(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 October 2013 (10.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/150507 A2

(51) International Patent Classification:
G06F 7/74 (2006.01)

(21) International Application Number:
PCT/IL2012/000147

(22) International Filing Date:
4 April 2012 (04.04.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **VARONIS SYSTEMS, INC.** [US/US]; 1250 Broadway, 31st Floor, New York, New York 10001 (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 Herzeliya (IL). **BASS, David** [IL/IL]; 26 Hatamar Street, 99797 Carmei Josef (IL). **KAYSAR, Yzhar** [IL/IL]; 29 Bet El Street, 44864 Kohav Yair (IL). **KRETZER-KATZIR, Ophir** [IL/IL]; 23 Tomer Street, 71799 Re'ut (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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: ENTERPRISE LEVEL DATA ELEMENT REVIEW SYSTEMS AND METHODOLOGIES

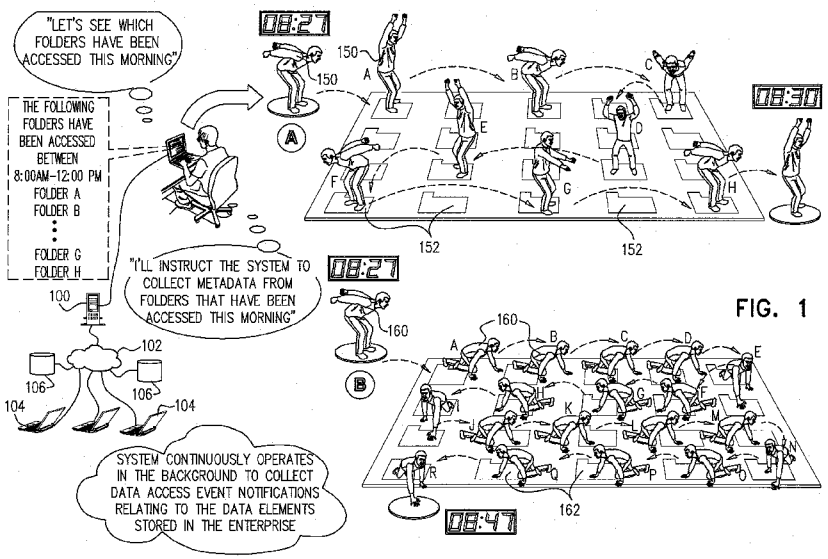

FIG. 1

(57) **Abstract**: An enterprise level data element review system including a data access event collection subsystem operative to collect data access event notifications relating to ones of a multiplicity of data elements, a data element metadata modification subassembly receiving an output from the data access event collection subsystem and providing a script indicating which data elements have had a metadata modification over a given period of time, and a data element dancer operative to collect at least one of metadata and access permissions for a plurality of data elements which is substantially less than the multiplicity of data elements and is selected on the basis of the script.

WO 2013/150507 A2

ENTERPRISE LEVEL DATA ELEMENT REVIEW SYSTEMS AND METHODOLOGIES

REFERENCE TO RELATED APPLICATIONS

Reference is 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; 2009/0265780; 2011/0010758; 2011/0060916; 2011/0061093, 2011/0061111, 2011/0184989, 2011/0296490 and 2012/0054283; and

U.S. Patent Application Serial Nos.: 13/106,023; 13/159,903; and 13/303,826.

FIELD OF THE INVENTION

The present invention relates generally to enterprise level data element review systems and methodologies.

BACKGROUND OF THE INVENTION

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

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

U.S. Published Patent Application Nos.: 2011/0060916, 2011/0061111 and 2011/0296490.

SUMMARY OF THE INVENTION

The present invention seeks to provide enterprise level data element review systems and methodologies.

There is thus provided in accordance with a preferred embodiment of the present invention an enterprise level data element review system including a data access event collection subsystem operative to collect data access event notifications relating to ones of a multiplicity of data elements, a data element metadata modification subassembly receiving an output from the data access event collection subsystem and providing a script indicating which data elements have had a metadata modification over a given period of time, and a data element dancer operative to collect at least one of metadata and access permissions for a selected plurality of data elements which is substantially less than the multiplicity of data elements and is selected on the basis of the script.

There is also provided in accordance with another preferred embodiment of the present invention an enterprise level data element review system including a data access event collection subsystem operative to collect data access event notifications relating to ones of a multiplicity of data elements, a data element modified metadata collector which is operative to collect at least one of metadata and access permissions for a plurality of data elements which is substantially less than the multiplicity of data elements, and a data element crawler operative to crawl over the multiplicity of data elements thereby to collect at least one of metadata and access permissions for the multiplicity of data elements.

There is also provided in accordance with another preferred embodiment of the present invention an enterprise level data element review system including a data access event collection failure monitoring subsystem operative to ascertain failure to collect data access events and to provide a failure notification, and a data element crawler operative in response to receipt of the failure notification to crawl over the multiplicity of data elements thereby to collect at least one of metadata and access permissions for the multiplicity of data elements.

There is also provided in accordance with another preferred embodiment of the present invention a method for enterprise level data element review including collecting data access event notifications relating to ones of a multiplicity of data elements, providing a script indicating which data elements have had a metadata modification over a given period of time, and collecting at least one of metadata and access permissions for a selected plurality of data elements which is substantially less than the multiplicity of data elements and is selected on the basis of the script.

There is also provided in accordance with another preferred embodiment of the present invention a method for enterprise level data element review including collecting data access event notifications relating to ones of a multiplicity of data elements collecting at least one of metadata and access permissions for a plurality of data elements which is substantially less than the multiplicity of data elements, and crawling over the multiplicity of data elements thereby to collect at least one of metadata and access permissions for the multiplicity of data elements.

There is also provided in accordance with another preferred embodiment of the present invention a method for enterprise level data element review including ascertaining failure to collect data access events, providing a failure notification, and in response to receipt of the failure notification, crawling over the multiplicity of data elements thereby to collect at least one of metadata and access permissions for the multiplicity of data elements.

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 drawing in which:

Fig. 1 is a simplified illustration of an enterprise level data element review system constructed and operative in accordance with a preferred embodiment of the invention;

Fig. 2 is an alternative simplified illustration of the enterprise level data element review system of Fig. 1;

Fig. 3 is a simplified block diagram illustration of the system and methodology of Fig. 1;

Fig. 4 is a simplified block diagram illustration of the operation of the system of Fig. 1; and

Fig. 5 is a simplified block diagram illustration of another aspect of the use of the system of Fig. 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1, which is a simplified illustration of an enterprise level data element review system constructed and operative in accordance with a preferred embodiment of the invention. The system of Fig. 1 is preferably suitable for operating in an enterprise computer network which includes, inter alia, multiple disparate servers and clients storing data elements such as files and folders.

The system of Fig. 1 preferably includes a data access event collection subsystem operative to collect data access event notifications relating to ones of a multiplicity of data elements, a data element metadata modification subassembly receiving an output from the data access event collection subsystem and providing a script indicating which data elements have had a metadata modification over a given period of time, and a data element dancer operative to collect at least one of metadata and access permissions for a selected plurality of data elements which is substantially less than the multiplicity of data elements and is selected on the basis of the script.

As shown in Fig. 1, the system resides on a server 100 which is connected to a computer network 102 to which are connected a plurality of computer servers 104 and storage devices 106, and preferably continuously operates in the background to collect data access event notifications relating to the multiplicity of data elements stored on servers 104 and storage devices 106.

As further shown in Fig. 1, an administrator of the system wishes to utilize the system to collect metadata of folders that were modified during a particular period of time, such as between 8AM – 12PM on January 5, 2012. Responsive to a request from the administrator, the system provides the administrator with a script 120 which comprises a list of folders which have been accessed during the period of interest. Thereafter, the administrator instructs the system to collect metadata of the folders which appear in the script.

It is a particular feature of the present invention that continuous collection of data access event notifications by the system is operative to enable efficient maintaining of a generally up-to-date collection of metadata of all data elements by periodically selectively collecting metadata only of data elements which are

known to have been accessed during a particular period of time. It is appreciated that the time and computer resources needed to periodically selectively collect metadata only from data elements which are known to have been accessed during a particular period of time is substantially less than the time needed to collect metadata from all data elements.

This particular feature is further illustrated in Fig. 1. As shown in option A, a data element dancer 150 begins to dance through a plurality of data elements 152 at 8:27 AM. As clearly shown in the illustration of option A, as dancer 150 dances through data elements 152, he lands on only a subset of data elements 152 which correspond to data elements listed in script 120, and completes dancing over data elements 152 at 8:30 AM.

Contrarily, as illustrated in option B, a data element crawler 160 begins to crawl through a plurality of data elements 162 at 8:27 AM., however, as crawler 160 crawls through data elements 162, he lands on every one of data elements 162, thereby completing to crawl over data elements 162 at 8:47 AM., significantly later than data element dancer 150.

It is appreciated that the system also comprises a data access event collection failure monitoring subsystem operative to ascertain failure to collect data access events and to provide a corresponding failure notification to a data element crawler which is operative in response to receipt of the failure notification to crawl over the multiplicity of data elements stored on servers 104 and storage devices 106 and to thereby collect at least one of metadata and access permissions for the multiplicity of data elements.

Reference is now made to Fig. 2, which is an alternative simplified illustration of the enterprise level data element review system of Fig. 1. Fig. 2 further illustrates the particular feature of the present invention, whereby initially ascertaining which particular elements of a group need to be treated and thereafter selectively treating only those particular elements is substantially more efficient than treating all the elements of the group.

As shown in option A of Fig. 2, a first pesticide applicator 200 begins to walk through the rows of a planted field 202 at 6:00 AM. As clearly shown in the illustration of option A, as pesticide applicator 200 walks through field 202, he applies

pesticide only to plants which have been identified as being infested, and completes walking through the entire filed at 6:30 AM.

Contrarily, as illustrated in option B, a second pesticide applicator 210 begins to walk through the rows of a planted field 212 at 6:00 AM., however as second pesticide applicator 210 walks through field 212 he applies pesticide to every one of the plants of field 212 regardless of whether they are infested or not, thereby completing to walk through the field at 7:15 AM, significantly later than first pesticide applicator 200.

Reference is now made to Fig. 3, which is a simplified block diagram illustration of the system of Fig. 1, to Fig. 4, which is a simplified block diagram illustration of the operation of the system of Fig. 1, and to Fig. 5, which is a simplified block diagram illustration of another aspect of the use of the system of Fig. 1.

As shown in Fig. 3, the enterprise level data element review system 300 comprises a data access event collection subsystem 302 operative to collect data access event notifications relating to ones of a multiplicity of data elements and to communicate with a data element metadata modification subassembly 304. Data element metadata modification subassembly 304 preferably communicates with a data element dancer 306.

System 300 also includes a data access event collection failure monitoring subsystem 310 operative to ascertain failure of data access event collection subsystem 302 to collect data access events and to provide a corresponding failure notification to a data element crawler 312 which is operative in response to receipt of the failure notification to crawl over the multiplicity of data elements stored in the enterprise and to thereby collect at least one of metadata and access permissions for the multiplicity of data elements.

As shown in Fig. 4, data access event collection subsystem 302 continuously collects data access event notifications relating to ones of a multiplicity of data elements and sends an output to data element metadata modification subassembly 304. Data element metadata modification subassembly 304 preferably provides a script indicating which data elements have had a metadata modification over a given period of time to data element dancer 306 which then collects at least one of metadata and access permissions only for the data elements included in the script.

As shown in Fig. 5, data access event collection failure monitoring subsystem 310 ascertains failure to collect data access events and provides a failure notification. Responsive to the failure notification, data element crawler 312 preferably crawls over the multiplicity of data elements thereby to collect at least one of metadata and access permissions for the multiplicity of data elements.

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.

CLAIMS

1. An enterprise level data element review system comprising:

a data access event collection subsystem operative to collect data access event notifications relating to ones of a multiplicity of data elements;

a data element metadata modification subassembly receiving an output from said data access event collection subsystem and providing a script indicating which data elements have had a metadata modification over a given period of time; and

a data element dancer operative to collect at least one of metadata and access permissions for a selected plurality of data elements which is substantially less than said multiplicity of data elements and is selected on the basis of said script.

2. An enterprise level data element review system comprising:

a data access event collection subsystem operative to collect data access event notifications relating to ones of a multiplicity of data elements;

a data element modified metadata collector which is operative to collect at least one of metadata and access permissions for a plurality of data elements which is substantially less than said multiplicity of data elements; and

a data element crawler operative to crawl over said multiplicity of data elements thereby to collect at least one of metadata and access permissions for said multiplicity of data elements.

3. An enterprise level data element review system comprising:

a data access event collection failure monitoring subsystem operative to ascertain failure to collect data access events and to provide a failure notification; and

a data element crawler operative in response to receipt of said failure notification to crawl over said multiplicity of data elements thereby to collect at least one of metadata and access permissions for said multiplicity of data elements.

4. A method for enterprise level data element review comprising:

collecting data access event notifications relating to ones of a multiplicity of data elements;

providing a script indicating which data elements have had a metadata modification over a given period of time; and

collecting at least one of metadata and access permissions for a selected plurality of data elements which is substantially less than said multiplicity of data elements and is selected on the basis of said script.

5. A method for enterprise level data element review comprising:

collecting data access event notifications relating to ones of a multiplicity of data elements;

collecting at least one of metadata and access permissions for a plurality of data elements which is substantially less than said multiplicity of data elements; and

crawling over said multiplicity of data elements thereby to collect at least one of metadata and access permissions for said multiplicity of data elements.

6. A method for enterprise level data element review comprising:

ascertaining failure to collect data access events;

providing a failure notification; and

in response to receipt of said failure notification, crawling over said multiplicity of data elements thereby to collect at least one of metadata and access permissions for said multiplicity of data elements.

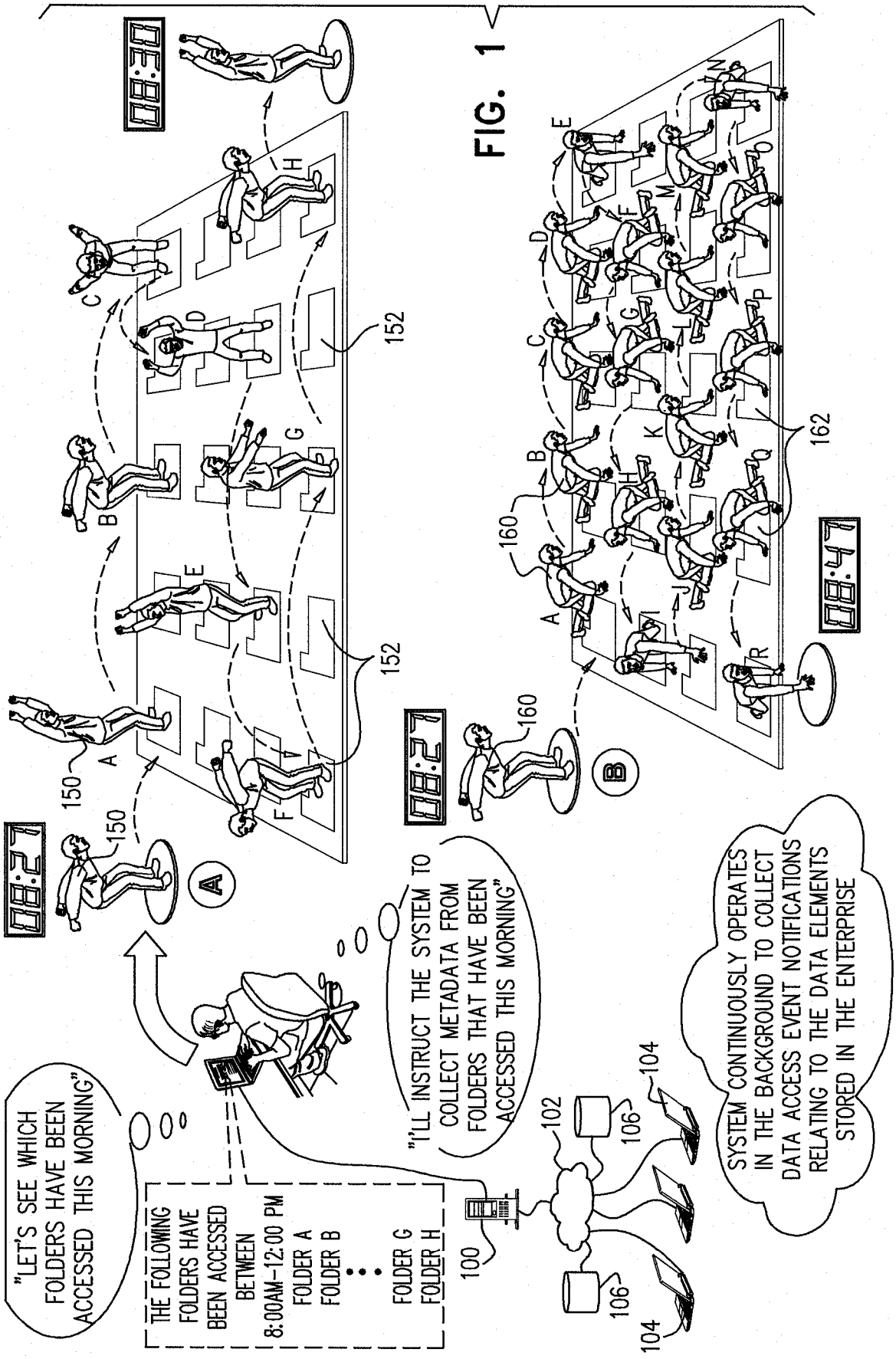
"LET'S SEE WHICH FOLDERS HAVE BEEN ACCESSED THIS MORNING"
THE FOLLOWING FOLDERS HAVE BEEN ACCESSED BETWEEN 8:00AM-12:00 PM
FOLDER A
FOLDER B
FOLDER G
FOLDER H
"I'LL INSTRUCT THE SYSTEM TO COLLECT METADATA FROM FOLDERS THAT HAVE BEEN ACCESSED THIS MORNING"
SYSTEM CONTINUOUSLY OPERATES IN THE BACKGROUND TO COLLECT DATA ACCESS EVENT NOTIFICATIONS RELATING TO THE DATA ELEMENTS STORED IN THE ENTERPRISE
08:27
08:30
08:27
08:47
150
152
160
162
100
102
104
106
A
B

FIG. 1

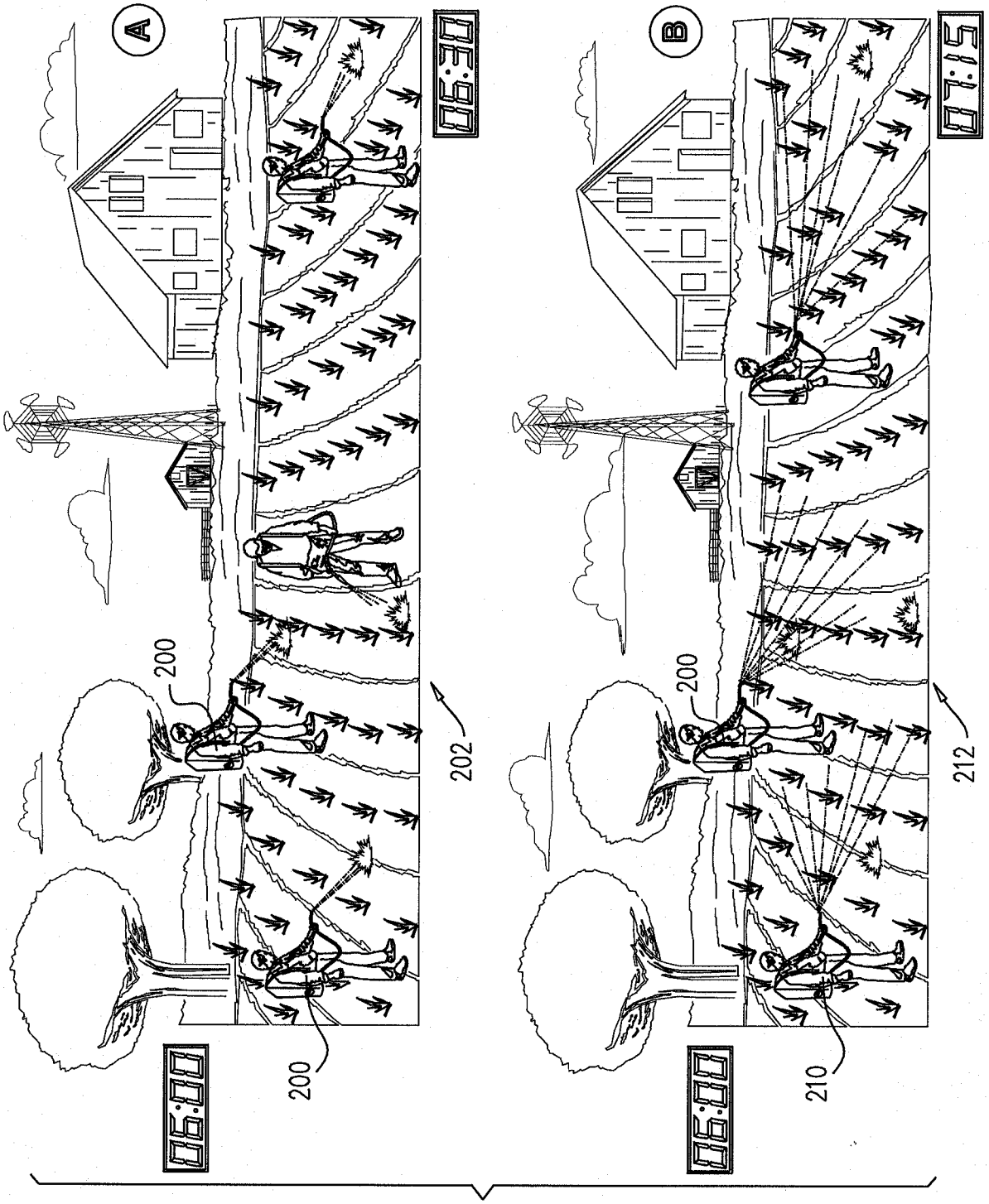

FIG. 2

FIG. 3

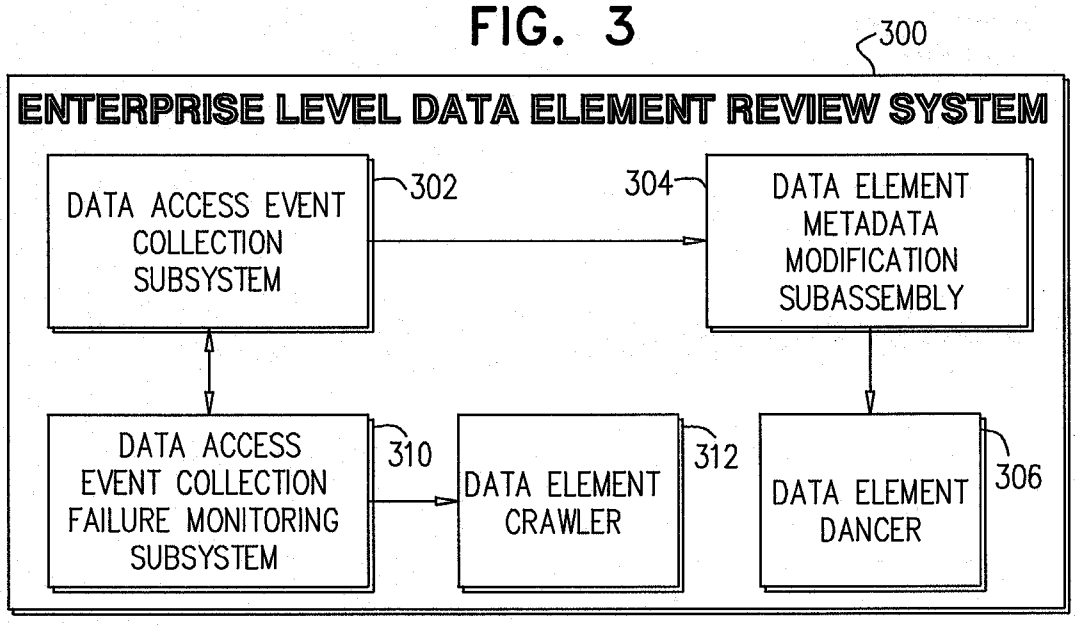

FIG. 4

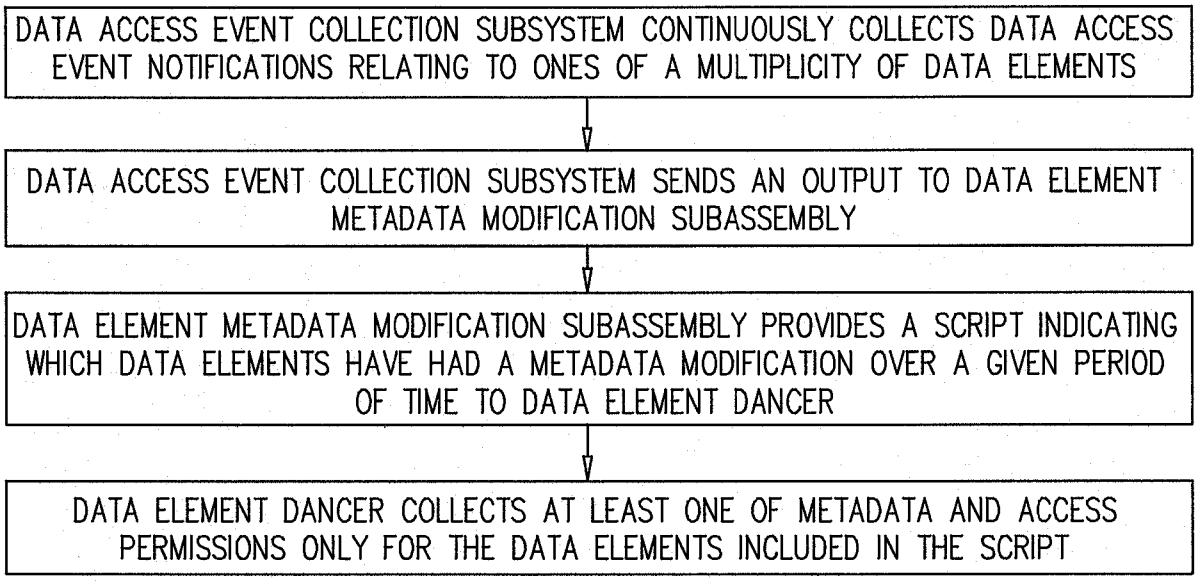

FIG. 5