



- (51) International Patent Classification:
G06F 21/50 (2013.01) *G06F 21/55* (2013.01)
- (21) International Application Number:
PCT/SG2016/050515
- (22) International Filing Date:
24 October 2016 (24.10.2016)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant: **CERTIS CISCO SECURITY PTE LTD**
[SG/SG]; 20 Jalan Afifi, Certis Cisco Centre, Singapore
409179 (SG).
- (72) Inventor: **LIM, Keng Leng Albert**; c/o Certis Cisco Security Pte Ltd, 20 Jalan Afifi, Certis Cisco Centre, Singapore
409179 (SG).

- (74) Agent: **ALLEN & GLEDHILL LLP**; One Marina Boulevard #28-00, Singapore 018989 (SG).

- (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, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, 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, KW, 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, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

- (54) Title: QUANTITATIVE UNIFIED ANALYTIC NEURAL NETWORKS

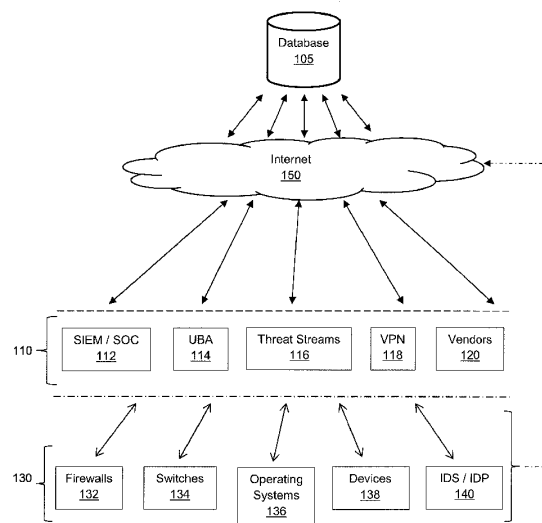


FIGURE 1

- (57) Abstract: A method for quantitative unified analysis of unstructured threat intelligence data, the method to be performed by a computer system comprising: receiving unstructured threat intelligence data from molecular level sources, wherein the unstructured threat intelligence data comprises security events generated from the molecular level sources; uniting the received unstructured threat intelligence data by translating the received threat intelligence data into a uniformed meta-format and storing the translated data in a database, wherein each translated data includes at least a time component; determining isolated data points from the translated data stored in the database by grouping the translated data into groups, wherein each group represents a unique time period, and applying unsupervised machine learning techniques to each group of the translated data; determining data outliers from the isolated data points; and generating a learned function using the data outliers.

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))