

(51) International Patent Classification:
G06F 21/72 (2013.01)(21) International Application Number:
PCT/US2014/045125(22) International Filing Date:
1 July 2014 (01.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/932,828 1 July 2013 (01.07.2013) US(71) Applicant: AMAZON TECHNOLOGIES, INC.
[US/US]; P.O. Box 8102, Reno, Nevada 89507 (US).

(72) Inventors: POTLAPALLY, Nachiketh Rao; 410 Terry Avenue North, Seattle, Washington 98109 (US). BRAND-WINE, Eric Jason; 410 Terry Avenue North, Seattle, Washington 98109 (US). WILSON, Matthew Shawn; 410 Terry Avenue North, Seattle, Washington 98109 (US).

(74) Agents: LOHR, Jason D. et al.; Novak Druce Connolly Bove + Quigg LLP, 1000 Louisiana Street, Fifty-Third Floor, Houston, Texas 77002 (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, 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))

[Continued on next page]

(54) Title: CRYPTOGRAPHICALLY ATTESTED RESOURCES FOR HOSTING VIRTUAL MACHINES

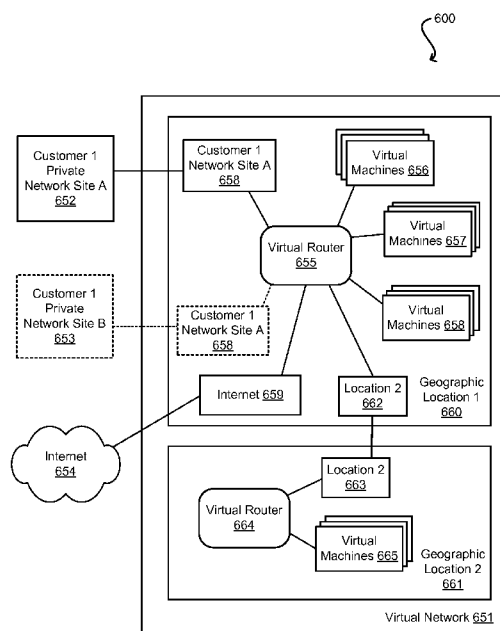


FIG. 6

(57) Abstract: Approaches to enable the configuration of computing resources for executing virtual machines on behalf of users to be cryptographically attested to or verified. When a user requests a virtual machine to be provisioned, an operator of the virtualized computing environment can initiate a two phase launch of the virtual machine. In the first phase, the operator provisions the virtual machine on a host computing device and obtains cryptographic measurements of the software and/or hardware resources on the host computing device. The operator may then provide those cryptographic measurements to the user that requested the virtual machine. If the user approves the cryptographic measurements, the operator may proceed with the second phase and actually launch the virtual machine on the host. In some cases, operator may compare the cryptographic measurements to a list of approved measurements to determine whether the host computing device is acceptable for hosting the virtual machine.



-
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) — 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))

Published:

- with international search report (Art. 21(3))