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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
31 July 2008 (31.07.2008)

PCT

(10) **International Publication Number**
WO 2008/090014 A3

(51) **International Patent Classification:**
G06F 21/24 (2006.01) ***G06F 17/30*** (2006.01)

(21) **International Application Number:** PCT/EP2008/050115

(22) **International Filing Date:** 8 January 2008 (08.01.2008)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
11/626,847 25 January 2007 (25.01.2007) US

(71) **Applicant** *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(71) **Applicant** *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB).

(72) **Inventors; and**

(75) **Inventors/Applicants** *(for US only)*: **PERNG, Chang-Shing** [CN/US]; 22 Green Hill Road, Goldens Bridge, New York 10526 (US). **WANG, Haixun** [CN/US]; 42 Victor Drive, Irvington, New York 10533 (US). **YIN, Jian** [US/US]; 1925 Eastchester Road, Apt #14B, Bronx, New York 10461 (US). **YU, Philip** [US/US]; 18 Stornowaye, Chappaqua, New York 10514 (US).

(74) **Agent: WILLIAMS, Julian, David**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) **Title:** QUERY INTEGRITY ASSURANCE IN DATABASE OUTSOURCING

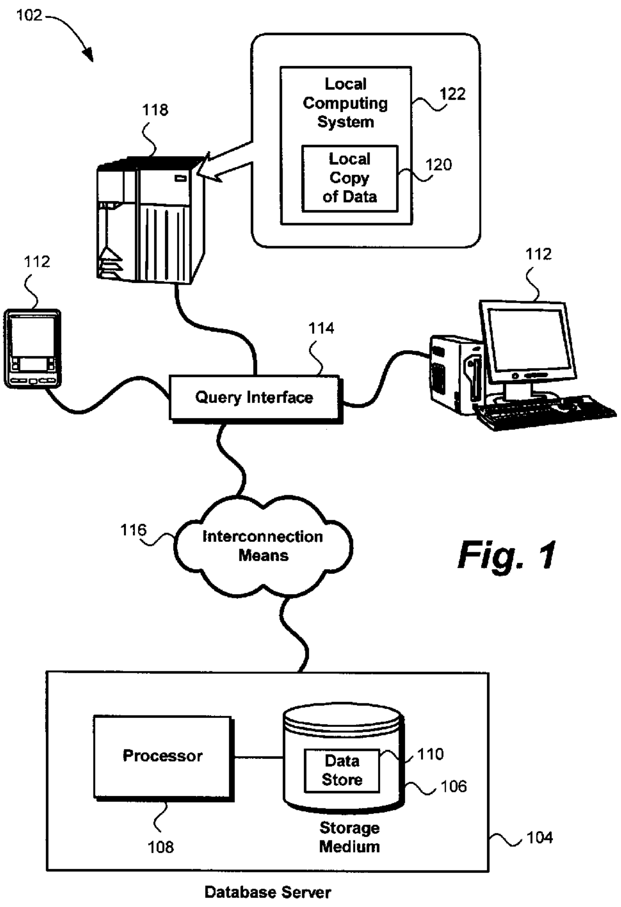

Fig. 1

(57) **Abstract:** A method, system and computer program product for confirming the validity of data returned from a data store. A data store contains a primary data set encrypted using a first encryption and a secondary data set using a second encryption. The secondary data set is a subset of the primary data set. A client issues a substantive query against the data store to retrieve a primary data result belonging to the primary data set. A query interface issues at least one validating query against the data store. Each validating query returns a secondary data result belonging to the secondary data set. The query interface receives the secondary data result and provides a data invalid notification if data satisfying the substantive query included in an unencrypted form of the secondary data result is not contained in an unencrypted form of the primary data result.

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

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) **Date of publication of the international search report:** 2 October 2008

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/050115

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/24 G06F17/30

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

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

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

EPO-Internal, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DAMIANI ERNESTO ET AL: "Balancing confidentiality and efficiency in untrusted relational DBMSs" PROC ACM CONF COMPUTER COMMUN SECUR; PROCEEDINGS OF THE ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY; PROCEEDINGS OF THE 10TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, CCS 2003 2003, [Online] 2003, pages 93-102, XP002491419 Retrieved from the Internet: URL:http://doi.acm.org/10.1145/948109.948124> paragraphs [0001], [0002] ----- -/--	1-20

☒ 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 document 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 7 August 2008	Date of mailing of the international search report 22/08/2008
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Mäenpää, Jari

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	HAKAN HACIGÜMÜS ET AL: "Executing SQL over Encrypted Data in the Database-Service-Provider Model" SIGMOD 2002. PROCEEDINGS OF THE ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT OF DATA. MADISON, WI, JUNE 4 - 6, 2002; [PROCEEDINGS OF THE ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT OF DATA], NEW YORK, NY : ACM, US, 1 June 2002 (2002-06-01), pages 216-227, XP002306244 ISBN: 978-1-58113-497-1 the whole document -----	1-20
Y	GEROME MIKLAU ET AL: "Implementing a Tamper-Evident Database System" ADVANCES IN COMPUTER SCIENCE - ASIAN 2005 LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER-VERLAG, BE, vol. 3818, 1 January 2005 (2005-01-01), pages 28-48, XP019025768 ISBN: 978-3-540-30767-9 page 31, line 19 - line 30 -----	1-20
A	HWEEHWA PANG ET AL: "Verifying Completeness of Relational Query Results in Data Publishing" SIGMOD 2005. PROCEEDINGS OF THE ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT DATA. BALTIMORE, MD, JUNE 14 - 16, 2005; [PROCEEDINGS OF THE ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT OF DATA], NEW YORK, NY : ACM, US, 14 June 2005 (2005-06-14), pages 407-418, XP002479510 ISBN: 978-1-59593-060-6 the whole document -----	1-20