



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)
- (21) **International Application Number:**
PCT/US2019/030415
- (22) **International Filing Date:**
02 May 2019 (02.05.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
PCT/US2018/062847
28 November 2018 (28.11.2018) US
62/784,194 21 December 2018 (21.12.2018) US
- (71) **Applicant:** VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).
- (72) **Inventors:** GADDAM, Sivanarayana; 3770 Flora Vista Avenue, Apt. 307, Santa Clara, California 95051 (US). KUMARESAN, Ranjit; 965 East El Camino Real #918, Sunnyvale, California 94087 (US). SINHA, Rohit; 640 Epic Way, Apt 292, San Jose, California 95134 (US).
- (74) **Agent:** BOUQUET, Bert E. 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, 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).

(54) **Title:** TECHNIQUES FOR PREVENTING COLLUSION USING SIMULTANEOUS KEY RELEASE

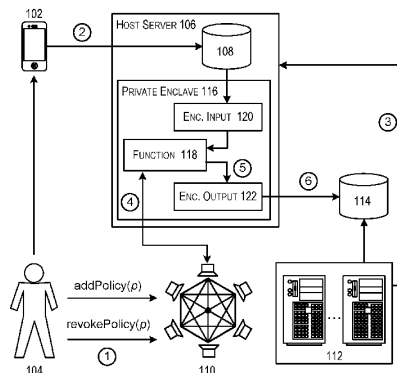


FIG. 1

(57) **Abstract:** Described herein are a system and techniques for enabling user control over usage of their information by data consumers, even when untrusted parties are involved, while also preventing collusion between the untrusted party and a data consumer. A user's information may be collected by a client device and provided to a host server. An encrypted version of the user's information may be stored at the host server so that it is processed on a private enclave of the host server. When the data is to be provided to multiple data consumers, the data may be encrypted for each of the data consumers and may be released to each of those data consumers simultaneously once confirmation has been received that the data has been made available to each of the data consumers.

Published:

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