



- (51) **International Patent Classification:**
G06F 9/00 (2006.01)
- (21) **International Application Number:**
PCT/IB2021/050346
- (22) **International Filing Date:**
18 January 2021 (18.01.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
16/750,328 23 January 2020 (23.01.2020) US
- (71) **Applicant:** **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York, 10504 (US).
- (71) **Applicants (for MG only):** **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB). **IBM (CHINA) INVESTMENT COMPANY LIMITED** [CN/CN]; 25/F, Pangu Plaza, No. 27, Cental North 4th Ring Road, Chaoyang District, Beijing 100101 (CN).
- (72) **Inventors:** **GU, Zhongshu**; IBM Corporation, PO Box 218, 1101 Kitchawan Road, Yorktown Heights, New York, 10598 (US). **SHU, Xiaokui**; IBM Corporation, PO Box

218, 1101 Kitchawan Road, Yorktown Heights, New York, 10598 (US). **JAMJOOM, Hani**; IBM Corporation, PO Box 218, 1101 Kitchawan Road, Yorktown Heights, New York, 10598 (US). **MA, Tengfei**; IBM Corporation, 1101 Kitchawan Road, Yorktown Heights, New York, 10598 (US).

(74) **Agent:** **GRAHAM, Timothy**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Hursley, 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, BN, BR, BW, 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, IT, JO, JP, KE, KG, KH, 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, 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, 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:** NEURAL FLOW ATTESTATION

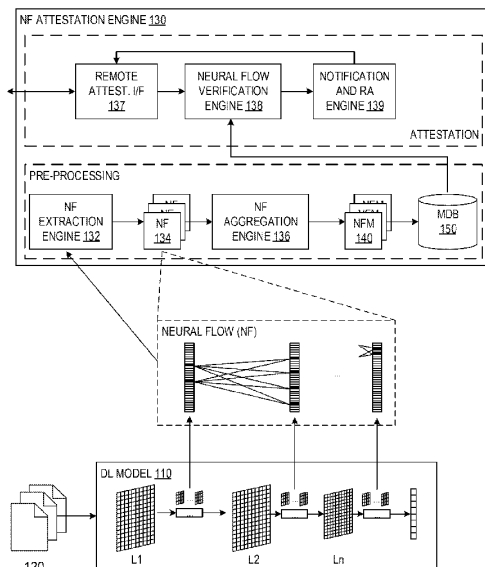


FIG. 1

(57) **Abstract:** Mechanisms are provided to implement a neural flow attestation engine and perform computer model execution integrity verification based on neural flows. Input data is input to a trained computer model that includes a plurality of layers of neurons. The neural flow attestation engine records, for a set of input data instances in the input data, an output class generated by the trained computer model and a neural flow through the plurality of layers of neurons to thereby generate recorded neural flows. The trained computer model is deployed to a computing platform, and the neural flow attestation engine verifies the execution integrity of the deployed trained computer model based on a runtime neural flow of the deployed trained computer model and the recorded neural flows.

[Continued on next page]

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))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*