

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 August 2011 (04.08.2011)

PCT

(10) International Publication Number
WO 2011/092686 A1

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/IL20 11/000078

(22) International Filing Date:
23 January 2011 (23.01.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/IL20 10/000069
27 January 2010 (27.01.2010) IL
61/348,822 27 May 2010 (27.05.2010) US
12/814,807 14 June 2010 (14.06.2010) US
12/861,967 24 August 2010 (24.08.2010) u s

(71) Applicant (for all designated States except US): **VARONIS SYSTEMS, INC.** [US/US]; 499 7th Avenue, 23rd Floor, South Tower, New York, New York 11018 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FAITELSON, Yakov** [IL/IL]; 3 Mishol Hasapir Street, 44814 Elkana (IL). **KORKUS, Ohad** [IL/IL]; 11 Galgaley Haplada Street, 46733 Herzelia (IL). **KRETZER-KATZIR, Ophir** [IL/IL]; 23 Tomer Street, 71799 Reut (IL). **BASS, David** [IL/IL]; 26 Hatamar Street, 99797 Carmei Yoseph (IL).

(74) Agents: **SANFORD T. COLB & CO.** et al; P.O. Box 2273, 76122 Rehovot (IL).

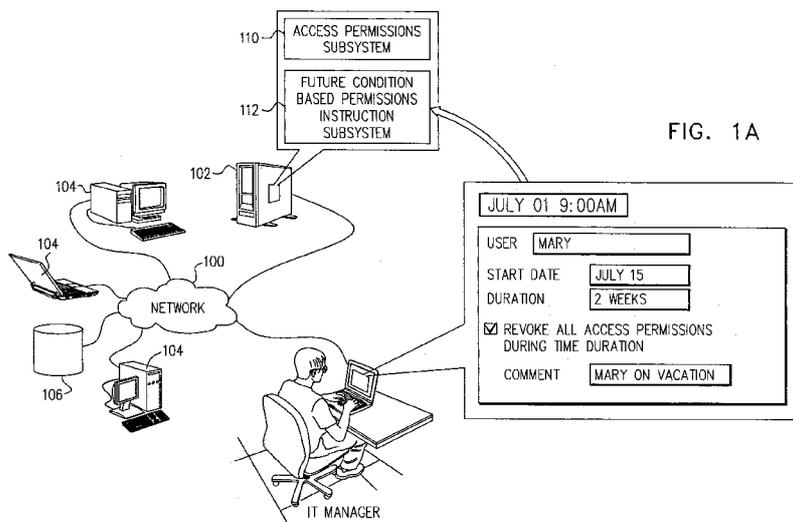
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: TIME DEPENDENT ACCESS PERMISSIONS



(57) Abstract: ABSTRACT A network object access permission management system useful with a computer network including at least one server and a multiplicity of clients, the system including an access permissions subsystem which governs access permissions of users to network objects in the computer network in real time and a future condition based permissions instruction subsystem providing instructions to the access permission subsystem to grant or revoke access permissions of the users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance.

WO 2011/092686 A1

TIME DEPENDENT ACCESS PERMISSIONS

REFERENCE TO RELATED APPLICATIONS

5

Reference is made to U.S. Patent Application Serial No. 12/673,691, filed February 16, 2010, and entitled "ENTERPRISE LEVEL DATA MANAGEMENT", which is a National Phase Application of PCT\IL2010\000069 filed January 27, 2010 and entitled "ENTERPRISE LEVEL DATA MANAGEMENT", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (1) and (2)(i).

Reference is also made to U.S. Patent Application Serial No. 12/814,807, filed June 14, 2010, and entitled "ACCESS PERMISSIONS ENTITLEMENT REVIEW", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (1) and (2)(i).

Reference is also made to U.S. Patent Application Serial No. 12/861,967 filed August 24, 2010, and entitled "TIME DEPENDENT ACCESS PERMISSIONS", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (1) and (2)(i).

Reference is also made to U.S. Provisional Patent Application Serial No. 61/348,822, filed May 27, 2010 and entitled "IMPROVED TOOLS FOR DATA MANAGEMENT BY DATA OWNERS", the disclosure of which is hereby incorporated by reference and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (4) and (5)(i).

Reference is also made to the following patents and patent applications, owned by assignee, the disclosures of which are hereby incorporated by reference:

U.S. Patent Nos. 7,555,482 and 7,606,801;

U.S. Published Patent Application Nos. 2007/0244899, 2008/0271157, 2009/0100058, 2009/0119298 and 2009/0265780; and

U.S. Provisional Patent Application No. 61/240,726.

FIELD OF THE INVENTION

The present invention relates to data management systems and methodologies generally and more particularly to data access permission management
5 systems and methodologies.

BACKGROUND OF THE INVENTION

10 The following patent publications are believed to represent the current state of the art:

U.S. Patent Nos.: 5,465,387; 5,899,991; 6,338,082; 6,393,468; 6,928,439; 7,031,984; 7,068,592; 7,403,925; 7,421,740; 7,555,482 and 7,606,801; and

U.S. Published Patent Application Nos.: 2003/0051026; 2004/0249847;
15 2005/0108206; 2005/0203881; 2005/0120054; 2005/0086529; 2006/0064313; 2006/0184530; 2006/0184459 and 2007/0203872.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved data access permission management systems and methodologies. There is thus provided in accordance with a preferred embodiment of the present invention a network object access permission management system useful with a computer network including at least one server and a multiplicity of clients, the system including an access permissions subsystem which governs access permissions of users to network objects in the computer network in real time and a future condition based permissions instruction subsystem providing instructions to the access permission subsystem to grant or revoke access permissions of the users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance.

In accordance with a preferred embodiment of the present invention, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant or revoke access permissions of the users to the network objects at future times set in advance by the operator. Preferably, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant or revoke access permissions of the users to the network objects in response to the occurrence of future events selected in advance by the operator. Additionally or alternatively, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant and thereafter revoke access permissions of the users to the network objects at future times set in advance by the operator.

Preferably, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to revoke and thereafter regrant pre-existing access permissions of the users to the network objects at future times set in advance by the operator. Additionally or alternatively, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant to the users access permissions to the network objects for a limited duration set in advance by the operator.

Preferably, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant or revoke access

permissions of the users to the network objects based on changes in at least one characteristic of at least one user of the network object indicated in advance by the operator. Additionally or alternatively, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant or revoke
5 access permissions of the users to the network objects based on changes in at least one characteristic of the network object indicated in advance by the operator.

Preferably, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant or revoke access permissions of the users to the network objects based on activity of at least one user
10 related to the network object as indicated in advance by the operator. Additionally or alternatively, the future condition based permission instruction subsystem provides instructions to the access permission subsystem to grant or revoke access permissions of the users to the network objects based on changes in at least one classification of the network object indicated in advance by the operator.

15 There is also provided in accordance with another preferred embodiment of the present invention a network object access permission management method useful with a computer network including at least one server and a multiplicity of clients, the method including providing instructions to grant or revoke access permissions of users to network objects in real time in response to future fulfillment of conditions which are
20 established by an operator in advance, and governing access permissions of the users to network objects in the computer network in real time in response to the instructions.

In accordance with a preferred embodiment of the present invention, the method includes providing instructions to grant or revoke access permissions of the users to the network objects at future times set in advance by the operator. Preferably,
25 the method includes providing instructions to grant or revoke access permissions of the users to the network objects in response to the occurrence of future events selected in advance by the operator. Additionally or alternatively, the method includes providing instructions to grant and thereafter revoke access permissions of the users to the network objects at future times set in advance by the operator.

30 Preferably, the method includes providing instructions to revoke and thereafter regrant pre-existing access permissions of the users to the network objects at future times set in advance by the operator. Additionally or alternatively, the method

includes providing instructions to grant to the users access permissions to the network objects for a limited duration set in advance by the operator.

5 Preferably, the method includes providing instructions to grant or revoke access permissions of the users to the network objects based on changes in at least one characteristic of at least one user of the network object indicated in advance by the operator. Additionally or alternatively, the method includes providing instructions to grant or revoke access permissions of the users to the network objects based on changes in at least one characteristic of the network object indicated in advance by the operator.

10 Preferably, the method includes providing instructions to grant or revoke access permissions of the users to the network objects based on activity of at least one user related to the network object as indicated in advance by the operator. Additionally or alternatively, the method includes providing instructions to grant or revoke access permissions of the users to the network objects based on changes in at least one classification of the network object indicated in advance by the operator.

15

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in
5 which:

Figs. 1A, 1B, 1C, 1D, and 1E are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for revoking and thereafter regranting pre-existing access permissions of a user to network objects at future times set in advance by an operator;

10 Figs. 2A, 2B, 2C, 2D, and 2E are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for revoking and thereafter regranting pre-existing access permissions of a user to network objects in response to a future event set in advance by an operator;

15 Figs. 3A, 3B and 3C are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for changing access permissions of a user to network objects in response to a future event at a known date set in advance by an operator;

20 Figs. 4A, 4B and 4C are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for changing access permissions of a user to network objects in response to a future event associated with a related user at a known date set in advance by an operator;

Fig. 5 is a simplified flowchart indicating steps in the operation of the data access permission management system of Fig. 1; and

25 Fig. 6 is another simplified flowchart indicating steps in the operation of the data access permission management system of Fig. 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Figs. 1A, 1B, 1C, 1D and 1E, which are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for revoking and thereafter regranting pre-existing access permissions of a user to network objects at future times set in advance by an operator.

As seen generally in Figs. 1A - 1E, the network object access permission management system is useful with a computer network 100 including at least one server 102 and a multiplicity of clients 104. One or more storage elements 106 are also preferably provided. The system preferably resides on the server 102 and preferably includes:

an access permissions subsystem 110 which governs access permissions of users to network objects in the computer network 100 in real time; and
a future condition-based permissions instruction subsystem 112 providing instructions to the access permission subsystem 110 to grant or revoke access permissions of the users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance.

The term "network object" for the purposes of this application is defined to include user generated enterprise computer network resources on any commercially available computer operating system. Examples of network objects include structured and unstructured computer data resources such as files and folders, and user groups.

Access permissions of users to network objects may include for example, read or write permissions to a file, modification permissions to a folder (e.g. permissions to create or delete files), and modification permissions to a user group (e.g. permissions to add or remove a user from the group).

Fig. 1A shows a stage in typical operation of the data access permission management system, wherein an IT manager employs the future condition-based permission instruction subsystem 112 for revoking all access permissions for an employee about to go on vacation. The IT manager sets a future start date and a duration for the revocation, after which duration, the access permissions will be automatically restored.

Fig. 1B shows that at 12:01AM on July 15, the future start date set by the IT manager, the future condition-based permission instruction subsystem 112 automatically provides instructions to the access permission subsystem to immediately revoke all access permissions to the employee.

5 As seen in Fig. 1C, for the duration of the employee's vacation, typically on July 21, access is denied to the employee.

Fig. 1D illustrates that automatically upon expiration of the above duration, the future condition-based permission instruction subsystem automatically provides instructions to the access permission subsystem to immediately regrant all
10 access permissions to the employee and Fig. 1E illustrates that thereafter, the employee employs the restored access permissions.

Reference is now made to Figs. 2A, 2B, 2C, 2D, and 2E, which are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for revoking and thereafter regranting
15 pre-existing access permissions of a user to network objects in response to a future event set in advance by an operator.

As seen generally in Figs. 2A - 2E, the network object access permission management system is useful with a computer network 200 including at least one server 202 and a multiplicity of clients 204. One or more storage elements 206 are also
20 preferably provided. The system preferably resides on the server 202 and preferably includes:

an access permissions subsystem 210 which governs access permissions of users to network objects in the computer network 200 in real time; and

25 a future condition-based permissions instruction subsystem 212 providing instructions to the access permission subsystem 210 to grant or revoke access permissions of the users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance.

Fig. 2A shows a stage in typical operation of the data access permission management system, wherein an IT manager employs the future condition-based
30 permission instruction subsystem 212 for revoking all access permissions for an employee who is about to give birth and go on maternity leave. The IT manager sets a

condition for revoking access permissions, i.e. maternity leave, after which duration, the access permissions will be automatically restored.

Fig. 2B shows that at 12:01AM on July 15, the future condition-based permission instruction subsystem 212 routinely queries a human resources system 218 residing on a server 220 connected to the network 200, whether the employee has given birth and is now on maternity leave. Upon discovering that the employee is now indeed on maternity leave, the future condition-based permission instruction subsystem 212 orders the access permissions subsystem 210 to revoke all access permissions from the employee.

As seen in Fig. 2C, for the duration of the employee's maternity leave, typically on July 21, access is denied to the employee.

Fig. 2D illustrates that on July 29 the future condition-based permission instruction subsystem 212 routinely queries the human resources system 218 and discovers that the employee is no longer on maternity leave. The future condition-based permission instruction subsystem 212 immediately orders the access permissions subsystem 210 to regrant all access permissions to the employee, and Fig. 2E illustrates that thereafter, the employee employs the restored access permissions.

Reference is now made to Figs. 3A, 3B and 3C, which are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for changing access permissions of a user to network objects in response to a future event at a known date set in advance by an operator

As seen generally in Figs. 3A - 3C, the network object access permission management system is useful with a computer network 300 including at least one server 302 and a multiplicity of clients 304. One or more storage elements 306 are also preferably provided. The system preferably resides on the server 302 and preferably includes:

an access permissions subsystem 310 which governs access permissions of users to network objects in the computer network 300 in real time; and

a future condition-based permissions instruction subsystem 312 providing instructions to the access permission subsystem 310 to grant or revoke access

permissions of the users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance.

Fig. 3A shows a stage in typical operation of the data access permission management system, wherein an IT manager employs the future condition-based permission instruction subsystem 312 for revoking all access permissions for an employee to certain enterprise resources and for granting access permissions for the employee to other enterprise resources, due to the employee transferring to another department in the enterprise. The IT manager sets a future start date for the simultaneous revocation and granting of access permissions.

Fig. 3B shows that at 12:01AM on July 15, the future start date set by the IT manager, the future condition-based permission instruction subsystem 312 automatically provides instructions to the access permission subsystem 310 to immediately revoke all existing access permissions to the employee, and to grant new, alternative, access permissions to the employee.

As seen in Fig. 3C, after transferring to another department in the enterprise, typically on July 21, access to resources belonging to the previous department is denied to the employee, while access to resources belonging to the employee's new department is granted.

Reference is now made to Figs. 4A, 4B and 4C, which are simplified pictorial illustrations of operation of the data access permission management system of an embodiment of the present invention for changing access permissions of a user to network objects in response to a future event associated with a related user at a known date set in advance by an operator.

As seen generally in Figs. 4A - 4C, the network object access permission management system is useful with a computer network 400 including at least one server 402 and a multiplicity of clients 404. One or more storage elements 406 are also preferably provided. The system preferably resides on the server 402 and preferably includes:

an access permissions subsystem 410 which governs access permissions of users to network objects in the computer network 400 in real time; and

a future condition-based permissions instruction subsystem 412 providing instructions to the access permission subsystem 410 to grant or revoke access

permissions of the users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance.

Fig. 4A shows a stage in typical operation of the data access permission management system, wherein an IT manager employs the future condition-based permission instruction subsystem 412 for revoking all access permissions for an employee to certain enterprise resources and for granting access permissions for the employee to other enterprise resources, due to the employee transferring to another department in the enterprise as a result of the employee's manager transferring to another department in the enterprise. The IT manager sets a future start date for the simultaneous revocation and granting of access permissions.

Fig. 4B shows that at 12:01AM on July 15, the future start date set by the IT manager, the future condition-based permission instruction subsystem 412 automatically provides instructions to the access permission subsystem 410 to immediately revoke all existing access permissions to the employee, and to grant new, alternative, access permissions to the employee.

As seen in Fig. 4C, after transferring to another department in the enterprise, typically on July 21, access to resources belonging to the previous department is denied to the employee, while access to resources belonging to the employee's new department is granted.

Reference is now made to Fig. 5, which is a simplified flowchart indicating steps in the operation of the data access-permission management system of Fig. 1. As shown in Fig. 5, an IT manager utilizes the system by entering to the system an access permissions modification instruction to be implemented by the system upon fulfillment of a future condition. For example, the future condition may comprise the occurrence of a future date or an employee related event such as leave of absence of an employee, maternity leave, vacation leave, termination of employment of an employee and transfer of an employee to another department in the enterprise. The access permissions modification instruction may comprise granting or revoking access permissions of users to network objects.

The system continuously monitors relevant resources on the computer enterprise network for the fulfillment of the future condition. The resources may include, for example, human resources databases and IT security-related systems.

Upon discovery that the future condition has been fulfilled, the system implements the access permissions modification instruction, and removes the access permissions modification instruction and its related future condition from the system.

Reference is now made to Fig. 6, which is another simplified flowchart indicating steps in the operation of the data access permission management system of Fig. 1. As shown in Fig. 6, an IT manager utilizes the system by entering to the system a temporary access permissions modification instruction to be implemented by the system for the duration of a future state. For example, the future state may comprise the occurrence of a future date or range of dates, or an employee related state such as leave of absence of an employee, maternity leave, vacation leave and temporary transfer of an employee to another department in the enterprise. The temporary access permissions modification instruction may comprise temporarily granting or revoking access permissions of users to network objects.

The system continuously monitors relevant resources on the computer enterprise network for the existence of the state. The resources may include, for example, human resources databases and IT security-related systems.

Upon discovering the existence of the state, the system implements the temporary access permissions modification instruction. The system continues to monitor relevant resources on the computer enterprise network for the continued existence of the state.

Upon discovering that the state no longer exists, the system reverses the temporary access permissions modification instruction, and removes the temporary access permissions modification instruction and its related future state from the system.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove as well as modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not in the prior art.

30

CLAIMS

1. A network object access permission management system useful with a computer network including at least one server and a multiplicity of clients, the system
5 comprising:
an access permissions subsystem which governs access permissions of users to network objects in said computer network in real time; and
a future condition based permissions instruction subsystem providing instructions to said access permission subsystem to grant or revoke access permissions
10 of said users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance.
2. A network object access permission management system according to claim 1 and wherein said future condition based permission instruction subsystem
15 provides instructions to said access permission subsystem to grant or revoke access permissions of said users to said network objects at future times set in advance by said operator.
3. A network object access permission management system according to
20 claim 1 and wherein said future condition based permission instruction subsystem provides instructions to said access permission subsystem to grant or revoke access permissions of said users to said network objects in response to the occurrence of future events selected in advance by said operator.
- 25 4. A network object access permission management system according to claim 1 and wherein said future condition based permission instruction subsystem provides instructions to said access permission subsystem to grant and thereafter revoke access permissions of said users to said network objects at future times set in advance by said operator.
30
5. A network object access permission management system according to claim 1 and wherein said future condition based permission instruction subsystem

provides instructions to said access permission subsystem to revoke and thereafter regrant pre-existing access permissions of said users to said network objects at future times set in advance by said operator.

5 6. A network object access permission management system according to claim 1 and wherein said future condition based permission instruction subsystem provides instructions to said access permission subsystem to grant to said users access permissions to said network objects for a limited duration set in advance by said operator.

10

7. A network object access permission management system according to claim 1 and wherein said future condition based permission instruction subsystem provides instructions to said access permission subsystem to grant or revoke access permissions of said users to said network objects based on changes in at least one
15 characteristic of at least one user of said network object indicated in advance by said operator.

8. A network object access permission management system according to claim 1 and wherein said future condition based permission instruction subsystem
20 provides instructions to said access permission subsystem to grant or revoke access permissions of said users to said network objects based on changes in at least one characteristic of said network object indicated in advance by said operator.

9. A network object access permission management system according to
25 claim 1 and wherein said future condition based permission instruction subsystem provides instructions to said access permission subsystem to grant or revoke access permissions of said users to said network objects based on activity of at least one user related to said network object as indicated in advance by said operator.

30 10. A network object access permission management system according to claim 1 and wherein said future condition based permission instruction subsystem provides instructions to said access permission subsystem to grant or revoke access

permissions of said users to said network objects based on changes in at least one classification of said network object indicated in advance by said operator.

11. A network object access permission management method useful with a
5 computer network including at least one server and a multiplicity of clients, the method comprising:

providing instructions to grant or revoke access permissions of users to network objects in real time in response to future fulfillment of conditions which are established by an operator in advance; and

10 governing access permissions of said users to network objects in said computer network in real time in response to said instructions.

12. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant or revoke
15 access permissions of said users to said network objects at future times set in advance by said operator.

13. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant or revoke
20 access permissions of said users to said network objects in response to the occurrence of future events selected in advance by said operator.

14. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant and
25 thereafter revoke access permissions of said users to said network objects at future times set in advance by said operator.

15. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to revoke and
30 thereafter regrant pre-existing access permissions of said users to said network objects at future times set in advance by said operator.

16. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant to said users access permissions to said network objects for a limited duration set in advance by said operator.

5

17. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant or revoke access permissions of said users to said network objects based on changes in at least one characteristic of at least one user of said network object indicated in advance by said operator.

10

18. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant or revoke access permissions of said users to said network objects based on changes in at least one characteristic of said network object indicated in advance by said operator.

15

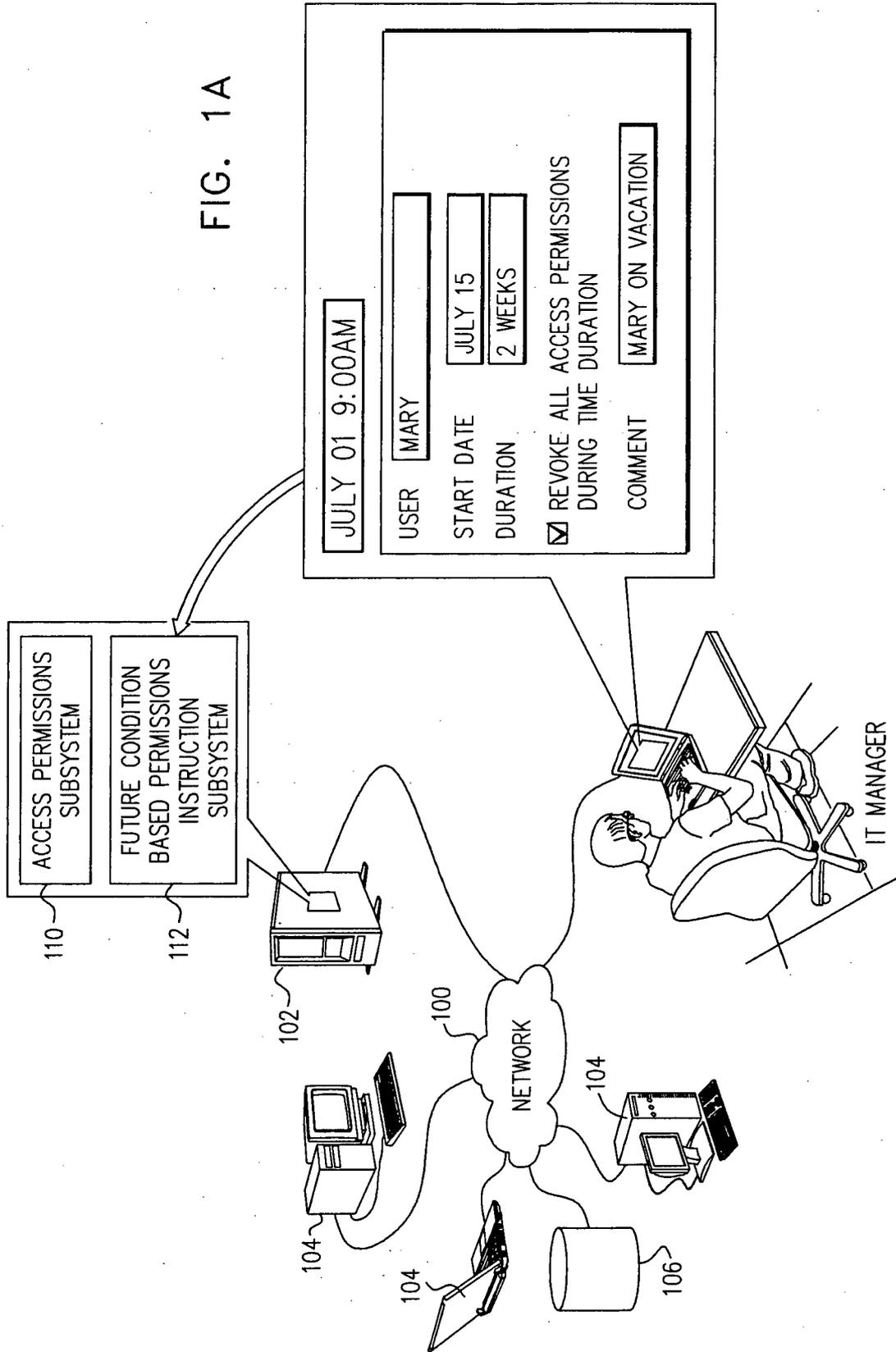
19. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant or revoke access permissions of said users to said network objects based on activity of at least one user related to said network object as indicated in advance by said operator.

20

20. A network object access permission management method according to claim 11 and wherein said method includes providing instructions to grant or revoke access permissions of said users to said network objects based on changes in at least one classification of said network object indicated in advance by said operator.

25

FIG. 1A



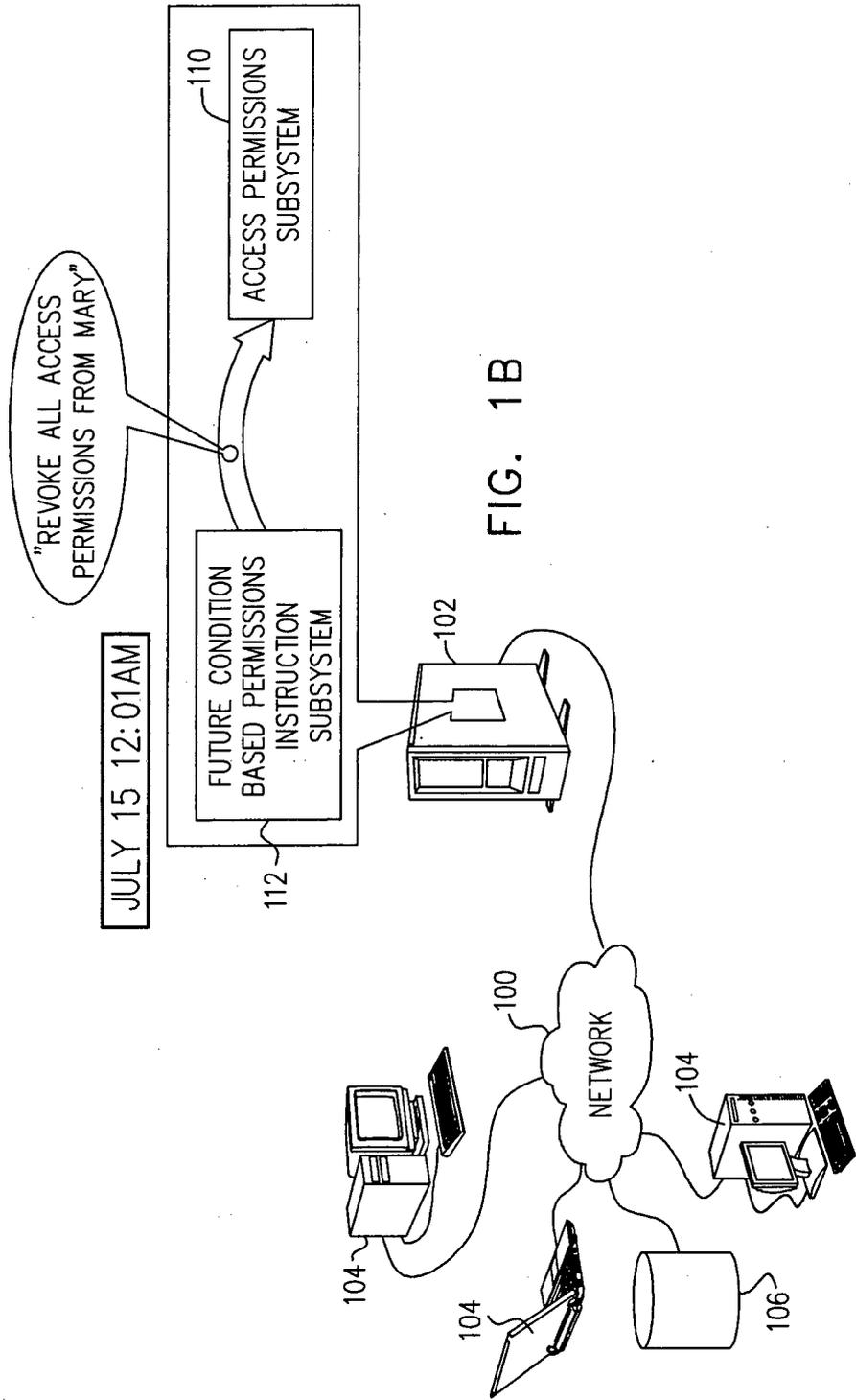
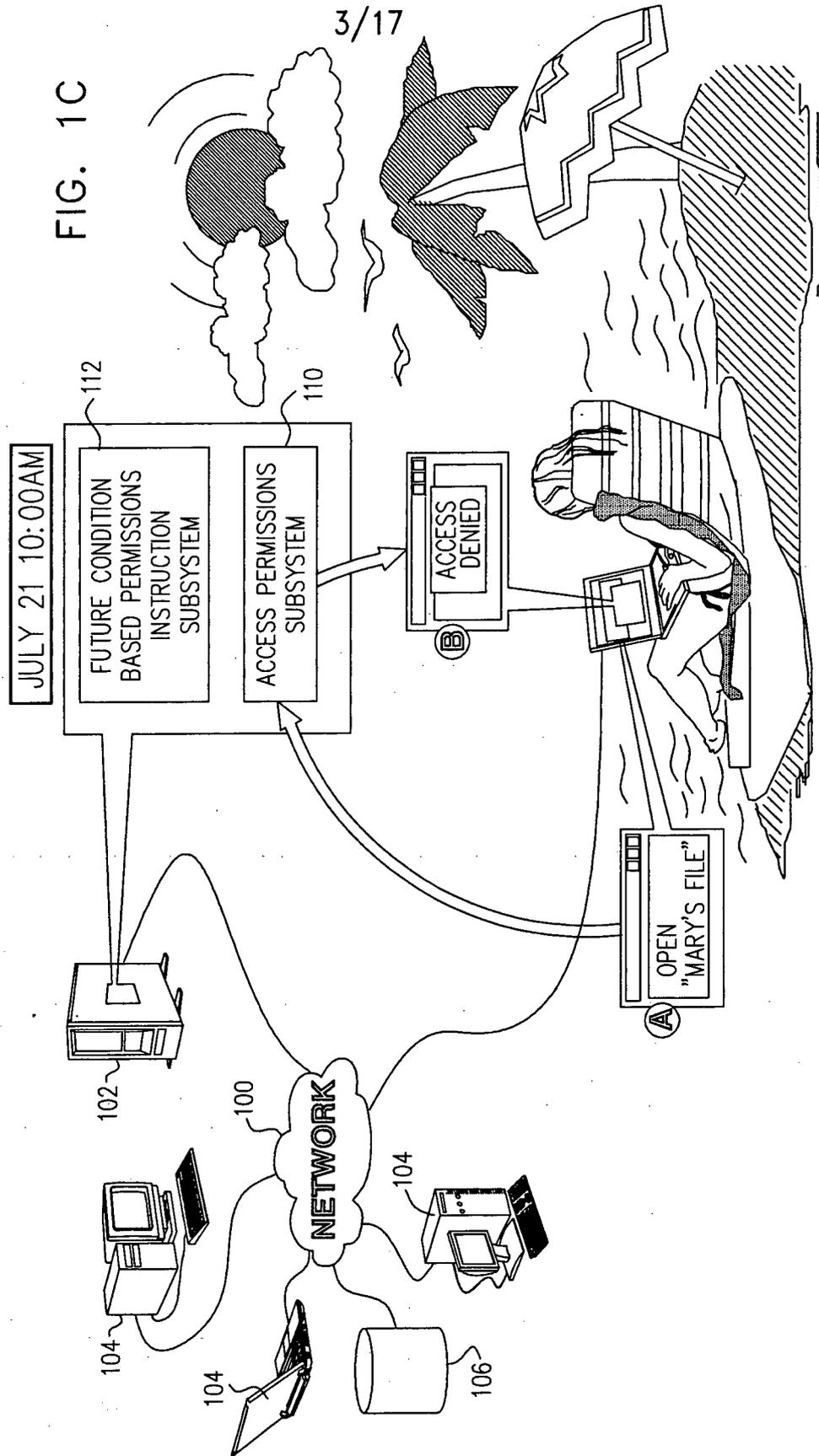
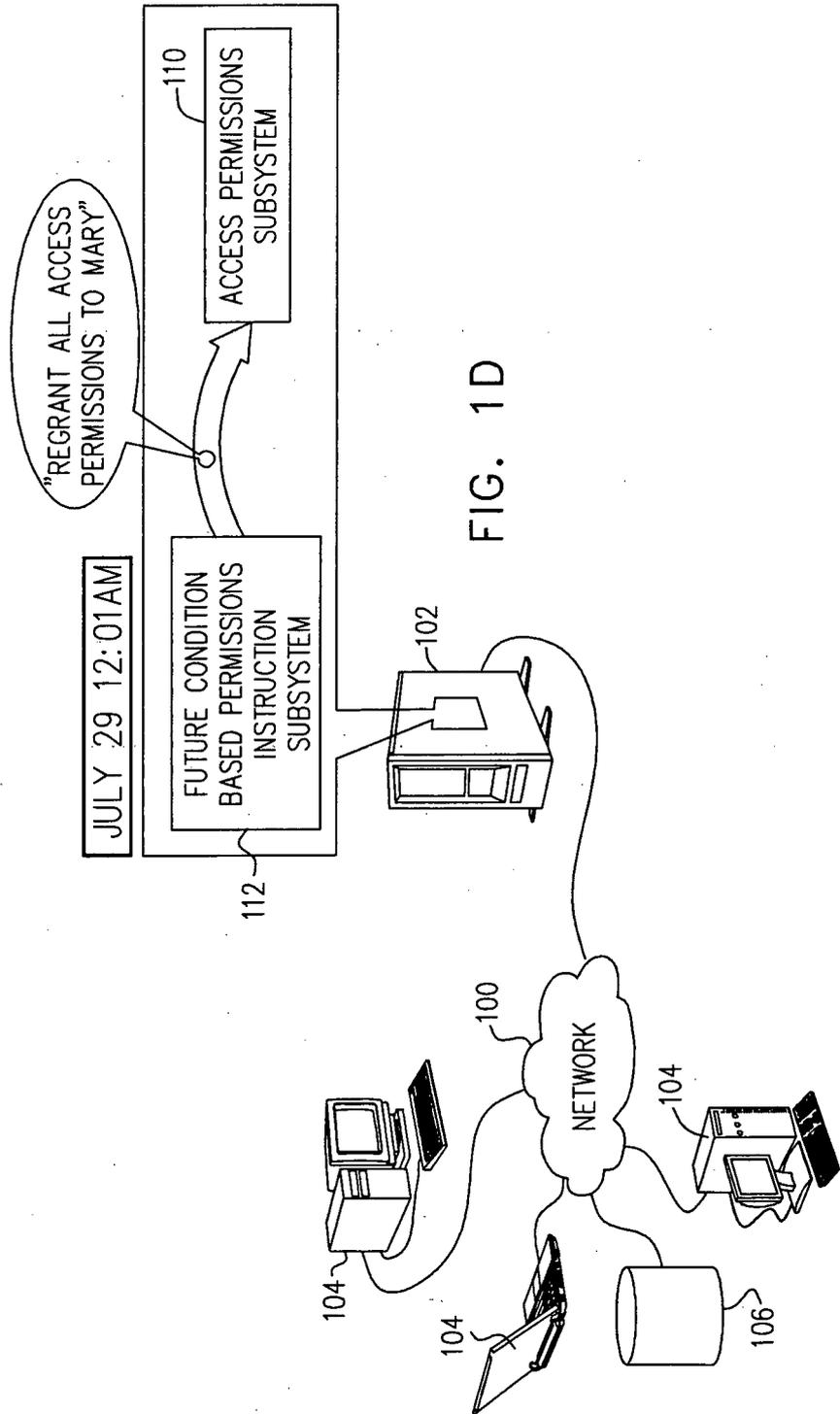


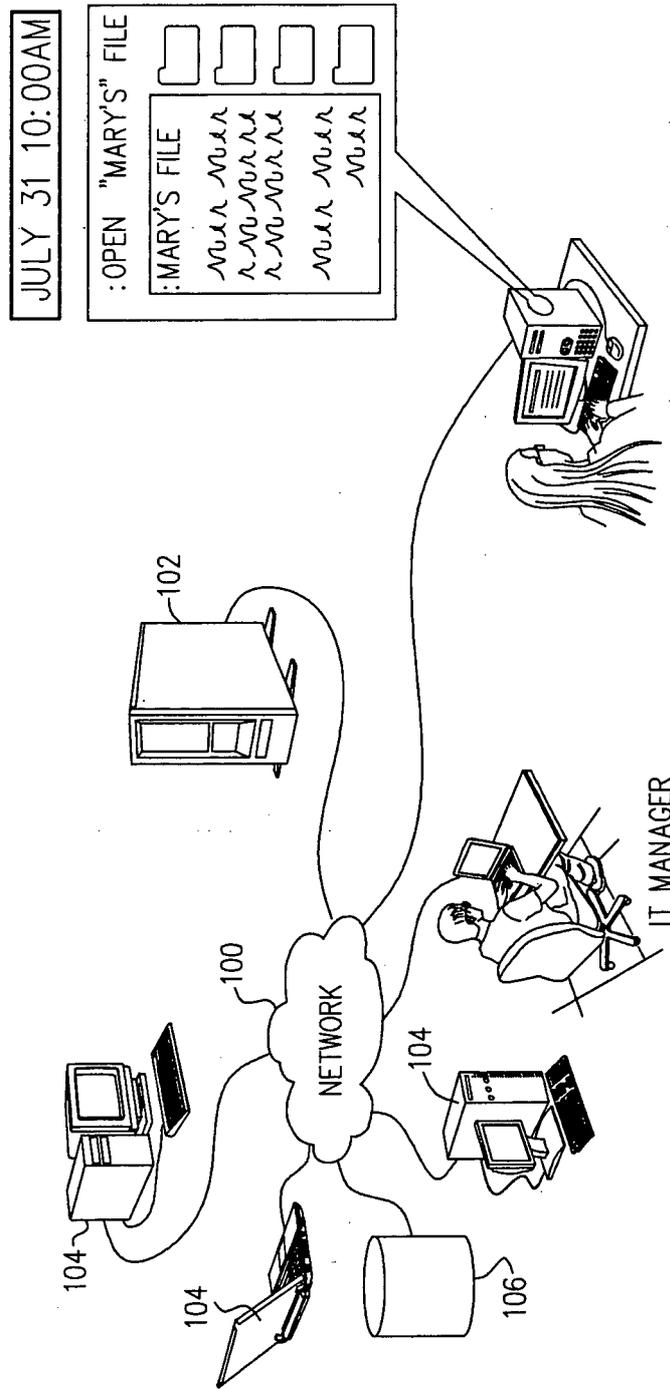
FIG. 1B





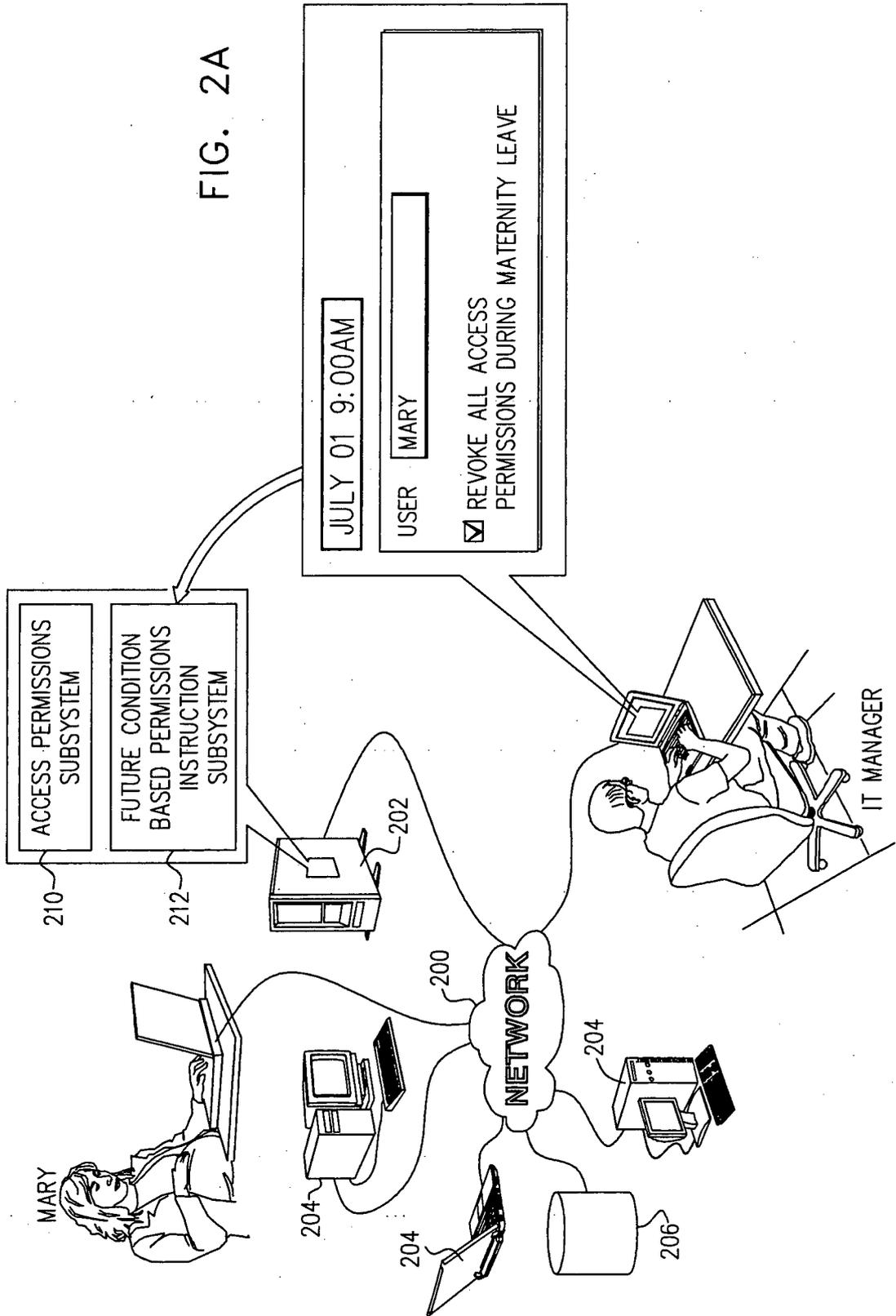
5/17

FIG. 1E



6/17

FIG. 2A



7/17

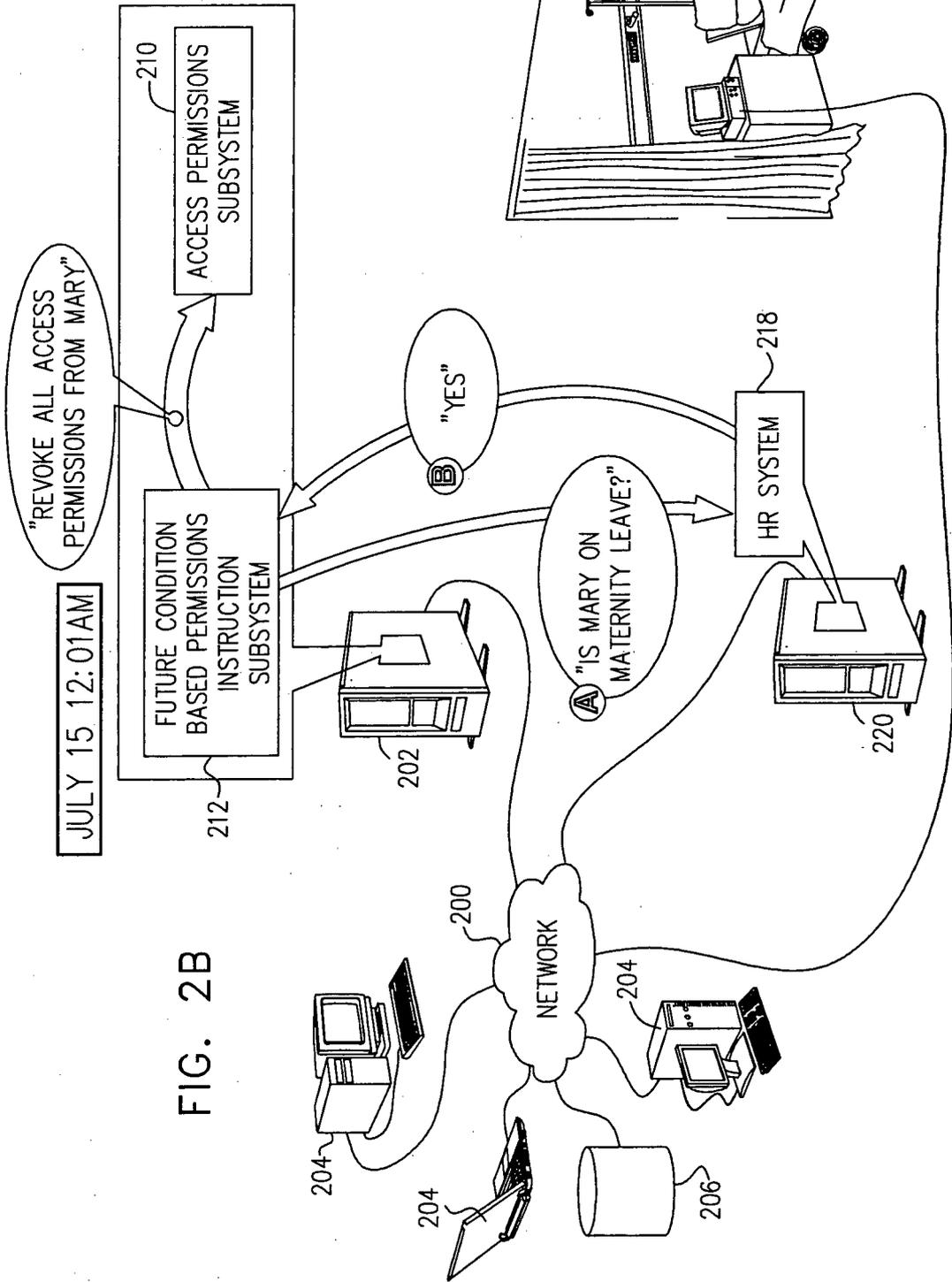
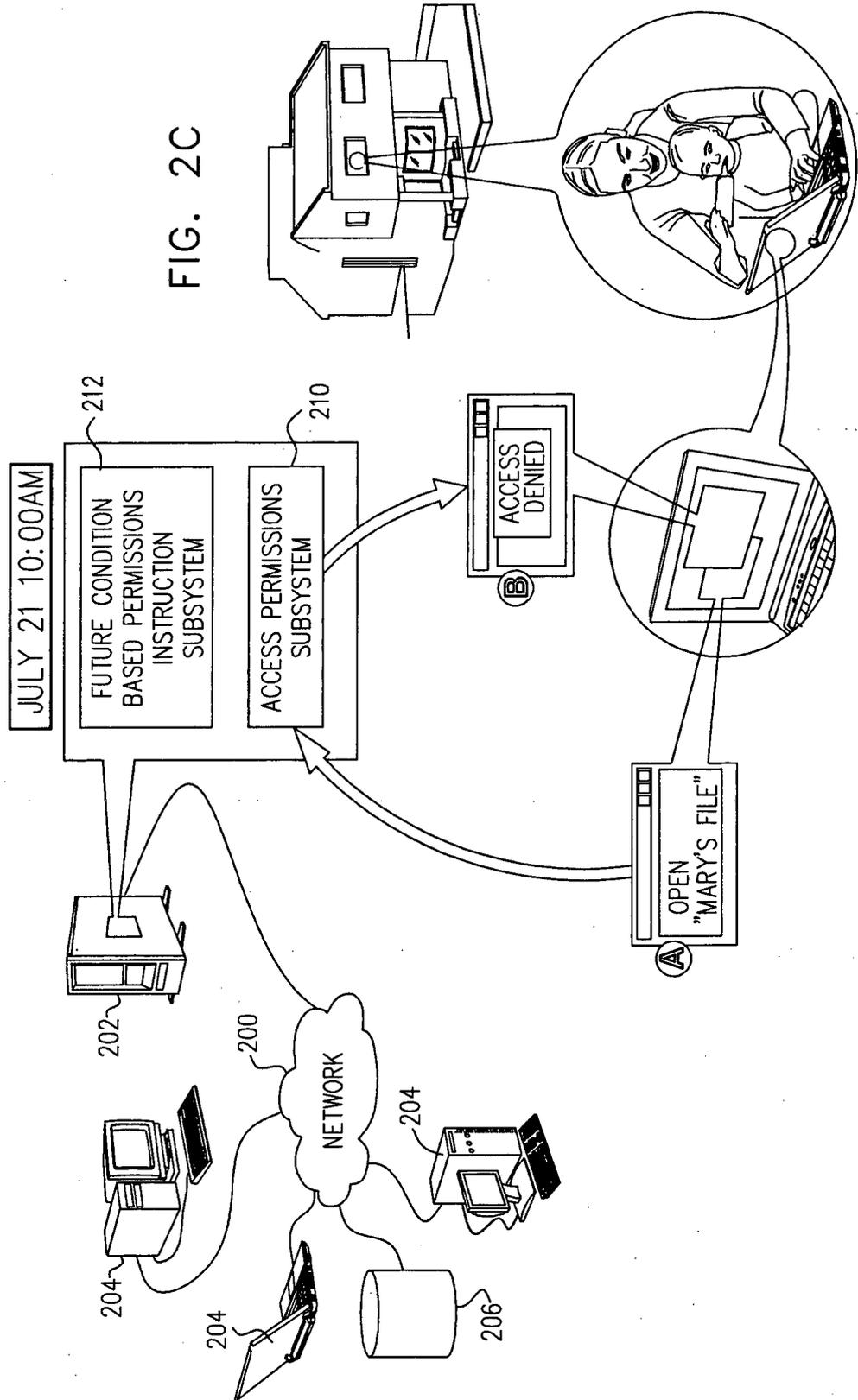


FIG. 2B

8/17

FIG. 2C



9/17

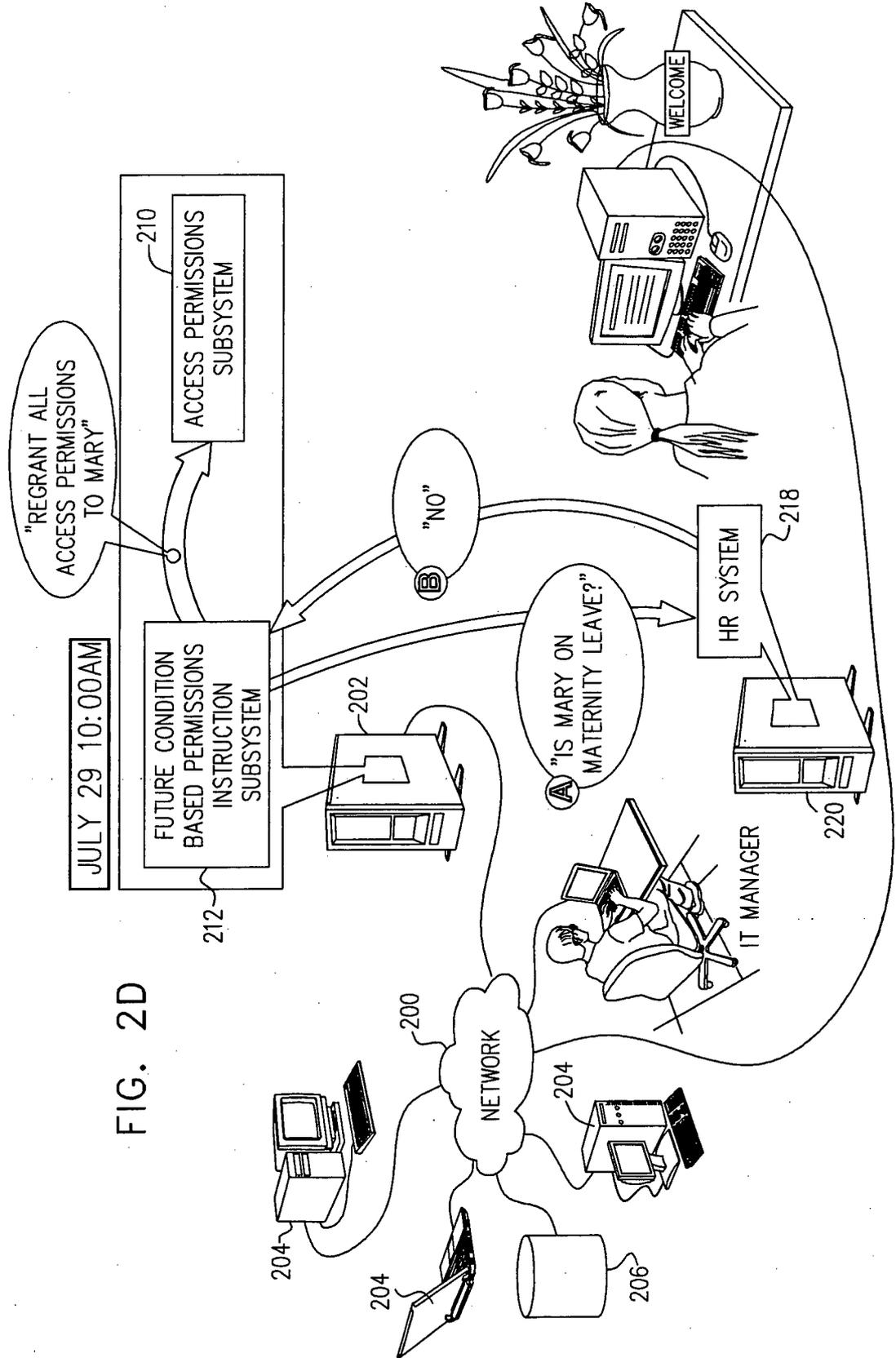
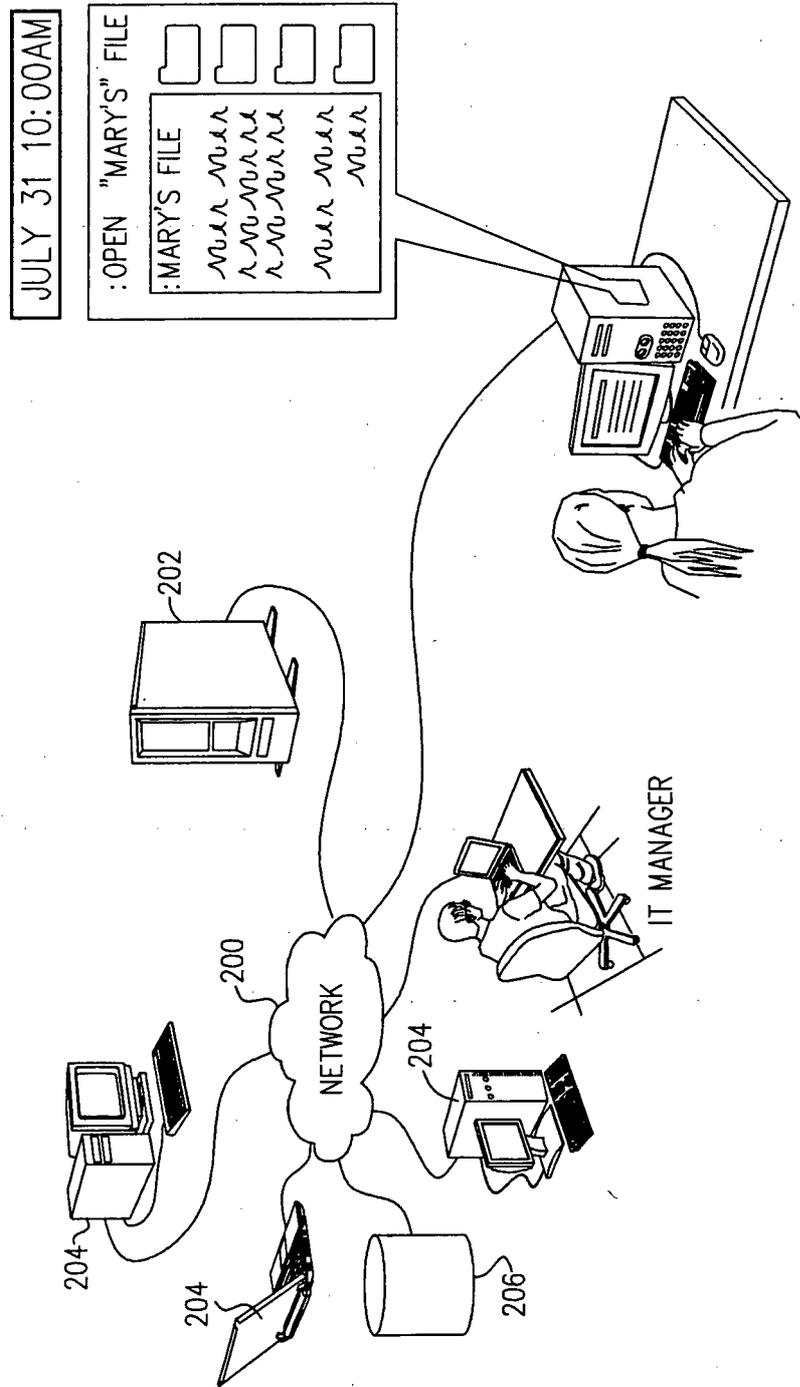


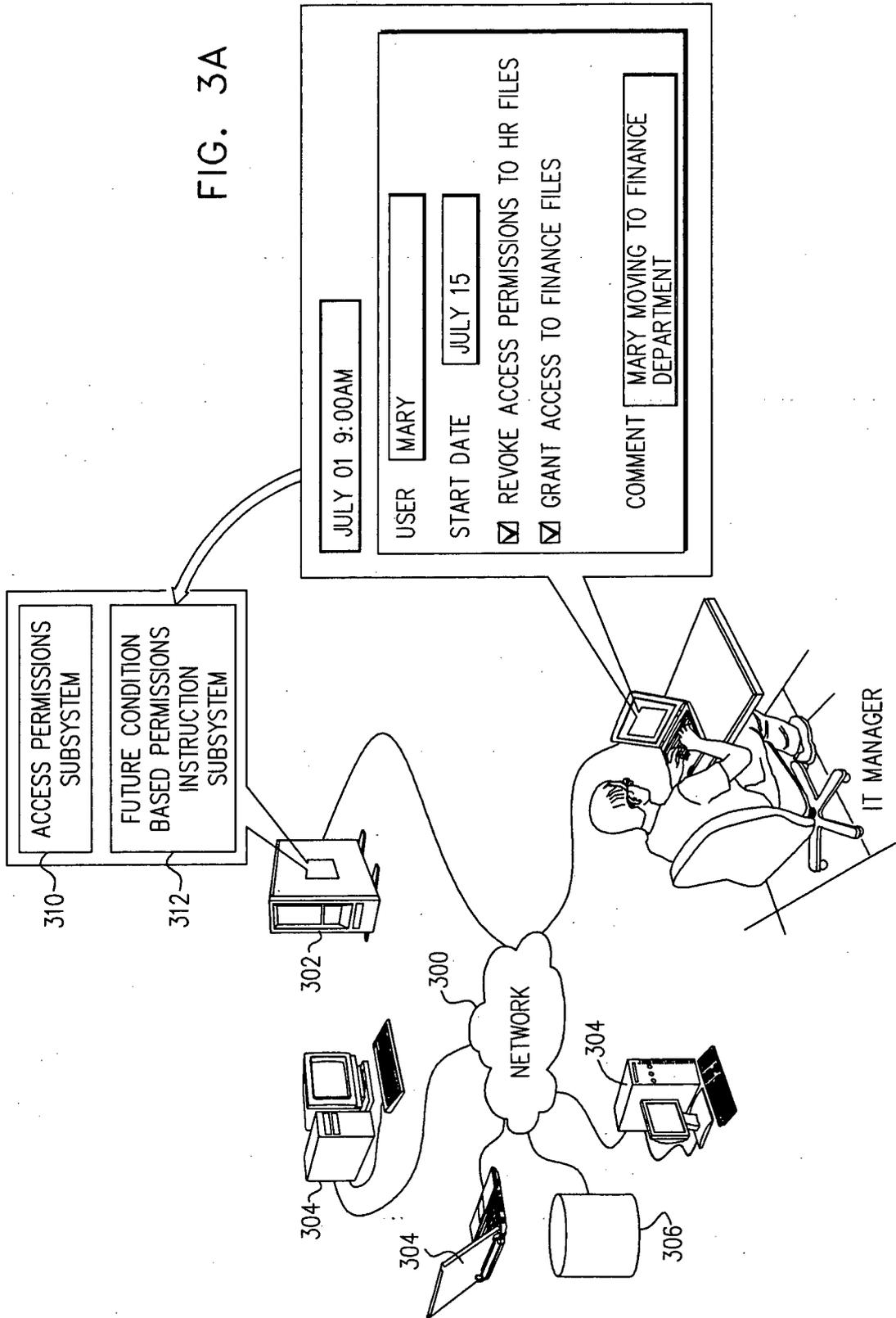
FIG. 2D

FIG. 2E



11/17

FIG. 3A



12/17

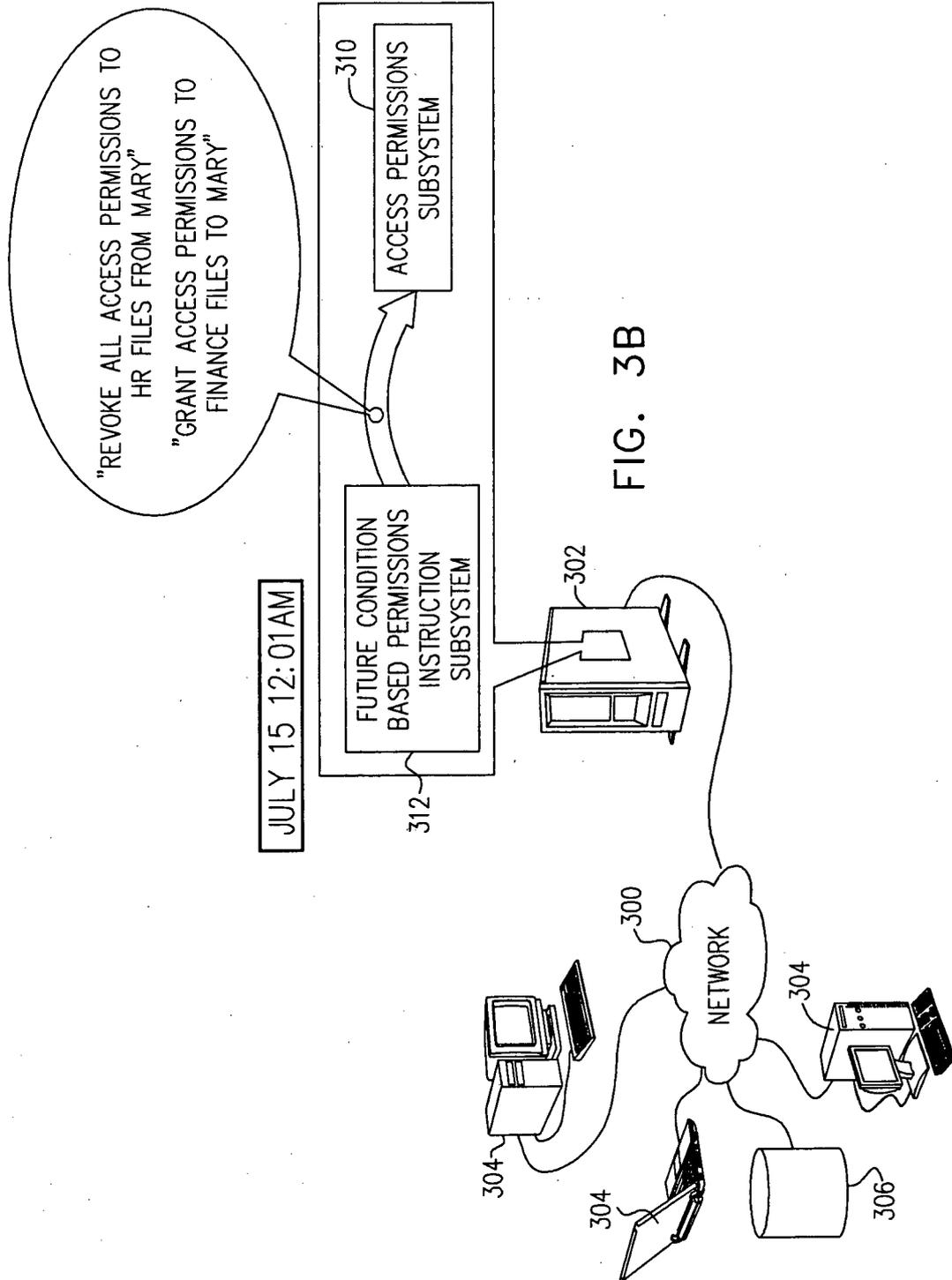


FIG. 3B

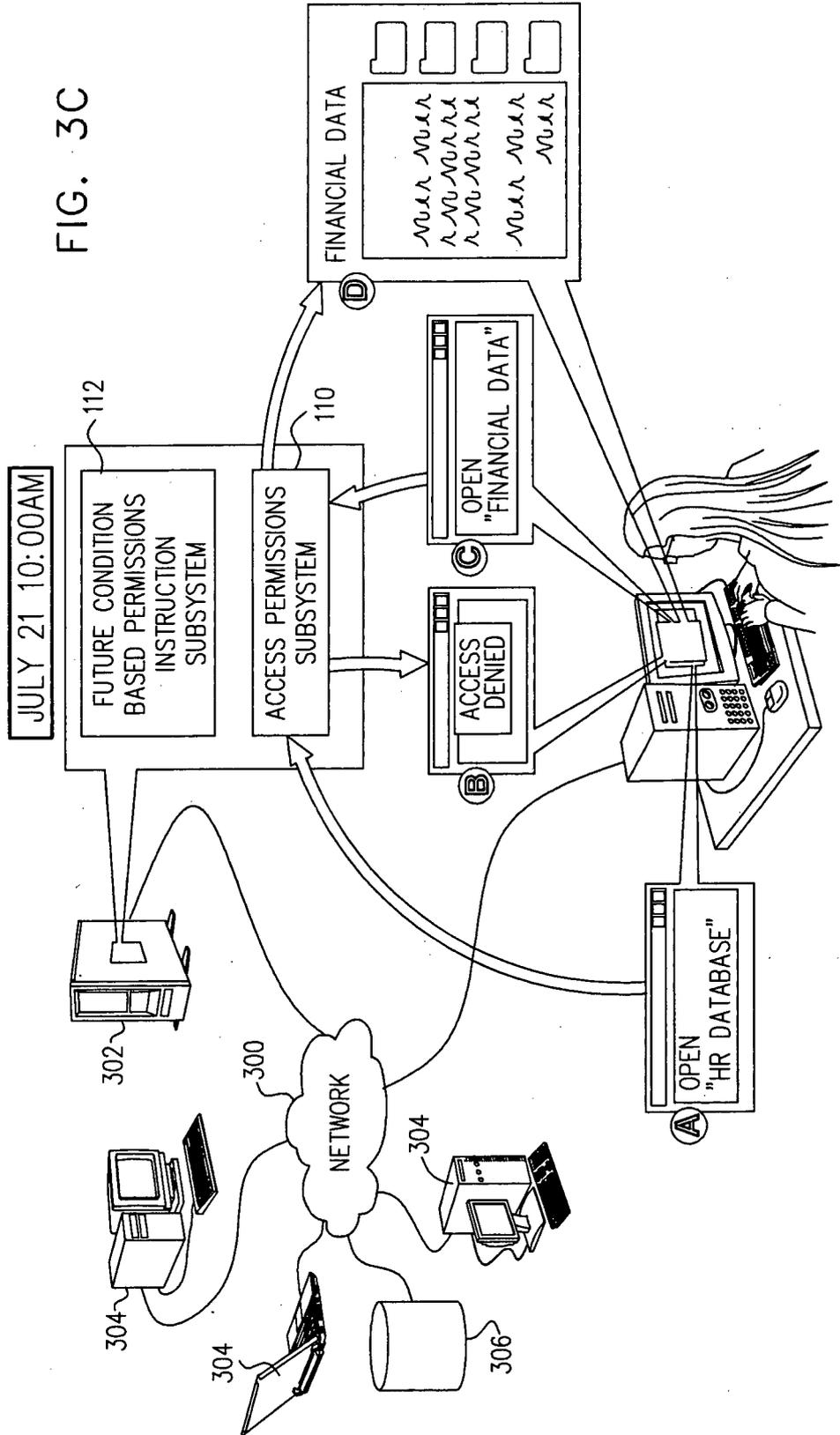
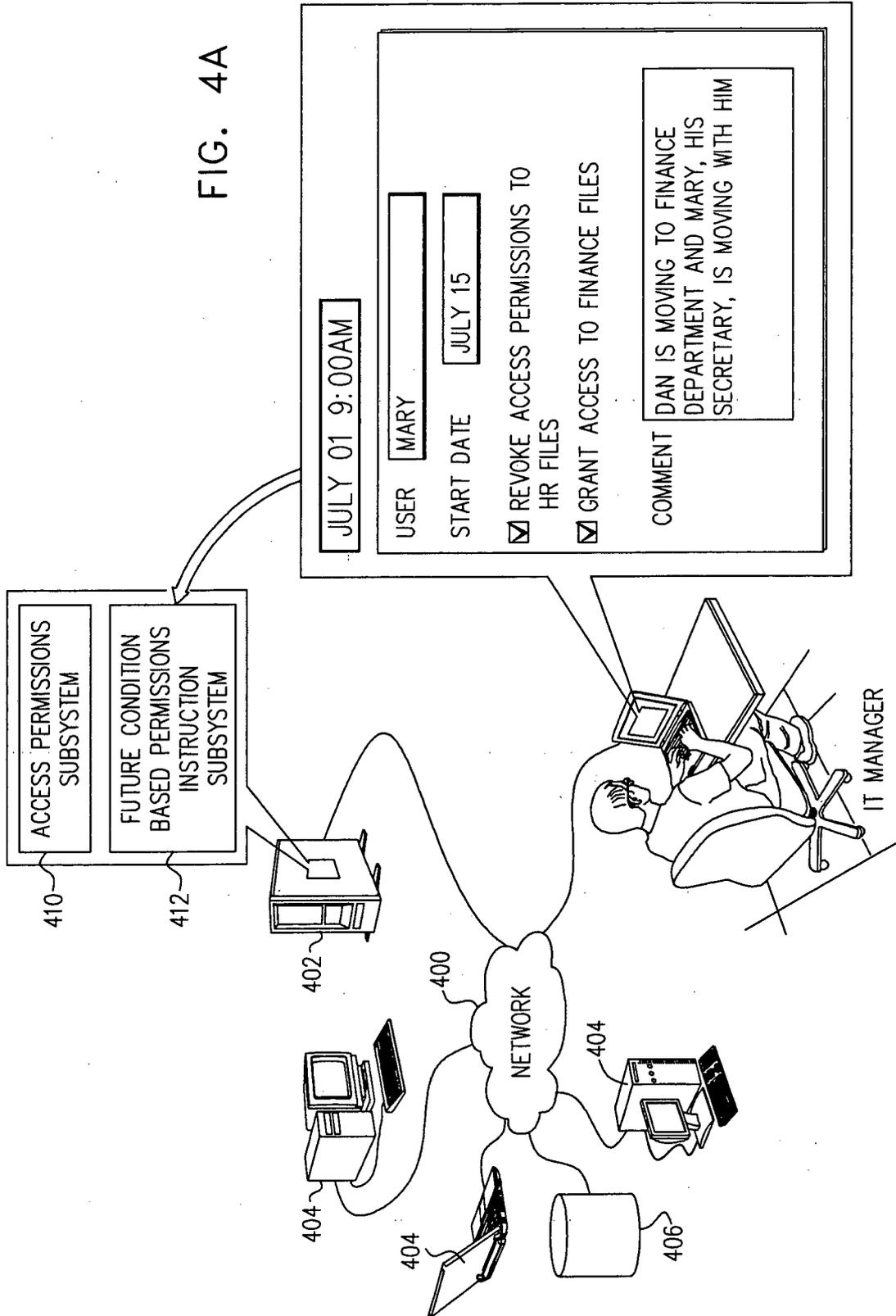


FIG. 4A



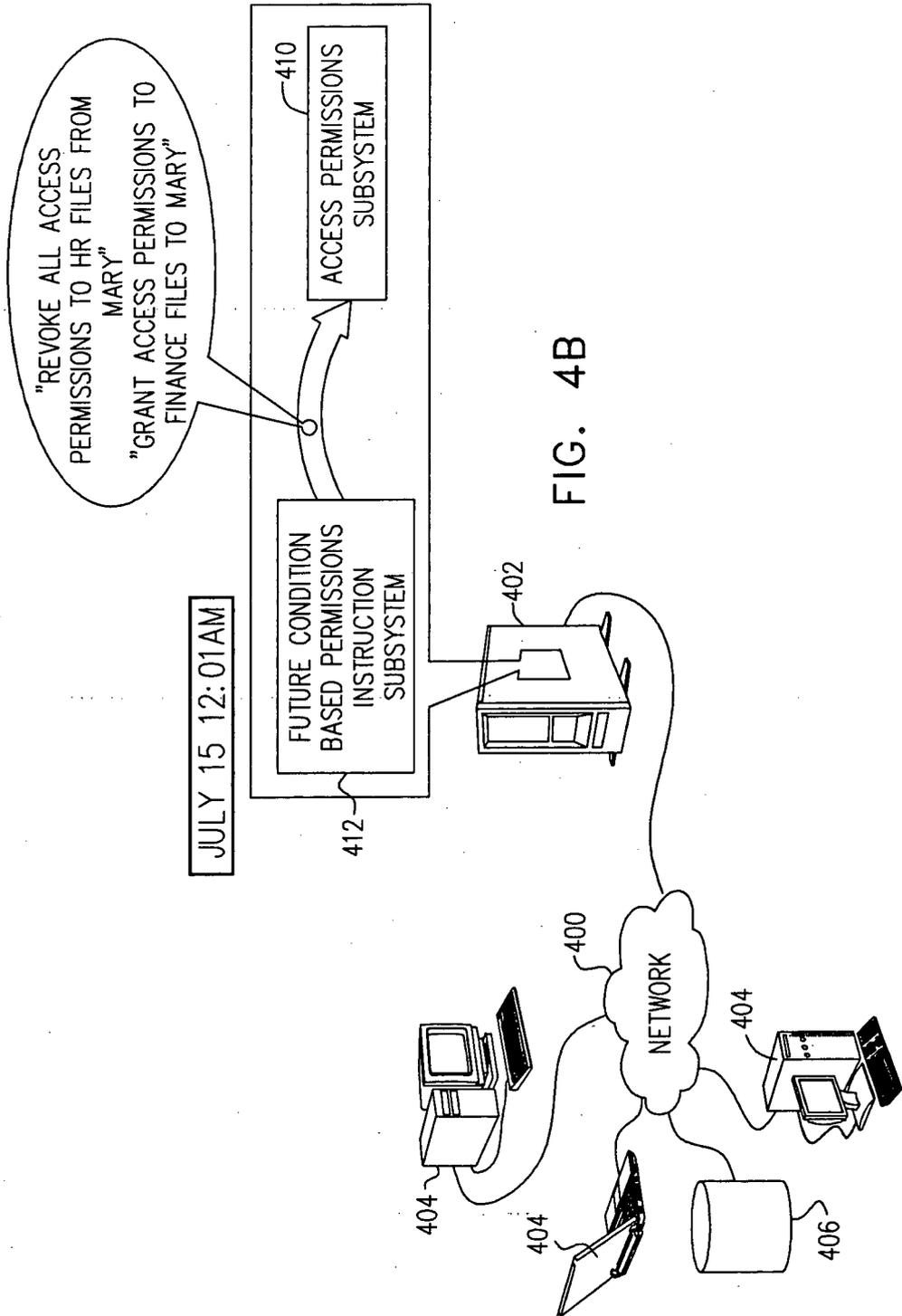


FIG. 4B

FIG. 4C

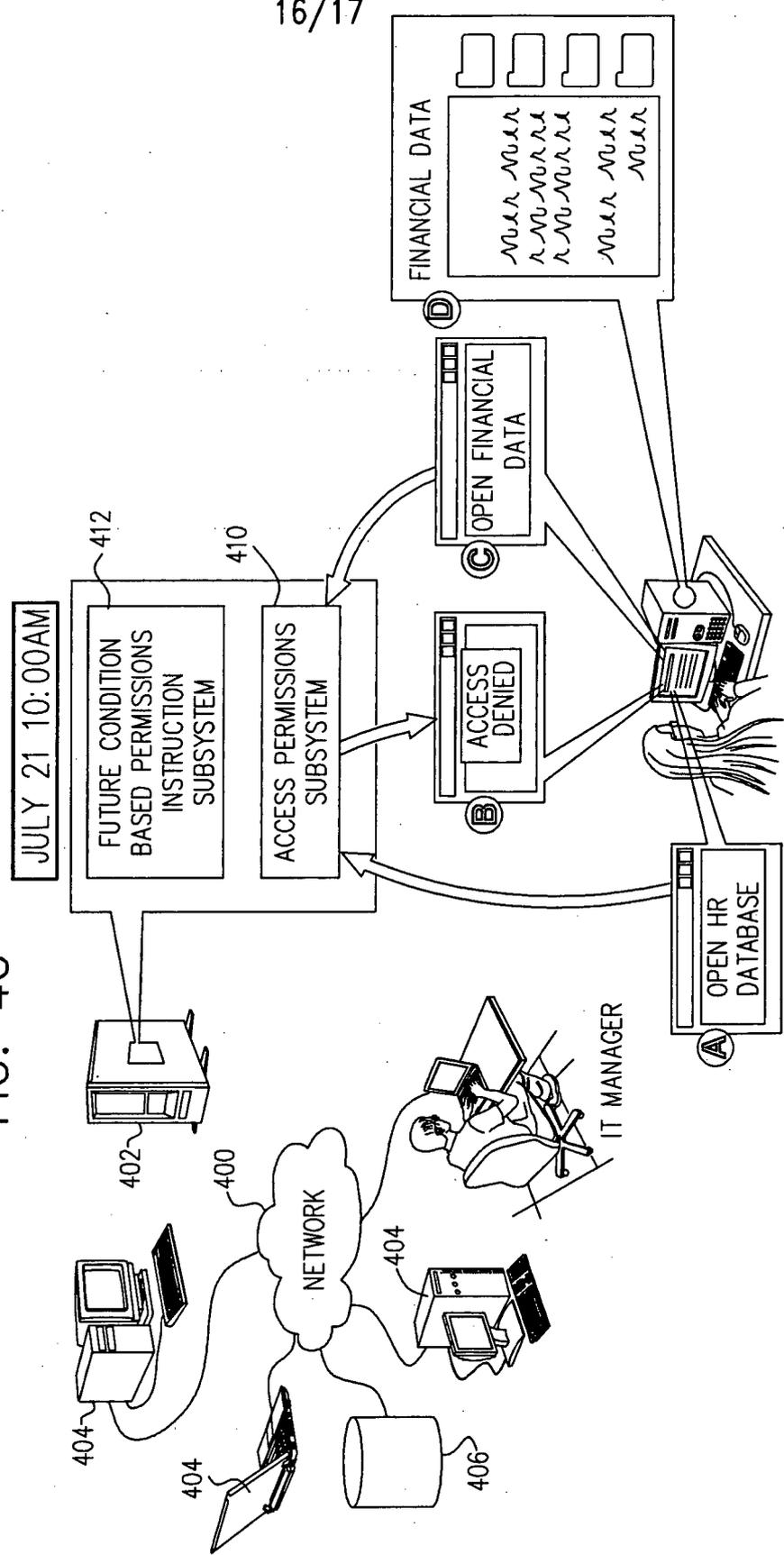


FIG. 5

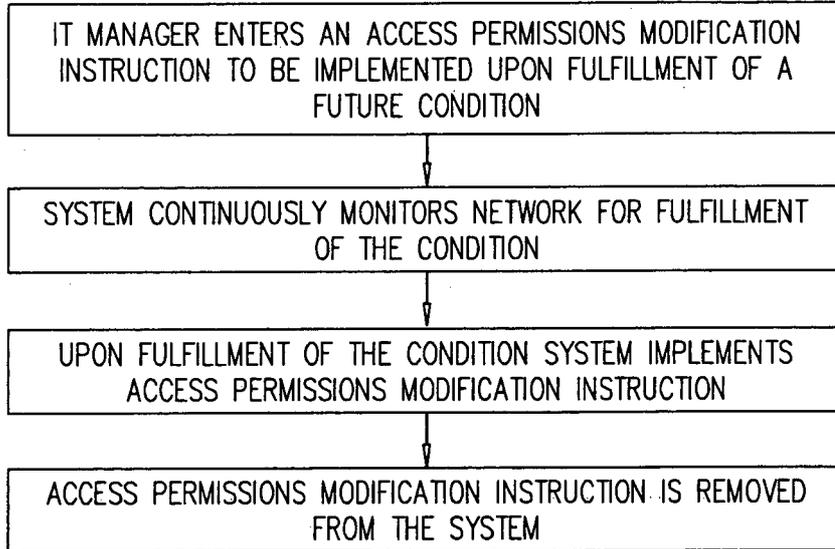
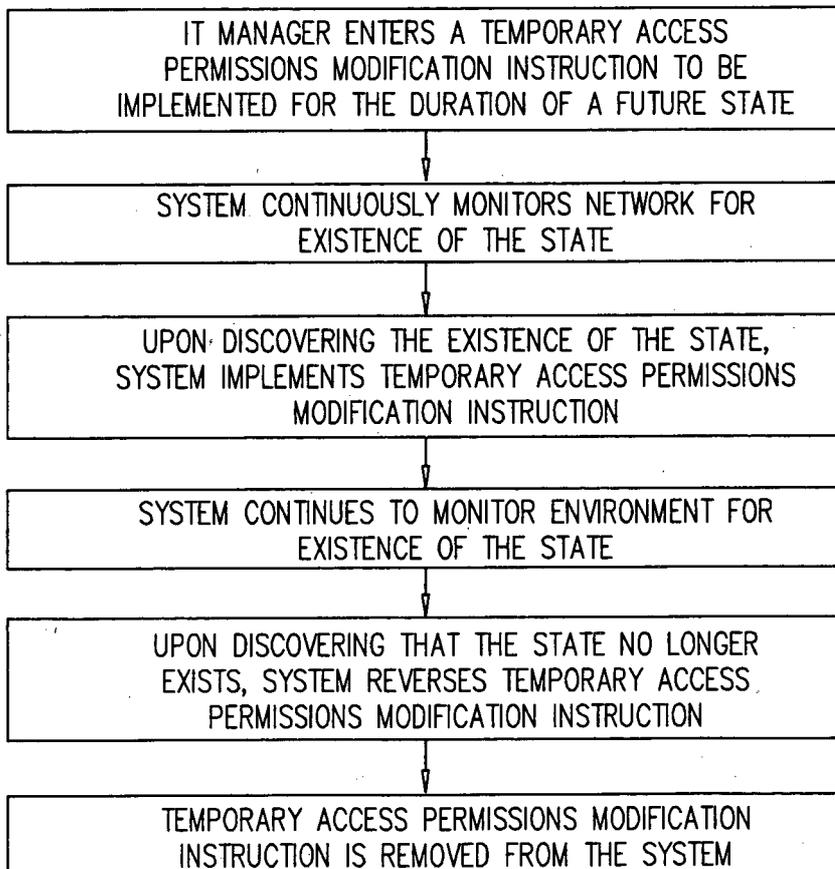


FIG. 6



INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL 11/00078

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/04 (201 1.01)
USPC - 726/6
 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)
 726/6

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
 726/6,18 1709/225 | 713/166,168

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
 PubWest(PGPB,USPT,EPAB,JPAB); Google Web; grant, revoke, suspend, access, permission, resource, file, folder, object, time, date, day, future, access control list, upcoming, forthcoming, maternity leave, leave of absence, employee, user, client, event, condition, status, manage, right, depend, limit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/0162707 A1 (Beck et al.) 03 July 2008 (03.07.2008) (entire document especially para I001 1)-[0012], [0020]-[0022], [0035H0037], [0039]-[0042])	1-20
A	US 2009/0031418 A1 (Matsuda et al.) 29 January 2009 (29.01.2009) entire document	1-20
A	US 2008/0097998 A1 (Herbach) 24 April 2008 (24.04.2008) entire document	1-20
A	US 2004/0205342 A1 (Roegner) 14 October 2004 (14.10.2004) entire document	1-20

Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 12 May 2011 (12.05.2011)	Date of mailing of the international search report 25 MAY 2011
---	--

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--