



(51) International Patent Classification:
G06F 21/20 (2006.01) **G06F 12/00** (2006.01)
G06F 13/14 (2006.01)

(21) International Application Number:
PCT/IB2010/052286

(22) International Filing Date:
24 May 2010 (24.05.2010)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US):
PRIVYLINK PRIVATE LIMITED [SG/SG]; 77 Science Park Drive, CINTech 3, #04-14, Singapore 118256 (SG).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **LAM, Kwok Yan, Karch** [SG/SG]; 38B Jalan Mat Jambol, #01-06, Island View Condominium, Singapore 119520 (SG).

(74) Agents: **SCHWEIGER, Martin** et al.; Schweiger & Partners (Singapore) LLP, 251b Victoria Street, Singapore 188035 (SG).

(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, 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, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK,

[Continued on next page]

(54) Title: METHOD AND SYSTEM OF SECURE COMPUTING ENVIRONMENT HAVING AUDITABLE CONTROL OF DATA MOVEMENT

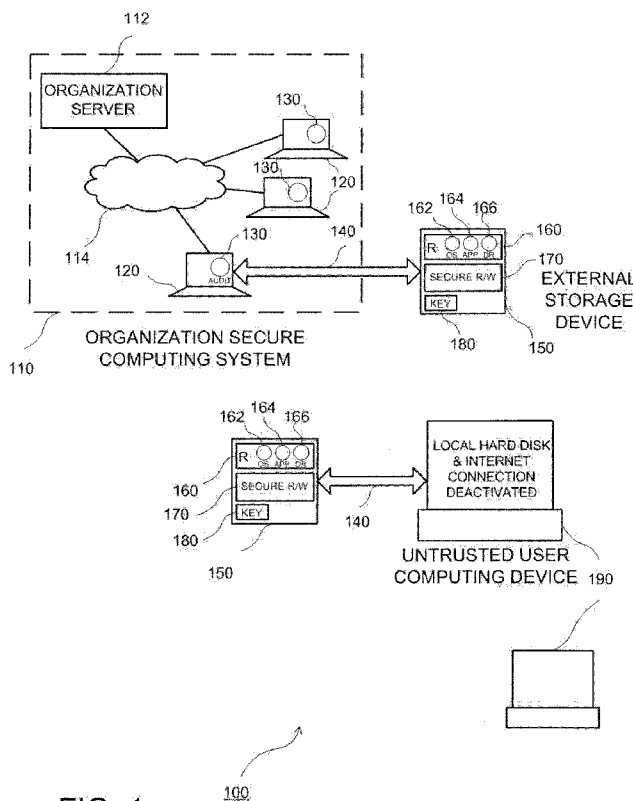


FIG. 1

(57) Abstract: Method and system of secure computing environment are provided. The secure computing environment allows a user to transfer organization data to an external storage device authorized by the organization. The external storage device comprises two partitions one of which is read-only whereas the second read/write-enabled partition stores organization data in encrypted form. When the user interfaces the external storage device with an untrusted user computing device, the untrusted user computing device is booted from an operating system pre-installed in the external storage device followed by deactivation of the Internet connection, local hard disk and all unauthorized input-output devices. Data movement and any other pre-determined events are recorded in auditable logs as per the organization security and data movement policy. The secure computing system extends the trusted computing environment of an organization to untrusted user computing devices outside the organization.

WO 2011/148224 A1



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, **Published:**
GW, ML, MR, NE, SN, TD, TG).

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