

(43) International Publication Date
08 August 2024 (08.08.2024)



(10) International Publication Number
WO 2024/163014 A1

(51) International Patent Classification:

G06F 18/214 (2023.01) *G06F 21/62* (2013.01)
G06F 18/20 (2023.01) *G06N 20/00* (2019.01)

(21) International Application Number:

PCT/US2023/061884

(22) International Filing Date:

02 February 2023 (02.02.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(71) **Applicant:** VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; PO BOX 8999, San Francisco, California 94128 (US).

(72) **Inventors:** MEISER, Sebastian; PO BOX 8999, San Francisco, California 94128 (US). BENDRE, Mangesh; PO

BOX 8999, San Francisco, California 94128 (US). **DAS, Mahashweta**; 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, 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, TJ,

(54) Title: PRIVACY-PRESERVING SYNTHESIS OF ARTIFICIAL DATA

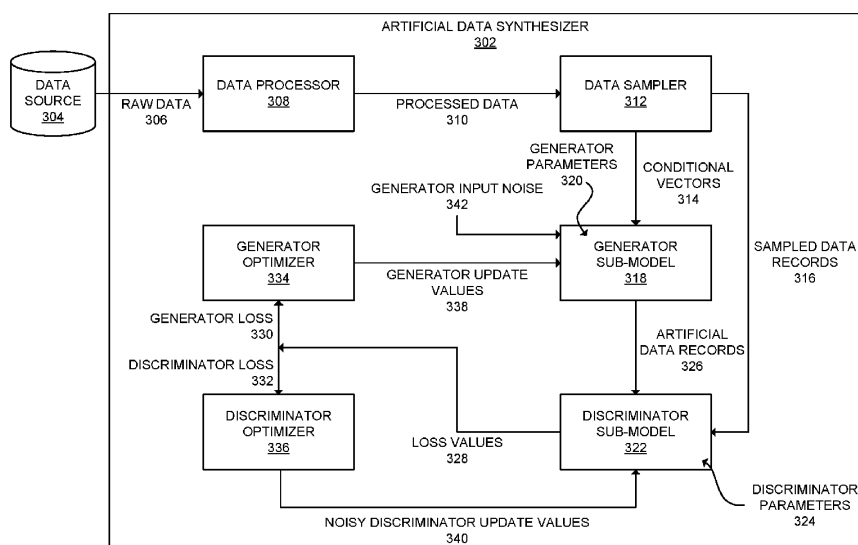


FIG. 3

(57) Abstract: Embodiments of the present disclosure are directed to the methods and systems for generating artificial data records from (potentially private or sensitive) data records in a privacy-preserving manner, particularly using machine learning models such as generative adversarial networks (GANs). Such artificial data records can be used in place of the real data in data analysis applications, such as training machine learning models. These artificial data records can be generated such that they do not (or have a low or negligible probability of) leaking information from the data records used to generate the artificial data records. As a result, artificial data records (or any machine learning models trained to generate such artificial data records) can potentially be published or distributed without violating rules, regulations, or laws restricting the transmission of sensitive data.

[Continued on next page]

WO 2024/163014 A1

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, 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, 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))