



- (51) **International Patent Classification:**
G06F 21/56 (2013.01)
- (21) **International Application Number:**
PCT/EP2023/079686
- (22) **International Filing Date:**
24 October 2023 (24.10.2023)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
18/049,654 26 October 2022 (26.10.2022) US
- (71) **Applicant: BITDEFENDER IPR MANAGEMENT LTD** [CY/CY]; 59-61 Acropolis ave. 3rd floor, office 302, Nicosia, 2012 (CY).
- (72) **Inventor: STEFAN, Tudor**; Bd. Nicolae Balcescu nr. 49, bl. 19, sc.B, ap. 47, Judet Hunedoara, 330126 Deva (RO).
- (74) **Agent: TULUCA, Doina / Cabinet Doina Tuluca**; Bd. Lacul Tei nr. 56, bl. 19, ap. 52, sector 2, 020392 Bucuresti (RO).
- (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.

- (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).

Published:
— with international search report (Art. 21(3))

- (54) **Title:** STACKED MALWARE DETECTOR FOR MOBILE PLATFORMS

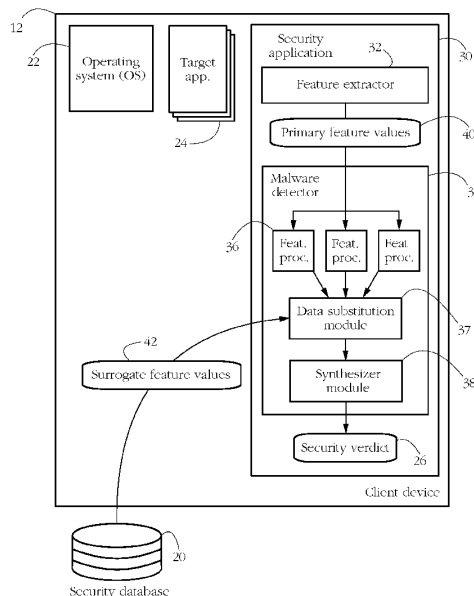


FIG. 1

(57) **Abstract:** Described systems and methods protect electronic devices such as smartphones and IoT devices against malicious software. In some embodiments, a malware detector comprises a stack/cascade of feature processors configured to determine a set of derived feature values according to primary features characterizing software executing on the respective device, and further comprises a synthesizer module configured to determine whether the client device comprises malware according to the derived feature values. When a derived feature value is currently unavailable or cannot be computed, some embodiments supply a surrogate value to replace the missing derived feature value, thus ensuring that the malware detector can always produce a verdict.