



(51) International Patent Classification:

G06F 21/50 (2013.01) G06N 20/00 (2019.01)
G06F 21/62 (2013.01) H04L 9/30 (2006.01)

(21) International Application Number:

PCT/US2019/064279

(22) International Filing Date:

03 December 2019 (03.12.2019)

(25) Filing Language:

English

(26) Publication Language:

English

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

(72) Inventor: XU, Minghua; 10810 Low Bridge Lane, Austin,
Texas 78750 (US).

(74) Agent: RICKETT, Cynthia H. et al.; Kilpatrick Townsend
& Stockton LLP, Mailstop: IP Docketing - 22, 1100
Peachtree Street, Suite 2800, Atlanta, Georgia 30309 (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, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, 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, 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,

(54) Title: TECHNIQUES FOR PROVIDING SECURE FEDERATED MACHINE-LEARNING

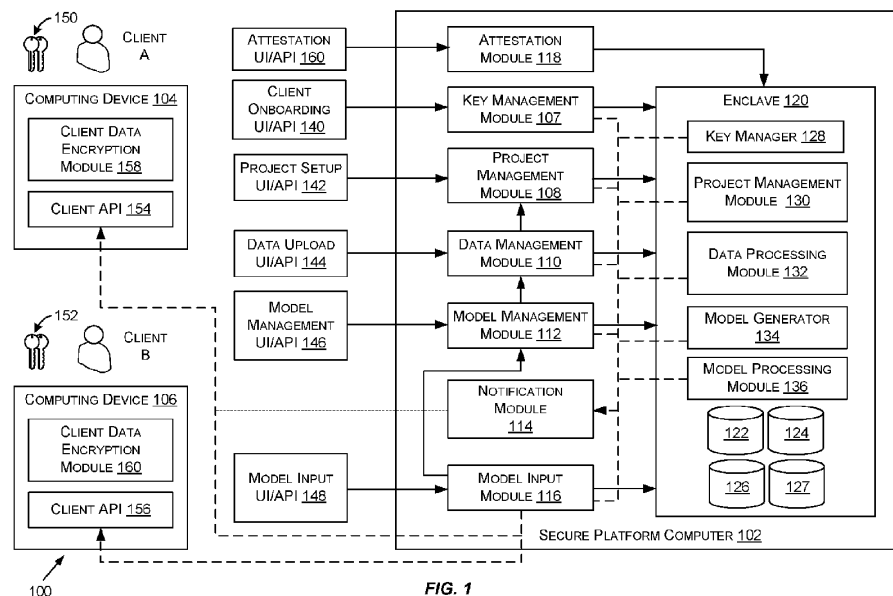


FIG. 1

(57) Abstract: Embodiments of the invention are directed to systems, methods, and devices for securely performing federated tasks (e.g., the generation and utilizing of machine-learning models). A secure platform computer may operate a secure memory space. Entities participating in a federated project may transmit respective portions of project data defining the federated project. Each entity may provide their respective (encrypted) data sets for the project that in turn can be used to generate a machine-learning model in accordance with the project data. The machine-learning model may be stored in the secure memory space and accessed through an interface provided by the secure platform computer. Utilizing the techniques discussed herein, a machine-learning models may be generated and access to these models may be restricted while protect each participant's data set from being exposed to the other project participants.

[Continued on next page]

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))*