



(51) International Patent Classification:

G06F 21/56 (2013.01) G06F 21/54 (2013.01)
G06F 21/55 (2013.01)

(21) International Application Number:

PCT/IB2023/060256

(22) International Filing Date:

11 October 2023 (11.10.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/415,852 13 October 2022 (13.10.2022) US

(71) Applicant: CYBERSENTRY.AI, INC. [US/US]; PO Box 3153, Rancho Santa Fe., CA 92067 (US).

(72) Inventors: LEWAK, Stanislaw Maria Aleksander; 378 Northlake Blvd, #166, North Palm Beach, Florida 33408 (US). SIEREK, Wacław Tomasz; ul. Górská 67, 32-082 Bolechowice (PL). BEEBY, Ian Philip; Aughclare, New Ross, Co. Wexford, Y34 KX68 (IE).

(74) Agent: SLOTNICK, Heather et al.; MLO, 888 Prospect Street, Suite 200, La Jolla, California 92037 (US).

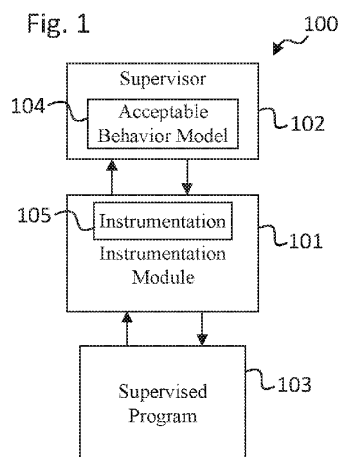
(81) Designated States (unless otherwise indicated, for every kind of national protection available):

AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available):

ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, 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, ME, 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).

(54) Title: PROGRAM EXECUTION ANOMALY DETECTION FOR CYBERSECURITY



(57) Abstract: A program is executed in a first mode of operation in a controlled environment in accordance with normal operations without malicious behavior. An acceptable behavior model is generated based on a plurality of sequences of events that occur during the normal operation of the program. The acceptable behavior model is indicative of normal behavior of the program that occurs during the normal operation. Then the program is executed in a second mode of operation in an operational environment. An operational sequence of events (determined during the second mode of operation) is compared with the acceptable behavior model. When there is a match between the operational sequence of events and the acceptable behavior model, execution in the second mode of operation continues. When there is not a match between the operational sequence of events and the acceptable behavior model, execution in the second mode of operation is halted.

Published:

- *with international search report (Art. 21(3))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*