

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
13 June 2024 (13.06.2024)



(10) International Publication Number
WO 2024/124119 A1

(51) International Patent Classification:

H04L 9/40 (2022.01) *H04L 43/00* (2022.01)
H04L 43/04 (2022.01) *G06F 21/00* (2013.01)
G06F 21/50 (2013.01)

(21) International Application Number:

PCT/US2023/083103

(22) International Filing Date:

08 December 2023 (08.12.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/431,400 09 December 2022 (09.12.2022) US

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

(72) Inventors: **CHEN, Hanlin**; Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **FEDRONIC, Dominique, Louis**; Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US). **CORPUS, Jorge, A.**; Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US).

(74) Agent: **PREPELKA, Nathan, J.** et al.; The Webb Law Firm, One Gateway Center, 420 Ft. Duquesne Blvd., Suite 1200, Pittsburgh, Pennsylvania 15222 (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,

(54) Title: SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR DETECTING ANOMALIES IN COMPUTING SYSTEMS BASED ON CORRELATED SESSION DATA

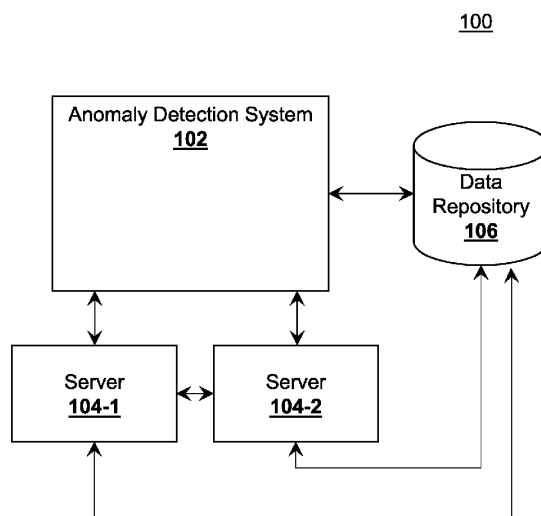


FIG. 1

(57) Abstract: Systems, methods, and computer program products are provided for detecting anomalies in computing systems using correlated session data from source servers and target servers. The method includes receiving a connection request for a connection to a target server from a source server, the connection request including a login request to a service account on the target server, the connection request initiated on the source server by a user account; generating a communication session for the user account between the source server and the target server based on the connection request; collecting target server session data associated with the target server and source server session data associated with the source server; correlating the target server session data with the source server session data to provide correlated session data; and detecting an anomaly based on the correlated session data.

[Continued on next page]

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, MU, 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, 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).

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))*
 - *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
-