



(51) International Patent Classification:
H04L 9/32 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/US2018/043872

(22) International Filing Date:
26 July 2018 (26.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/543,500 10 August 2017 (10.08.2017) US

(71) Applicant: VISA INTERNATIONAL SERVICE
ASSOCIATION [US/US]; P.O. Box 8999, San Francisco,
California 94128 (US).

(72) Inventors: BLACKHURST, Jason; 1536 Pacific Avenue,
Suite #6, San Francisco, California 94109 (US). WAG-
NER, Kim; 606 Alberta Avenue, Sunnyvale, California
94087 (US). SHEETS, John; 915 Elizabeth Street, San
Francisco, California 94114 (US). JIANG, Chunxi; 636

Octavia Street, Apt. 304, San Francisco, California 94102
(US). ARORA, Sunpreet Singh; 1950 Elkhorn Court, Unit
213, San Mateo, California 94403 (US).

(74) Agent: RICKETT, Cynthia H. 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,

(54) Title: USE OF BIOMETRICS AND PRIVACY PRESERVING METHODS TO AUTHENTICATE ACCOUNT HOLDERS
ONLINE

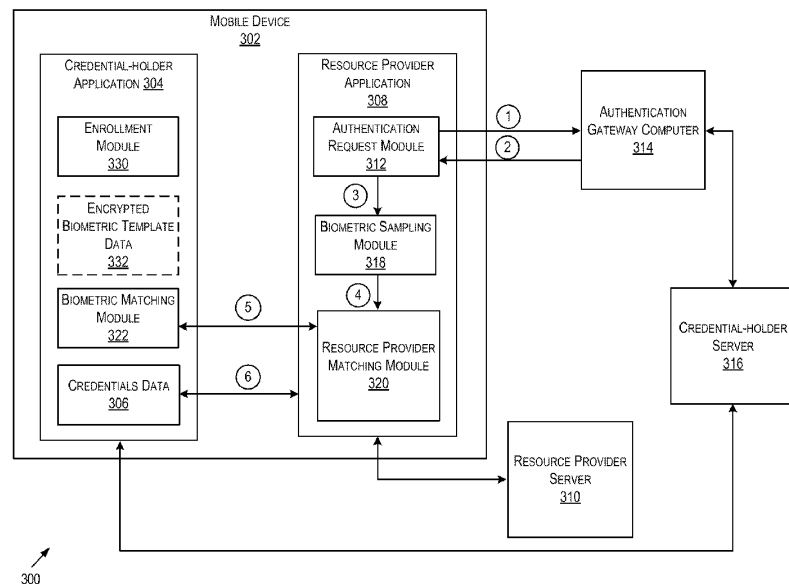


FIG. 3

(57) Abstract: Embodiments are directed to a method for securely performing biometric authentication online. The method described can be used to securely perform biometric authentication on a mobile device. For protecting the privacy of the users biometric data, a cryptographic comparison protocol can be used to perform matching of encrypted templates. For example, the cryptographic comparison protocol may involve Fuzzy Extractors (FE), Homomorphic Encryption (HE), and/or Secure Multi-Party Computation (SMPC).

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).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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