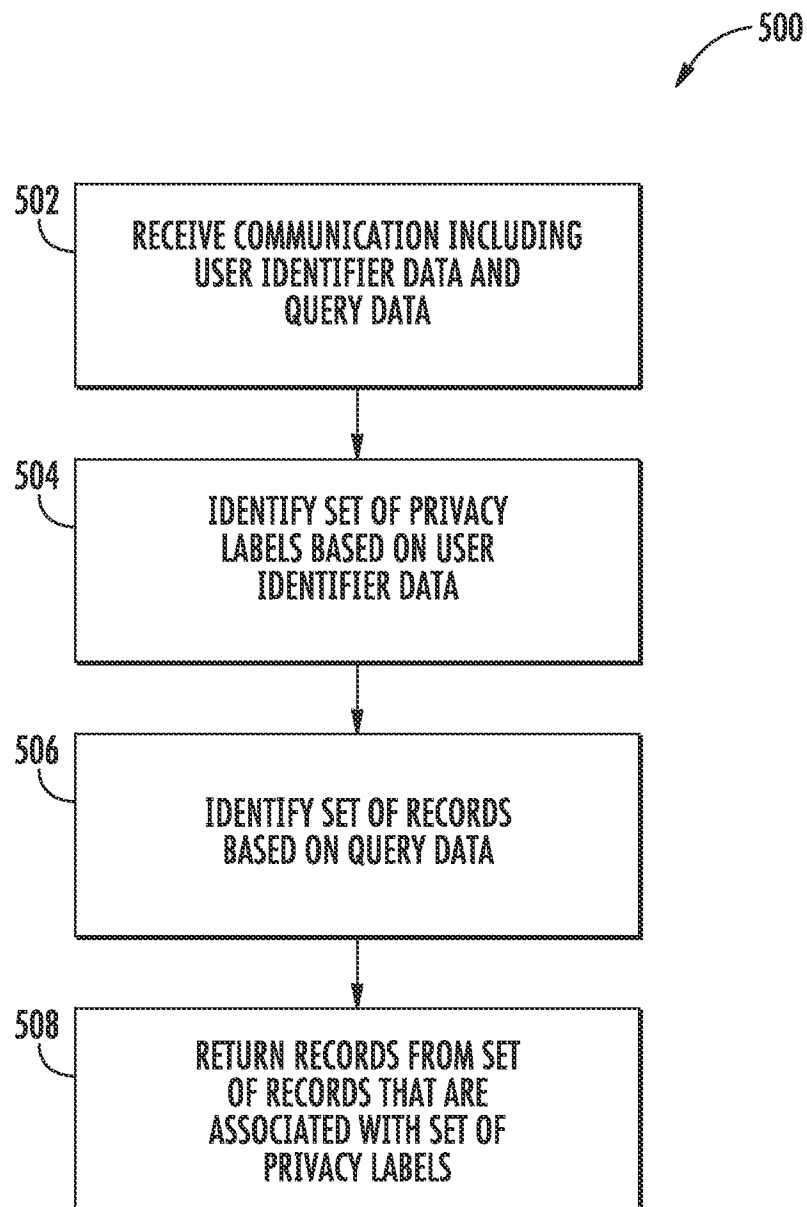


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/013987**A. CLASSIFICATION OF SUBJECT MATTER****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 17/30; G06F 15/16; H04K 1/00; G06F 7/00

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: user, identifier, record, relational, label, tree, structure, 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.
A	US 2008-0046440 A1 (PHILIP F. ESTES) 21 February 2008 See paragraphs [0005], [0008], [0018] and [0025]-[0026]; and figures 1-2.	1-15
A	US 2005-0198017 A1 (MARK GAPONOFF) 08 September 2005 See paragraphs [0037]-[0077] and figures 2-3.	1-15
A	US 2010-0262631 A1 (JOHAN ER ANDERSSON et al.) 14 October 2010 See paragraphs [0024]-[0051] and figures 3-7.	1-15
A	US 2014-0089350 A1 (THOMSON REUTERS GLOBAL RESOURCES) 27 March 2014 See paragraphs [0016]-[0038] and figures 1-4.	1-15
A	US 2006-0005036 A1 (LIMIN HU et al.) 05 January 2006 See paragraphs [0034]-[0042] and figures 3-4C.	1-15

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

30 September 2015 (30.09.2015)

Date of mailing of the international search report

01 October 2015 (01.10.2015)

Name and mailing address of the ISA/KR

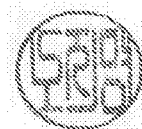
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 35208,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

NHO, Ji Myong

Telephone No. +82-42-481-8528



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/013987

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0046440 A1	21/02/2008	None	
US 2005-0198017 A1	08/09/2005	GB 2427053 A US 7412444 B2 WO 2005-077123 A2 WO 2005-077123 A3	13/12/2006 12/08/2008 25/08/2005 05/07/2007
US 2010-0262631 A1	14/10/2010	None	
US 2014-0089350 A1	27/03/2014	AR 071136 A1 EP 2263161 A1 US 2009-265380 A1 US 8600942 B2 WO 2009-146039 A1	26/05/2010 22/12/2010 22/10/2009 03/12/2013 03/12/2009
US 2006-0005036 A1	05/01/2006	CN 1716305 A US 2006-0004651 A1 US 2012-0158787 A1 US 2014-0373105 A1 US 8126920 B2 US 8762357 B2 US 8990254 B2	04/01/2006 05/01/2006 21/06/2012 18/12/2014 28/02/2012 24/06/2014 24/03/2015