



- (51) **International Patent Classification:**
G06N 3/08 (2023.01) *G06F 21/62* (2013.01)
- (21) **International Application Number:**
PCT/SG2025/050055
- (22) **International Filing Date:**
23 January 2025 (23.01.2025)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10202400198U 23 January 2024 (23.01.2024) SG
- (71) **Applicant:** **NANYANG TECHNOLOGICAL UNIVERSITY** [SG/SG]; 50 Nanyang Avenue, Singapore 639798 (SG).
- (72) **Inventors:** **LAM, Kwok Yan**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **WANG, Huaxiong**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **LU, Xi-anhui**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **ZHANG, Linru**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **WANG, Xiangning**; c/o Nanyang

Technological University, 50 Nanyang Avenue, Singapore 639798 (SG).

- (74) **Agent:** **DAVIES COLLISON CAVE ASIA PTE. LTD.**; 10 Collyer Quay, #07-01 Ocean Financial Centre, Singapore 049315 (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, 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, UY, 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,

- (54) **Title:** METHOD AND SYSTEM FOR SECURE TRAINING OF NEURAL NETWORK

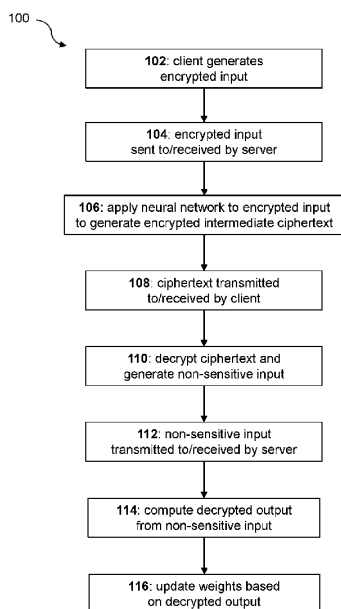


Figure 1

(57) **Abstract:** Method and System for Secure Training of Neural Network The present invention relates to a computer-implemented method for secure training of a neural network, comprising receiving a label and an encrypted input from a client, performing homomorphic computations on the encrypted input using the neural network to obtain an encrypted intermediate ciphertext, providing the encrypted intermediate ciphertext to the client, receiving a non-sensitive decrypted input from the client, wherein the non-sensitive decrypted input corresponds to a decryption of the encrypted intermediate ciphertext, performing computations on the non-sensitive decrypted input using the neural network to obtain a decrypted output, and updating weights of the neural network based on the decrypted output.

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:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*