

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
10 August 2023 (10.08.2023)



(10) International Publication Number
WO 2023/150137 A1

(51) International Patent Classification:

G06F 18/241 (2023.01) G06F 16/90 (2019.01)
G06F 9/50 (2006.01) G06N 3/0464 (2023.01)

(21) International Application Number:

PCT/US2023/012076

(22) International Filing Date:

01 February 2023 (01.02.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/305,845 02 February 2022 (02.02.2022) US

(71) Applicant: VISA INTERNATIONAL SERVICE
ASSOCIATION [US/US]; P.O. Box 8999, San Francisco,
California 94128 (US).

(72) Inventors: LIU, Miaomiao; 1114 Pinnacle Dr., Merced,
California 95348 (US). HE, Runxin; 1604 Tahoka Daisy
Dr., Cedar Park, Texas 78613 (US). CHENG, Yinhe; 8909
Marybank Drive, Austin, Texas 78750 (US). GU, Yu; 5
Grove Court, Austin, Texas 78746 (US).

(74) Agent: PREPELKA, Nathan, J. et al.; The Webb Law
Firm, One Gateway Center, 420 Ft. Duquesne Blvd., Suite
1200, Pittsburgh, Pennsylvania 15222 (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, 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,

(54) Title: SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR SECURE EDGE COMPUTING OF A MACHINE
LEARNING MODEL

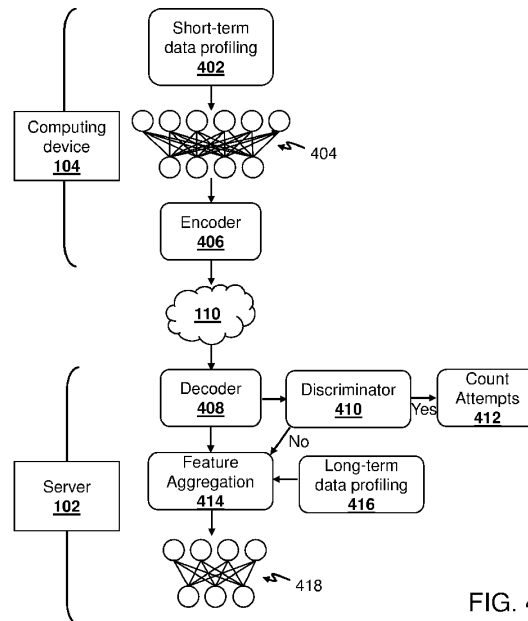


FIG. 4

(57) Abstract: Described are a system, method, and computer program product for secure edge computing of a machine learning model. The method includes transmitting, with a server, a first portion of a machine learning model to a computing device remote from the server. The first portion includes at least one first layer of the machine learning model configured to process a first input of data collected by the computing device and generate an output. The method also includes receiving, with the server from the computing device, encoded model data including the output. The method further includes decoding, with the server, the encoded model data to produce decoded model data, and generating, with the server, a classification based on the first input of data by executing a second portion of the machine learning model.

[Continued on next page]

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, 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).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

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))*