

(51) International Patent Classification:
G06F 21/56 (2013.01)(21) International Application Number:
PCT/RO2012/000020(22) International Filing Date:
5 September 2012 (05.09.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/554,859 2 November 2011 (02.11.2011) US
13/312,686 6 December 2011 (06.12.2011) US(71) Applicant (for all designated States except US): **BITDEFENDER IPR MANAGEMENT LTD** [CY/CY]; Kreon-
tos 12, PC 1076, Nicosia (CY).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **TOFAN, I. Vlad**
[RO/RO]; Str. Albert Einstein nr.4, Cluj-Napoca, jud. Cluj
(RO). **DUDEA, V. Sorin** [RO/RO]; Str. Sold, Ene Modor-
an nr. 10, bl. M90, sc.2. et 6, ap. 88, Sector 5, Bucuresti
(RO). **CANJA, D. Viroel** [RO/RO]; Sat. Petresti (Com.
Corbeanca) jud. Ilfov, Ale. Gardenia nr. 22 (RO).(74) Agent: **TULUCA, Doina**; Bd. Lacul Tei nr. 56, bl. 19,
sc.B, ap. 52, sector 2, RO-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, CZ, DE, DK, DM,DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
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, 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, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

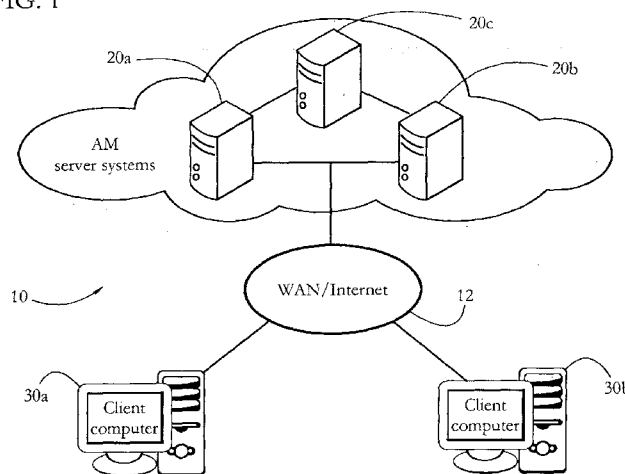
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

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))

(54) Title: FUZZY WHITELISTING ANTI-MALWARE SYSTEMS AND METHODS

FIG. 1



(57) **Abstract:** In some embodiments, an anti-malware system accounts for benign differences between non-malicious data objects, such as differences introduced by compilers and other polymorphisms. A target object is separated into a multitude of code blocks, and a hash is calculated for each code block. The obtained set of target hashes is then compared against a database of hashes corresponding to code blocks extracted from whitelisted objects. A target object may be labeled as whitelisted (trusted, non-malicious) if it has a substantial number of hashes in common with a whitelisted object. Objects which are slightly different from known whitelisted objects may still receive whitelisting status. By allowing a certain degree of mismatch between the sets of hashes of distinct objects, some embodiments of the present invention increase the efficiency of whitelisting without an unacceptable decrease in safety.