

(51) International Patent Classification:  
*G06N 20/00* (2019.01)(21) International Application Number:  
PCT/US2020/058980(22) International Filing Date:  
04 November 2020 (04.11.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
16/675,499 06 November 2019 (06.11.2019) US(71) Applicant: VISA INTERNATIONAL SERVICE  
ASSOCIATION [US/US]; P.O. Box 8999, San Francisco,  
California 94128 (US).(72) Inventors: MOHASSEL, Payman; PO Box 8999, San  
Francisco, California 94128 (US). TRIEU, Ni; PO Box  
8999, San Francisco, California 94128 (US).(74) Agent: RACZKOWSKI, David B. et al.; Kilpatrick,  
Townsend & Stockton LLP, 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, 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,  
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))

(54) Title: TWO-SERVER PRIVACY-PRESERVING CLUSTERING

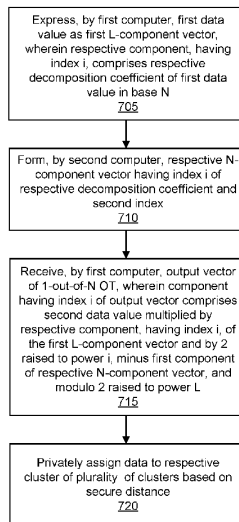


FIG. 7A

700 (57) Abstract: Described herein are systems and techniques for privacy-preserving unsupervised learning. The disclosed system and methods can enable separate computers, operated by separate entities, to perform unsupervised learning jointly based on a pool of their respective data, while preserving privacy. The system improves efficiency and scalability, while preserving privacy and avoids leaking a cluster identification. The system can jointly compute a secure distance via privacy-preserving multiplication of respective data values  $x$  and  $y$  from the computers based on a 1-out-of- $N$  oblivious transfer (OT). In various embodiments,  $N$  may be 2, 4, or some other number of shares. A first computer can express its data value  $x$  in base- $N$ . A second computer can form an  $l \times N$  matrix comprising  $l$  random numbers  $m_i, o$  and the remaining elements  $m_i, o = (y_j N^i - m_i, o) \bmod N^l$ . The first computer can receive an output vector from the OT, having components  $m_i = (y_j N^i - m_i, o) \bmod N^l$ .