

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
12 December 2024 (12.12.2024)



(10) International Publication Number
WO 2024/254614 A2

- (51) International Patent Classification:
G06F 21/56 (2013.01)
- (21) International Application Number:
PCT/US2024/033305
- (22) International Filing Date:
10 June 2024 (10.06.2024)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
18/332,254 09 June 2023 (09.06.2023) US
- (71) Applicant: **BREX INC.** [US/US]; 12832 Frontrunner Blvd., Suite 500, Draper, Utah 84020 (US).
- (72) Inventor: **LIBURDI, Joshua**; 12832 Frontrunner Blvd., Suite 500, Draper, Utah 84020 (US).
- (74) Agent: **PETTIT, Andrew**; P.O. Box 1247, Seattle, Washington 98111-1247 (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, 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.

(54) Title: SYSTEM ALERT MODELING BASED ON HYPERGRAPH ALERT CLUSTERS

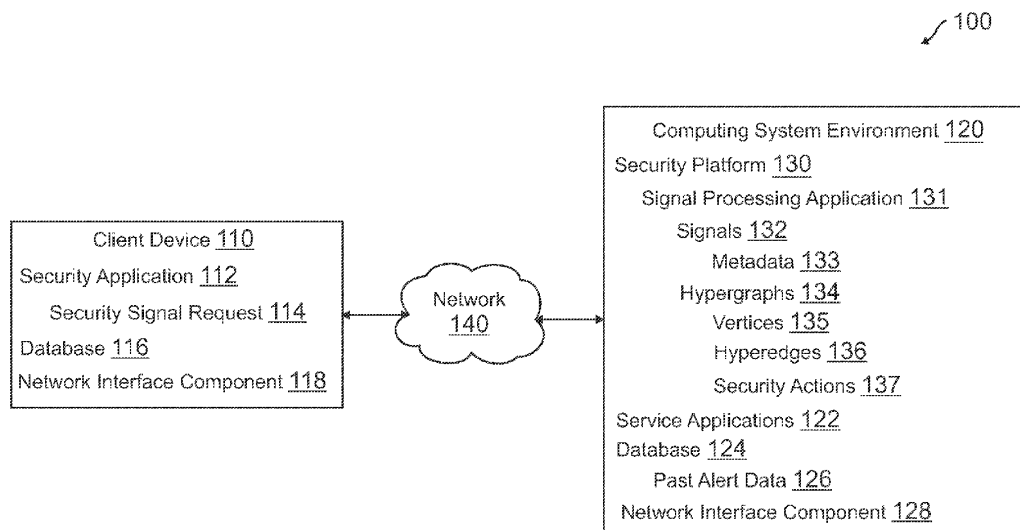


FIG. 1

(57) Abstract: There are provided systems and methods for system alert modeling based on hypergraph alert clusters. An entity, such as company or business, may utilize computing services provided by a service provider. Use of computing services provided by the service provider to different entities may generate security alerts when computing events are flagged as risky, fraudulent, malicious, computing attacks, or the like. For better security alert management, search, and alert linking, the service provider may utilize hypergraphs generated from metadata and hashes of data extracted from security alerts, such as a name, payload and the like. The service provider may model the hypergraphs using vertices and hyperedges associated with this metadata and hashes, which then allow for identifying of a threat or security alert scope, retrieval of linked security alerts during investigations, and correlation of security alerts to provide threat-focused alerts.

WO 2024/254614 A2

[Continued on next page]

(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))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*