地 平 线
Horizon Robotics

模型加密功能介绍

Horizon Robotic

2021-05-25

目录

简介

地平线的模型加密设计支持指定模型进行加密，加密后的模型只能运行在指定设备上。同时支持能力集的方式进行加密，指定不同的设备运行一个打包的模型当中的不同能力的模型。

加密应用场景举例

场景 1：

用户 A 有一套人脸识别算法模型，但为了保证模型的安全和私密性，不希望其模型被任何人拿到后都可以使用，因此可以通过地平线工具进行加密操作，完成后该加密模型仅能在被授权设备上运行。

场景 2：

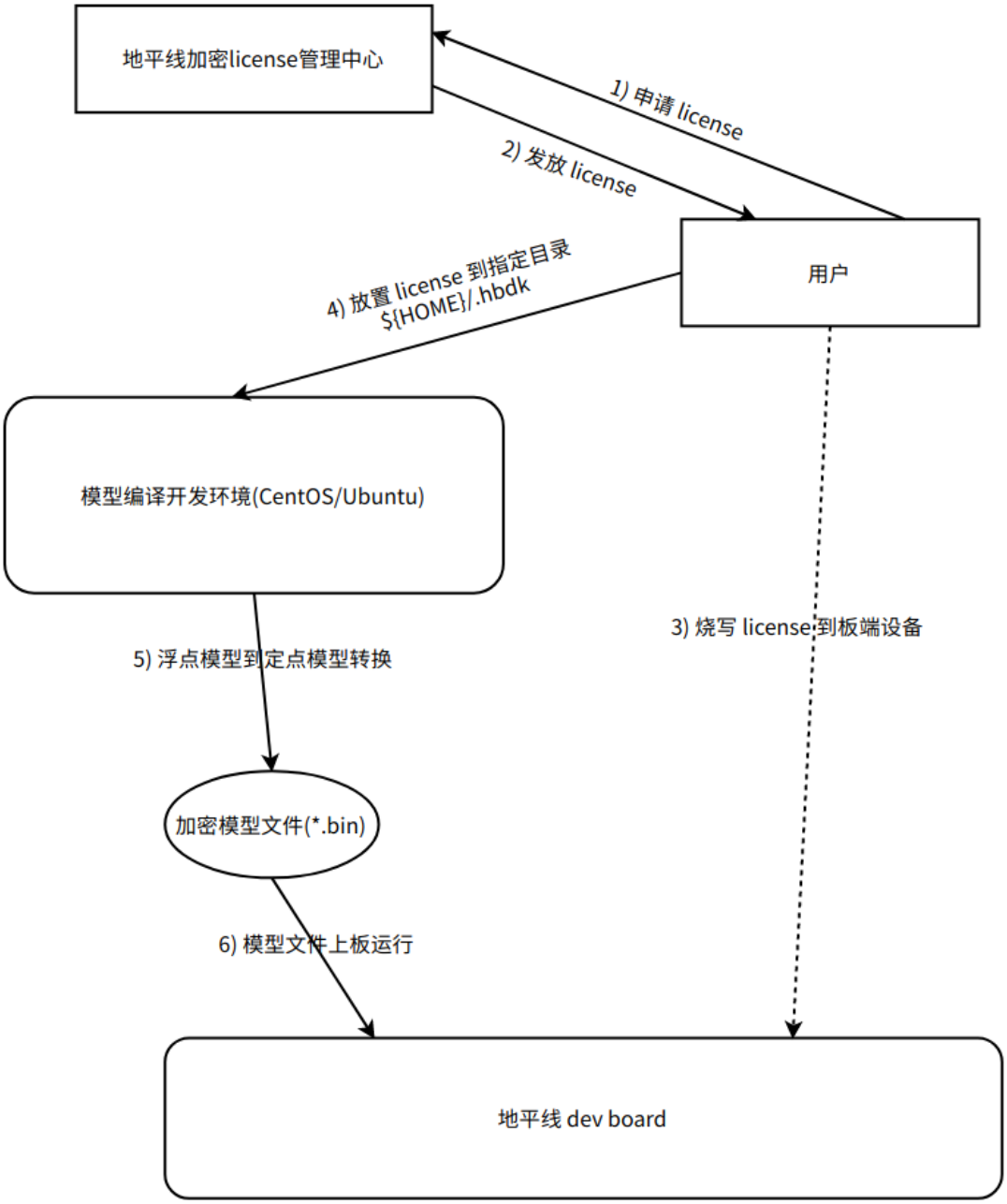
用户 B 有一套检测算法模型，其中包括了人脸检测、人体检测、宠物检测等等不同能力的模型，这些模型都被打包为一个 pack 模型进行售卖。

用户 B 希望根据其客户的付费程度不同，给予不同的检测能力使用权限，因此可以通过地平线工具指定能力集的方式进行加密。

例如，可以指定人脸检测为能力集：0.人体检测为能力集；1.宠物检测为能力集；2.模型经过加密后，针对客户的付费高中低情况，给与含有不同能力集 license 的芯片开发板，低付费用户仅开放能力集 0.仅能够使用人脸检测模型；中付费用户可开放能力集 0 和 1，能够使用人脸及人体检测模型；高付费用户可开放能力集 0- 2，能够使用全部三种模型。

模型加密流程

模型加密流程如图所示：



用户可根据自身的不同需求，向地平线申请 license。拿到相应的 license 后便可以放置到开发环境的指定目录(${HOME}/.hbdk)下，指定模型的能力集，利用工具进行浮点模

型的转换。转换完成后会得到扩展名为 "bin"的模型文件，该文件即为加密的模型文件。当需要将 license 烧写到制定开发板上时，只需将 license 包中的 json 文件通过 "Hobot Secure Chip Tool" 工具，从串口连接进行烧写即可。

模型加密的注意事项

1) 若模型转换过程中并未指定能力集，且指定目录下有 license 文件放置，则会默认使用 license 中序号最小的，并且为“on"的能力集编号对模型进行加密。此时若想编译无加密模型，请先移除指定目录下的 license 文件。
2) 单个模型仅支持归属于一个能力集，目前不支持一个模型归属于多个能力集的功能。
3) 板子上目前只能烧写一个 license。生成编译模型的 license 时可以指定不同的能力集，但需要知道板子上 license 的明文。一旦知道板子上 license 的明文，就可以生成任意能力集的编译 license。
4) license 文件可在芯片贴片前就完成烧写，加快产品生产进度，详情请联系项目代表。