

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2023 年 5 月 11 日 (11.05.2023)



(10) 国际公布号
WO 2023/078161 A1

(51) 国际专利分类号:
G06N 3/04 (2006.01)

中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(21) 国际申请号: PCT/CN2022/128036

(22) 国际申请日: 2022 年 10 月 27 日 (27.10.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111309418.7 2021 年 11 月 6 日 (06.11.2021) CN

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): 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, 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。

(72) 发明人: 顾婉玉 (GU, Wanyu); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。郑显义 (ZHENG, Xianyi); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。辛知 (XIN, Zhi); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。郭栗 (GUO, Li); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。万小飞 (WAN, Xiaofei);

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (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,

(54) Title: OPERATION OF MODEL

(54) 发明名称: 模型的运行

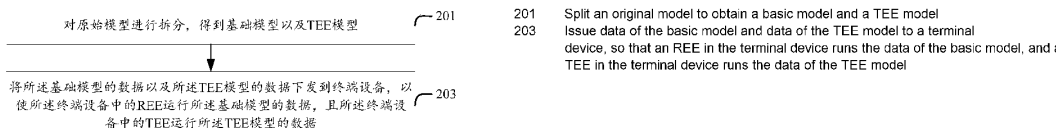


图 2

(57) Abstract: Provided in the embodiments of the present description are an operation method and apparatus for a model. The method comprises: splitting an original model to obtain a basic model and a trusted execution environment (TEE) model (201); and issuing data of the basic model and data of the TEE model to a terminal device, so that a rich execution environment (REE) in the terminal device runs the data of the basic model, and a TEE in the terminal device runs the data of the TEE model (203). By means of the present description, the operation safety of a model can be improved.

(57) 摘要: 本说明书实施例提供了模型的运行方法和装置。在方法中, 对原始模型进行拆分, 得到基础模型以及 TEE (Trusted Execution Environment) 模型 (201); 将基础模型的数据以及 TEE 模型的数据下发到终端设备, 以使终端设备中的 REE (Rich Execution Environment) 运行基础模型的数据, 且终端设备中的 TEE 运行 TEE 模型的数据 (203)。本说明书能够提高模型运行的安全性。

[见续页]

WO 2023/078161 A1

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)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。