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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083267 A3

(51) International Patent Classification:
*G06F 12/00* (2006.01)

(21) International Application Number:
PCT/US2007/089027

(22) International Filing Date:
28 December 2007 (28.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/882,289 28 December 2006 (28.12.2006) US

(71) Applicant *(for all designated States except US)*: **ARCSIGHT, INC.** [US/US]; 5 Results Way, Cupertino, CA 95014 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HUANG, Wei** [US/US]; c/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US). **TANG, Wenting** [CN/US]; c/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US). **BEEDGEN, Christian, F.** [DE/US]; c/o ArcSight, Inc., 5 Results Way, Cupertino, CA 95014 (US).

(74) Agents: **TRUESDALE, Sabra-Anne** et al.; Fenwick & West LLP, Silicon Valley Center, 801 California Street, Mountain View, CA 94041 (US).

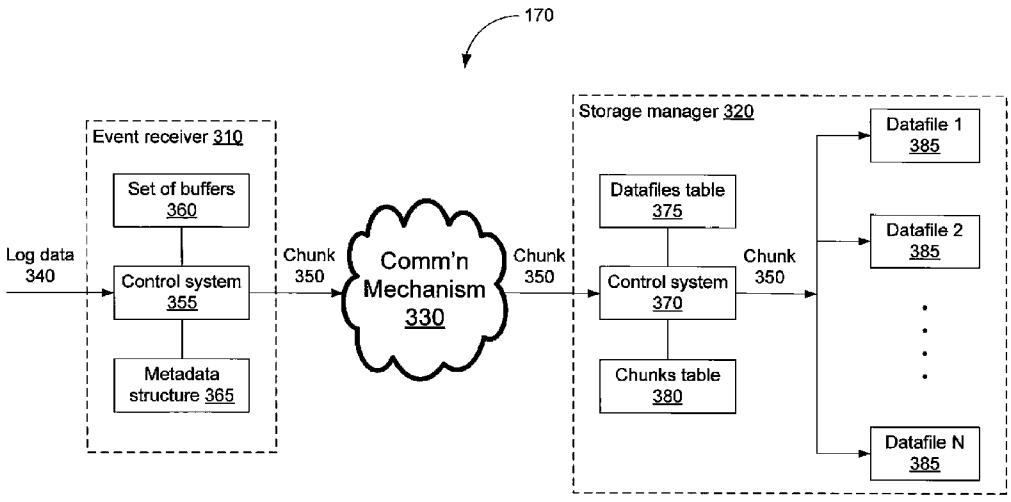
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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.

(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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, 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:
28 August 2008

(54) Title: STORING LOG DATA EFFICIENTLY WHILE SUPPORTING QUERYING TO ASSIST IN COMPUTER NETWORK SECURITY




(57) Abstract: A logging system includes an event receiver and a storage manager. The receiver receives log data, processes it, and outputs a data "chunk." The manager receives data chunks and stores them so that they can be queried. The receiver includes buffers that store events and a metadata structure that stores metadata about the contents of the buffers. The metadata includes a unique identifier associated with the receiver, the number of events in the buffers, and, for each "field of interest," a minimum value and a maximum value that reflect the range of values of that field over all of the events in the buffers. A chunk includes the metadata structure and a compressed version of the contents of the buffers. The metadata structure acts as a search index when querying event data. The logging system can be used in conjunction with a security information/event management (SIEM) system.

WO 2008/083267 A3