



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/US2018/055947
- (22) **International Filing Date:**
15 October 2018 (15.10.2018)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/668,725 08 May 2018 (08.05.2018) US
- (71) **Applicant:** VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, San Francisco, California 94128-8999 (US).
- (72) **Inventors:** MOHASSEL, Payman; 1831 Hurst Ave., San Jose, California 95125 (US). AGRAWAL, Shashank; 395 Sierra Vista Avenue, Apt. 12, Mountain View, California 94043 (US). MUKHERJEE, Pratyay; 3549 Monroe St. Apt. 524, Santa Clara, California 95051 (US). MIAO, Pei-han; 2215 Jefferson Ave Apt C, Berkeley, California 94703 (US).
- (74) **Agent:** RACZKOWSKI, David 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, 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,

(54) **Title:** PASSWORD BASED THRESHOLD TOKEN GENERATION

Token Generation (Sign-On Phase)

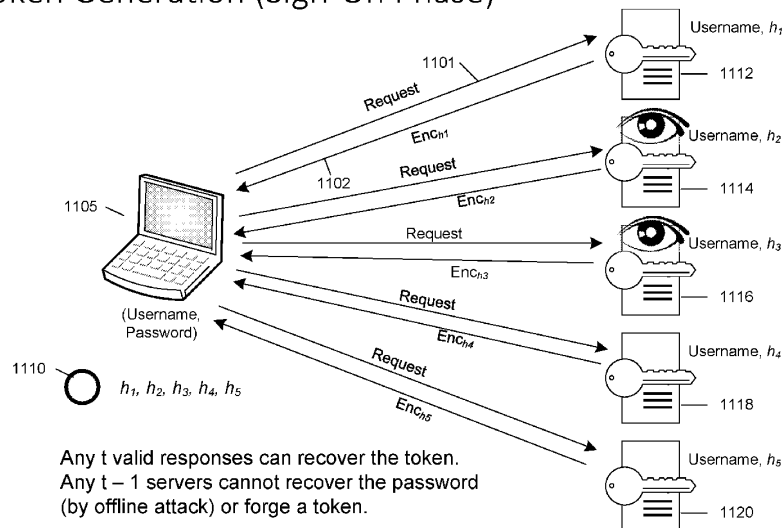


FIG. 11

(57) **Abstract:** Embodiments disclosed herein are directed to methods and systems of password-based threshold authentication, which distributes the role of an authentication server among multiple servers. Any t servers can collectively verify passwords and generate authentication tokens, while no $t-1$ servers can forge a valid token or mount offline dictionary attacks.

[Continued on next page]



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).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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