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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 January 2017 (26.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/014823 A3

(51) International Patent Classification:
G06F 11/00 (2006.01)

(21) International Application Number:
PCT/US2016/030660

(22) International Filing Date:
4 May 2016 (04.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/156,884	4 May 2015 (04.05.2015)	US
62/198,091	28 July 2015 (28.07.2015)	US
62/206,675	18 August 2015 (18.08.2015)	US
62/210,546	27 August 2015 (27.08.2015)	US
62/220,914	18 September 2015 (18.09.2015)	US
62/286,437	24 January 2016 (24.01.2016)	US
62/294,258	11 February 2016 (11.02.2016)	US
62/307,558	13 March 2016 (13.03.2016)	US
62/323,657	16 April 2016 (16.04.2016)	US
15/145,800	4 May 2016 (04.05.2016)	US

(72) Inventor; and
(71) Applicant : **HASAN, Syed Kamran** [US/US]; 622 River Bend Road, Great Falls, VA 22066 (US).

(74) Agent: **PARK, Chanmin**; Law Offices of Lee & Park, 8383 Wilshire Blvd. Ste 510, Beverly Hills, CA 90211 (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,

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR MANAGING SECURITY IN A COMPUTER NETWORK

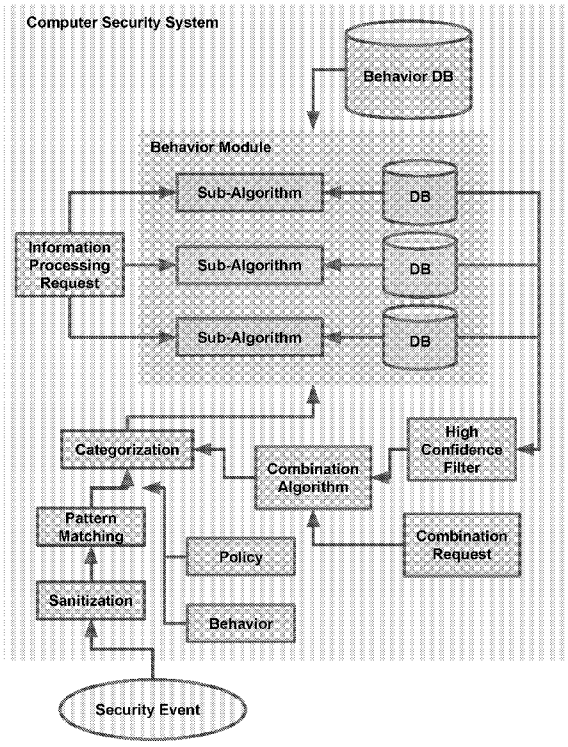

FIG. 79

(57) Abstract: Method and device for managing security in a computer network include algorithms of iterative intelligence growth, iterative evolution, and evolution pathways; sub-algorithms of information type identifier, conspiracy detection, media scanner, privilege isolation analysis, user risk management and foreign entities management; and modules of security behavior, creativity, artificial threat, automated growth guidance, response/generic parser, security review module and monitoring interaction system. Applications include malware predictive tracking, clandestine machine intelligence retribution through covert operations in cyberspace, logically inferred zero-database a-priori realtime defense, critical infrastructure protection & retribution through cloud & tiered information security, and critical thinking memory & perception.

WO 2017/014823 A3

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).

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))*

(88) Date of publication of the international search report:
20 April 2017

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 16/30660

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 11/00 (2016.01)
CPC - G06F 21/577; H04L 63/1433; H04L 63/1416
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)
CPC: G06F 21/577; H04L 63/1433; H04L 63/1416; IPC(8): G06F 11/00 (2016.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/25; 726/22; 726/1; 713/189; CPC: G06F 21/577; H04L 63/1433; H04L 63/1416; H04L 63/20, H04L 63/1408; IPC(8): G06F 11/00 (2016.01) (keyword limited, terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, IEEE; Search Terms: security analysis; cyber threat; cyber security; artificial intelligence, AI; expert system; behavior; pattern; category; conspiracy; detecting, finding, revealing; intelligence, intelligent; personality trait; evolution pathway; selector; parent form; merge

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- A	US 2008/0133518 A1 (Kapoor et al.) 05 June 2008 (05.06.2008), entire document especially paras [0076], [0137], [0140], [0156], [0174], [0203]	1-10 ----- 11-69
Y ----- A	US 2014/0208439 A1 (Sasaki) 24 July 2014 (24.07.2014), entire document especially paras [0057], [0063], [0069], [0070], [0172], [0186]	11-46 1-10 and 47-69
Y ----- A	US 2010/0287608 A1 (Khuti et al.) 11 November 2010 (11.11.2010), entire document especially Abstract, paras [0012], [0015], [0058], [0067]	11-46 ----- 1-10 and 47-69
A	US 2012/0136840 A1 (Oaten et al.) 31 May 2012 (31.05.2012), entire document	47-52
A	US 2010/0036783 A1 (Rodriguez) 11 February 2010 (11.02.2010), entire document	53-69
A	US 2003/0084322 A1 (Schertz et al.) 01 May 2003 (01.05.2003), entire document	1-69
A	US 2004/0025044 A1 (Day) 05 February 2004 (05.02.2004), entire document	1-69
A	US 2010/0257580 A1 (Zhao) 07 October 2010 (07.10.2010), entire document	1-69

☐ 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
"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	Date of mailing of the international search report
03 February 2017 (03.02.2017)	17 FEB 2017
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. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 16/30660

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1.

Group I: Claims 1-10, directed to a system for providing a security analysis based on the output of the behavior module.

Group II: Claims 11-46, directed to a system for determining patterns and correlations between the security events and declaring confidence in a data type.

Group III: Claims 47-52, directed to a method for iterative intelligence growth involving evolution pathways evolving in a plurality of generations according to a given personality trait in a security environment.

Group IV: Claims 53-69, directed to a system for cyber threat intelligence identification, integration and analysis involving merging parent intelligence based on an intelligent selector in a security environment.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.