中国人工智能产业发展联盟
Artificial Intelligence Industry Alliance

深度学习技术选型白皮书

(2018 年)

中国人工智能产业发展联盟

2018 年 10 月

版权声明

前　言

人工智能是一种引发诸多领域产生颠覆性变革的前沿技术，当前以机器学习，特别是深度学习为核心，在视觉、语音、自然语言等应用领域迅速发展，已经开始像水电煤一样赋能于各个行业。

深度学习软件框架及相关工具集是人工智能应用落地的重要抓手，是人工智能相关服务及产品的核心。本白皮书专注于以深度学习为核心的软件框架及工具，以实际需求为指引，提出深度学习技术选型考虑及指标，旨在为企业应用深度学习技术开展业务提供参考，同时为以开源框架为技术核心的服务及产品选型评测提供依据。

深度学习技术选型白皮书是中国人工智能产业发展联盟开源开放推进组的研究成果。本白皮书从深度学习训练框架、推断框架及技术生态工具集三个维度系统梳理总结了基于开源的深度学习技术体系，结合企业自身业务开展需求，分析了技术选型因素，提出了选型指标体系，并就软件框架目前存在的问题及技术发展趋势进行了研判。中国人工智能产业发展联盟后续将在此研究基础上继续深入开展相关研究及评估标准制定工作，并继续发布相关研究成果。

目　录

一、深度学习软件框架发展概述

（一）深度学习框架是人工智能产业化落地的核心

当前，基于深度学习的人工智能算法主要依托计算机技术体系架构实现，深度学习算法通过封装至软件框架[1]的方式供开发者使用。**软件框架是整个人工智能技术体系的核心，实现对人工智能算法的封装，数据的调用以及计算资源的使用，起到承上启下的重要作用。**深度学习软件框架在人工智能技术产业化实现详见图 1 所示。

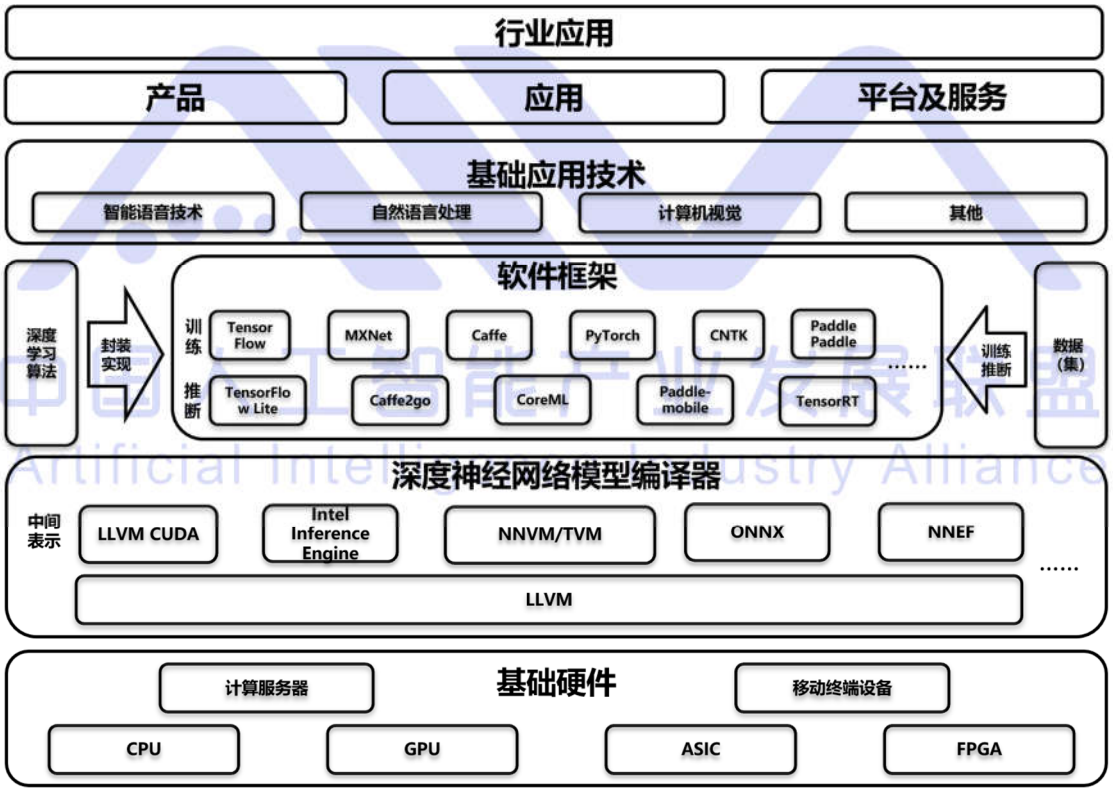

图 1 基于深度学习的人工智能技术应用架构图[2]

[1] 软件框架（software framework），通常指的是为了实现某个业界标准或完成特定基本任务的软件组件规范，也指为了实现某个软件组件规范时，提供规范所要求之基础功能的软件产品。

[2] 该图摘自中国信息通信研究院、中国人工智能产业发展联盟于 2018 年 9 月 6 日联合发布的《人工智能发展白皮书-技术架构篇（2018 年）》

人工智能基础性算法理论研究已经较为成熟，各大厂商纷纷发力建设算法模型工具库，并将其封装为软件框架供开发者使用。**软件框架是算法的工程实现。**企业的软件框架实现有闭源和开源两种形式：少数企业选择闭源方式开发软件框架，目的是打造技术壁垒；目前业内主流软件框架基本都是开源化运营。本白皮书主要关注开源软件框架的技术及应用特点，对闭源软件框架不做过多讨论。

（二）深度学习框架的分类

基于深度学习技术的服务及产品主要涉及到三类软件框架，按照应用场景分为云端训练、云端推断以及端侧推断。不同应用场景任务不同，所需承载的计算及限制条件也存在差异，因此针对各场景计算工具的功能及性能要求均有不同。

云端训练框架主要完成面向海量数据的模型训练任务，对算力要求最高，实际应用中需要采用分布式计算等技术，同时对于工业级模型及稳定性也有特殊要求；云端推断框架主要完成训练模型的优化、云端部署及推断计算等工作，对于效率及并发性等具有特殊要求；终端推断框架主要完成训练模型在终端的部署及计算，由于终端功耗、功能、芯片等众多限制，终端推断框架的性能、能耗及自身优化需满足多种限制性要求。

本白皮书第二章重点对云端训练软件框架技术选型进行分析阐述，第三章重点对基于云端及终端的推断框架技术选型进行对比分析，并分别研提了选型考虑及评价指标体系。

二、 深度学习训练框架技术选型

（一） 深度学习训练框架应用现状

1. 深度学习训练框架使用趋同

由于深度学习训练框架技术及生态已经趋于成熟，从目前产业界实际使用情况来看，以 TensorFlow 及 Caffe/Caffe2 为引领的深度学习训练框架占据了相对主导地位，PaddlePaddle，MXNet，PyTorch，Keras 等主流训练框架由于其各自特性也在业务部属中得到了充分使用。

TensorFlow 已在各行各业的生产场景中得到了充分的应用，企业选择 TensorFlow 训练框架主要有以下原因：

一是该框架生态成熟，功能完备。得益于其成熟的生态建设，基于该框架已有众多实用网络结构模型开源可供使用，其模型库（Model Zoo）及开源社区涵盖了几乎所有深度学习算法模型，同时也支持包括概率编程、强化学习在内的多种先进算法，在如目标识别、图像处理、视频分析、自然语言处理、各类数据分析等领域得到广泛应用。同时其基于计算图和低层次 OP 描述计算，提供了最大程度的灵活度，非常适合作为 “底层”框架使用，在其基础上通过高层封装来支持不同种类的学习算法，如深度学习（Keras）、深度强化学习（Dopamine）、深度概率图模型（Edward）等，并且都具备 GPU 加速能力，这一点对于希望通过单一框架支持其各类复杂应用的企业来说具备很大的吸引力。

二是该框架容易上手，相对易用。得益于其良好的生态及丰富的社区资源，该框架使用文档及相关教程相对完善，开发人员丰富，已

成为算法工程师主流技能。企业选用该训练框架能够良好匹配开发人员使用习惯，降低业务开发门槛，提升业务开发效率。

三是该框架性能稳定，功能成熟。得益于谷歌公司为主导的技术支持，该框架在处理大规模数据训练时表现稳定，性能优良，具备端到端训练、推理能力。TensorFlow 训练完成后的模型，可以由 TensorFlow Lite 加载并运行于 Android 平台之上，对于手机厂商开发端侧智能应用非常方便。同时由于采用该框架底层技术架构的推断芯片市面占比也相对较高，因此从模型训练、模型优化到模型部署的产品线功能相对成熟且完善，能够有效提升企业相关业务的开发及实际部署效率。

四是该框架灵活性高，改进方便。该框架提供的 API 接口丰富，灵活性高，在算法改进上较为方便，非常适合于企业算法预研及快速实现验证等工作。同时其兼容开源接口，能够以丰富、便捷、高效的品质帮助用户轻松使用深度学习技术，通过灵活调度按需服务化方式提供模型训练、评估与预测。

Caffe/Caffe2 凭借其在计算机视觉领域成熟的生态及技术深耕，成为了企业在计算机视觉领域开展相关业务的首选框架，企业主要考虑如下：

一是训练速度快，性能优异。该框架在图像处理、3D 卷积计算等领域性能突出，在计算机视觉领域训练速度相对较快，广泛应用于包括人脸识别、目标跟踪、图像视频内容识别、视频图像分析等领域。

二是支持算法多，生态成熟。该框架在计算机视觉领域拥有深厚

的技术积累，包括企业及学术界在内的基础受众多，同时版本相对稳定，基于 Caffe 开发的计算机视觉领域模型众多，降低了企业开展业务的门槛，同时该框架能够有效匹配计算机视觉领域专家及工程师使用习惯，相关文档及教程丰富，使用门槛低，能够有效提升企业业务开展效率。

三是扩展功能丰富，使用灵活。基于该框架的开源扩展功能众多，可以支持多机多 GPU 分布式训练，同时在模型移植方面也有较为成熟的开源模型转换工具，企业在算法研究、算法调参、算法快速产品化等研发阶段可快速进行验证，能够有效满足实际业务的定制化需求。

PaddlePaddle 作为我国自主研发并开源的深度学习训练框架，在支撑百度公司内部业务及工业级应用场景中得到了广泛应用，企业选择 PaddlePaddle 训练框架主要有以下原因：

第一是工业性能优异。在面向海量数据处理的应用场景下，模型参数及特征达到上万亿级别，其工业性能及分布式计算支持为此类业务提供了强有力的支撑，企业在信息流广告点击率预估、粗排模型及大规模稀疏矩阵模型计算等场景方便易用，高效快速，修改少量参数即可运行大规模 embedding 模型。

第二是中文支持优异。该框架中文技术文档齐全，对于中文支持较好，内置对应的初步模型，可以直接使用推断函数，提供少量的样本就可以定制化模型。同时框架对于中文问答系统及其文本语义相关模型支持较好，也可以同其他自然语言处理的开源工具配套使用。

第三是易用性优良。依托于百度公司技术研发力量，该框架生态

技术工具较为完备，提供统一的 PaddlePaddle Cloud 训练及推断环境，降低开发者生产环境搭建工作，可以根据实际需求支持简洁的 GPU 多机多卡训练调起等工作，极大降低开发者使用门槛，提升开发效率。

其他主流框架的使用主要基于三方面的考虑，第**一是**企业用于研发及算法研究所使用的 PyTorch、Theano，第**二是**企业在开展实际业务中为实现高性能产品服务，快速产品迭代开发所使用的 MXNet、Keras 等框架，第**三是**专门针对特定应用领域而使用的工具框架，如 Kaldi、Spark MLIB 等。

PyTorch、Theano 等框架主要应用于算法研究领域，由于其在学术界使用历史较长，资源相对丰富，因此企业一般将其用于算法预研与快速实现验证，同时由于其提供参数可视化及动态图等特性，为参数调节提供极大便利，在分类算法、语义相似度计算、序列标注算、句子生成等应用较多。

MXNet 以其优越性能得到广泛应用，该框架同时其兼容开源接口，内置大量优化的网络模型算法，以丰富、便捷、高效的品质帮助用户轻松使用深度学习技术。该框架支持 C++、Python、R,、Scala 以及 Matlab 等语言，同时还支持命令和符号编程；可以运行在各种通用异构的 CPU、GPU 集群上。Keras 以其比 TensorFlow 更加便易的使用和调节，极大简化了做后期模型更新迭代尝试的效率。

在具体应用场景中，Kaldi 作为语音训练常用训练框架在语音算法训练算法研究、调参、快速产品化得到广泛使用，企业在基于 Spark 生态下部署深度学习计算任务时，倾向采用具有强大的数据处理能力

和封装多种常用算法的 Spark Mllib 框架，以实现与现有大数据 Spark 平台的无缝对接。

2. 产业对训练框架提出新需求

随着业务开展的不断深入，产业界对于深度学习训练相关计算及业务开展不断提出新的需求。总体来讲，在实际人工智能产品研发中，各框架系统及其组件存在复杂性，不同的应用场景涉及到的系统及组件不同，版本碎片化和独立性问题严重，系统与系统之间，组件与组件之间的信息交互与共享难度较大，模型复用率低，造成建模和算法训练工作量大，时间较长。具体来看主要存在以下主要问题：

一是开源框架及工具无法直接满足实际生产需求。在实际生产过程中，算法及应用多样化，尽管开源社区及模型库已有海量算法可供选择参考，但依然无法满足实际业务需求，不具备算法研发能力的企业面临较高门槛。同时，开源框架及工具集所能提供的训练速度及训练效率、训练可视化工具、框架可扩展性以及易用性等均无法满足工程化需要。

二是企业自定义实现的算法在多平台间切换时需要重复开发。由于算法与平台耦合程度高，相同算法在不同平台不同框架下实现时技术差异大，由于各个训练框架数据的输入输出格式也各不相同，实际业务开展中不同平台间的适配工作也需要投入大量人力资源。

三是训练框架与硬件平台耦合程度相对较高。实际业务开发需要算法工程师也了解一定的平台开发技术，提高了实际开发门槛，因此训练框架对于底层的硬件优化解耦程度有待加强。

（二） 训练框架选型考虑

针对以上产业需求，结合学术界前期已经在深度学习训练框架选型对比方面做出的工作，现就训练框架选型提出以下指标体系供参考。

整个指标体系纵向分为五个大类，分别从生态建设、易用性、性能、支持架构以及安全稳定性入手进行了分析，横向分为三级指标进行细化，每级指标是对前一级指标的细化。具体二、三级指标的细化会在同步开展的《深度学习技术选型评估规范（名称待定）》中做进一步的讨论。深度学习训练框架选型指标体系如表 1 所示。

表格 1 深度学习训练框架选型指标体系

一级指标	二级指标	三级指标
生态建设	支持的编程语言（接口）	Python/C++/R 等
	教程、文档及培训材料	官方文档、社区文档以及合作培训机构资源等
	核心开发者及贡献者	活跃程度及参与者数量
易用性	模型搭建/复用/迁移	模型复用难易程度
	可用高级语言程序二次开发	Python/R 等
	自定义扩展	提供功能性扩展接口
	跨平台情况	支持不同软硬件平台开发
	模型库支持	CNN RNN 模型支持
		工业/应用级模型支持
性能	模型库模型运行表现	模型库模型运行表现
	自定义应用表现	并发性；稳定性
		特征规模；数据规模 处理速度；吞吐量
	硬件加速支持	支持不同硬件加速；提供针对不同底层的优化

支持架构	CPU/FPGA
	单 GPU/多 GPU
	分布式训练
	对于虚拟环境的支持
稳定性	第三方库使用

生态建设是项目技术及人员的重要保障。主要从三方面进行考虑：一是训练框架是否支持多种高级语言。多种高级语言支持能够灵活匹配不同开发者使用习惯，同时能够有效降低实际开发门槛，多种开发语言的兼容性也意味着能够让更多的开发者加入到开源社区的工作中来，是生态建设的重要环节。二是教程、文档及培训材料的质量及数量。不同深度学习训练框架学习曲线不同，权威易用的官方教程，开源社区针对不同项目提供的文档，以及产业界提供的培训材料及服务能够降低企业业务开展门槛，同时为后续技术及算法研发提供有力保障。三是核心开发者及贡献者情况。核心开发者是开源社区的技术中坚力量和保障，对于整个项目的推动及运营具有非常重要的意义，项目贡献者的活跃程度及数量是项目健康运营及发展的重要保障，也是项目技术能力及生态建设的重要体现。

易用性是企业高效开展业务的重要考虑因素。主要从五方面考虑：**一是**模型复用的难易程度，相同模型在不同框架上的无缝开发及部署能够极大提升业务开展效率，节约开发成本。**二是**对于高级语言程序编写的支持情况。高级编程语言的使用能够有效增加代码可读性，提升项目开展效率，降低项目开发门槛，训练框架对于高级编程语言的支持对于项目高效开展具有重要意义。**三是**框架对于用户自定义扩展

的支持。尽管开源社区及框架模型库提供了多种算法模型及功能模块可供使用，但在实际业务开展中依然无法满足企业实际需求，针对框架进行的算法及功能二次开发具有重要实际意义，因此框架本身对于扩展性功能开发的支持程度决定了其实际使用范围。**四是**跨平台情况，根据前文需求分析可以看出，训练框架与底层硬件架构仍未能完全解耦，不同训练框架跨平台部署及使用情况不尽相同，使用不同框架在不同平台上完成相同算法开发需要大量适配及调优工作，因此训练框架对于跨平台的支持能够对业务开展成本产生重要影响。**五是**对于模型的支持情况，这里主要考虑是对于深度学习模型以及在产业及工业场景中实际使用模型的支持情况，成熟的生态能够吸引来自各行业领域的专家的使用和回馈，在支持更多模型的基础上也能够对框架底层优化提供指导案例。

训练框架在实际工程中的性能表现是最为主要的选型考虑。训练框架开发主要来自学术机构和企业两股力量，其中学术界开发的训练框架一般结构相对简单，应用方向相对较窄，在特定的领域有较高的性能，其设计的出发点是算法开发的便捷性；企业界开发的训练框架（如 PaddlePaddle、TensorFlow、MXNet）结构更为复杂，应用领域宽广，实际功能更为齐全，其出发点是结合企业商业考虑及实际工程目的的算法开发。各大硬件产商基于开源训练框架的深度定制版本的性能表现是其核心考虑要素。

综上，根据训练框架主导开发机构的不同，总结来看主要分为两方面的考虑：针对学术机构所指导开发的框架，主要考虑其原生自带

模型库中模型的性能表现，主要体现为在不同 Batch Size 下运行经典网络所涉及到的包括时间在内的性能指标；针对企业深度定制计算框架，主要考虑依托开源计算框架自行开发使用的模型计算性能表现，由于各框架设计机理及应用场景各具特点，因此主要从并发性、稳定性、特征规模以及优化工具支持四个方面入手进行测试分析：并发性旨在衡量深度学习计算系统中能够同时执行的特定计算，及其之间的交互效率；稳定性旨在衡量深度学习训练框架在执行任务时系统的稳定可靠程度；特征规模旨在衡量深度学习训练框架及系统所能达到的训练数据处理吞吐能力；同时，企业针对不同底层硬件所定制的优化加速工具支持也是非常重要的考虑因素。

训练框架对于多种底层硬件架构的支持对于实际生产具有重要意义。对于云端训练场景来说，针对单机单卡、单机多卡，计算集群，FPGA 加速等场景的定制化加速能够显著提高训练速度，降低开发成本，在面临大量的计算任务面前，更高的计算效率，更低的设备互联延迟，能够有效降低设备投入成本，有效利用 CPU 和 GPU 多个核心的分布式训练能力，能够提升整体处理效率。

训练框架的安全性是业务稳定开展的核心保障。尽管安全性一般来说更多的是从系统层级进行统筹考虑，但训练框架本身作为系统重要核心组件，其本身也存在特定的安全问题。当前深度学习框架及系统均面临着包括对于输入数据可控、监测程序缺失等问题，同时深度学习依赖框架众多，任何在深度学习框架以及它所依赖的组件中的安全问题都会威胁到框架之上的应用系统。同时，训练框架模块往往来

自不同开发者，对模块间的接口理解及实现也存在差异，这种不一致性也带来了很大的安全隐患。

（三） 产业优秀使用案例

目前产业界已基于开源计算框架开发打造了一系列便于开发者使用的开放能力平台及服务，提升了 AI 开发效率，降低了 AI 使用门槛，取得了非常好的社会经济效益。

1. 基于 TensorFlow 构建大规模应用系统

1) 深度学习训练云

如前所述，TensorFlow 在构建企业级深度学习训练云中，相对于其它框架具备独特优势，然而企业级训练场景中，需要的是基于 TensorFlow 的分布式训练作业高效运行于容器云环境之上的服务。具体来说，就是将 TensorFlow 部署在 K8s 和 Docker 之上运行。这其中主要包括三项主要工作：

一是扩展 K8s[3]，使其能够优化资源的分配。图 2 是将分布式 TensorFlow 运行于 k8s 和 Docker 之上的示意图。

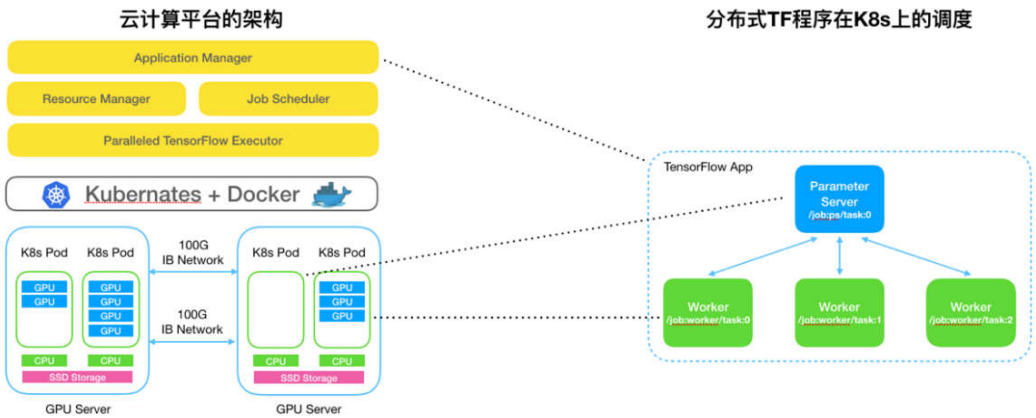

图 2 分布式 TensorFlow 运行于 K8S 与 Docker 示意图

[3] K8s，Kubernetes 简称，是一个开源的，用于管理云平台中多个主机上的容器化的应用。

二是自动改写 TensorFlow 计算图，使其能够分布式计算。图 3 展示了单机 TensorFlow 转变为分布式 TensorFlow 程序的处理流程。

图 3 单机转换为分布式 TENSORFLOW 程序处理流程

三是匹配数据传输与计算速率。基于 GPU 计算的瓶颈其实并不在于 GPU 的算力，而是向 GPU 提供数据的能力。目前有多种技术手段可完成流水线的优化，包括：通过灵活的数据缓存方案降低节点间的网络传输；每个作业设置合理的 CPU core 和 GPU 的比例，使数据与处理速度与 GPU 计算速度匹配；以及使用 Stage Area 隐藏 GPU-CPU 之间的数据拷贝等。

2）智慧城市交通系统

智慧城市交通系统 TrafficGo 基于 TensorFlow 框架打造，通过智能化调度策略，动态调整交通情况，以坂田一个路口为例平均减少等待时间 24%，能够有效治理交通拥堵，减少碳排放量。以区域信号灯协同调度为例，其在 TrafficGo 系统中业务流程如下：

图 4 TRAFFICGO 区域信号灯协同调度业务流程

系统通过采集交通卡口数据，在云端基于 TensorFlow 框架实现识别车流、人流信息的云端训练，实时获取感知最新的交通流量变化，实时更新训练模型模型公有云推断或边缘推断，能够使信号机厂商集成使用 TrafficGo 服务。系统支持离线周期，在线周期，中央感应，区域协同调度模式，分小时级别，分钟级别，秒级别的调度尺度，以适配不同场景、不同地市信息化建设水平的交通大脑落地需求。

3) 实现机械轴承的智能故障诊断

轴承故障是机械系统常见的故障模式之一，对长期运行中的设备来讲，平时的检测跟踪尤为重要。检测项目包括轴承的旋转音、振动、温度、润滑剂的状态等，根据检测结果，设备维护人员可以准确地判断设备的问题点，提早作出预防和解决方案。

使用状态监控系统收集机器的全时段数据，针对目标的被测电机在邻近电机轴承位置添加加速度传感器，进行实时的数据采集、存储并上传到 INDICS 平台上。通过 TensorFlow 框架实现对上传数据的训练，实时对轴承的状态数据进行深度挖掘，提取数据的隐含信息，对

于数据特征的相关性进行判断和选择，最终输出轴承的健康状态。此方法能够很好地识别滚动轴承的健康状态，将轴承内滚道故障、外滚道故障、球故障，并进行准确分类，达到 97%左右的准确率。

2. 基于 Keras 简洁高效实现智能化运维

运营商在固定宽带离网预测场景中使用 Keras 框架实现智能化运维的目标。Keras 具有易操控性和代码的高效性特征，一个模型的搭建只需要短短几行代码便可实现。使用 Keras 的简便程度就好比在搭积木，逐一往上叠加即可。除了代码的效率高，简洁之外，Keras 的可调整性可实验性更高。在固定宽带离网预测项目中，开发人员可以利用 Keras 随意的添加隐藏层层数，选择激活函数、损失函数等一系列关键东西，这些改变添加都是以十分简便明了的代码即可完成。研发人员使用 TensorFlow 写完模型的时间大约为 2 小时，使用 Keras 写完模型的时间大约为 30 分钟，在开发时间维度上提速了 75%。

3. 基于 PaddlePaddle 实现多种业务部署

PaddlePaddle 训练模式灵活，支持各种类型的模型训练。小规模的图像 OCR 模型，使用了单个机器上的多个 GPU，进行数据并行训练，通过框架特有的 Model Average 功能，能够显著提高模型的精度。PaddlePaddle 的分布式训练能够满足广告推荐业务，基于分布式的 lookup table，可以支持上亿的稀疏特征，使用上百台机器进行异步训练，训练后模型服务广告推荐。PaddlePaddle 还能在云端训练，用户可以非常灵活的提交训练任务，通过共享集群资源，弹性调度，提高了硬件资源的利用效率。

4. 基于 Caffe 满足目标检测实际业务需求

目标检测不仅在民用方面有着广泛地应用，在军事方面有着广泛地应用前景，例如精确制导、战场分析等。目前主流的目标检测算法主要基于深度学习模型，可以分为 two-stage（精度较高）和 one-stage（速度较快）两大类。针对图像中建筑、车辆、舰船等目标检测这一工程应用需求，基于 Caffe 框架的 Python 版 Faster R-CNN 算法可以有效地实现目标的分类和定位，较传统的检测算法在性能上有很大的提高。

Faster R-CNN 属于 two-stage 检测算法，在该类算法中具有里程碑意义。它的源码主要是基于 Caffe 框架，分为 Matlab 和 Python 两个版本。目前，大多数基于 Faster R-CNN 的检测算法会在 Python 版本源码的基础上进行二次开发。由于 Caffe 框架使用 Google 的 Protobuf 来定义超参数和网络模型，使得其在修改超参和网络模型时十分方便。针对不同场景的需求，可以根据任务选择已有的经典网络模型文件及对应的在 ImageNet 分类数据上的预训练模型参数，或者自定义合适的网络模型。同时，在原始超参的基础上，可以直接在文件中修改对应参数来进行实验对比及调优。此外，利用其提供的 Python 接口，可以容易地添加新的功能层，使得代码处于应用层而非框架层，在便于调试分析的同时减少了在框架底层添加新的功能层带来重新编译的时间消耗。在训练时，经过简单的修改，可以利用服务器上的多块 GPU，加快模型的训练速度。在网络模型文件中，可以通过重用 Blob 名称的方式来去掉一些中间变量，以减少整个模型占用

的 GPU 显存空间。Caffe 框架训练出来的模型采用键值对的方式进行储存，利用这种特性，既可以根据已用的预训练模型参数生成自定义网络模型的预训练参数（自定义与预训练模型结构有相似部分），也可以读取出每层的参数并转化成其他方式进行保存。除此之外，在开源社区，有大量基于 Caffe 框架实现的算法及对应的模型资源，从中不仅可以学习 Caffe 框架相关知识，还能不断拓展自身编程水平，从而促进自身业务发展。

三、 深度学习推断框架技术选型

（一）深度学习推断框架应用现状

1. 推断框架体系呈现碎片化

基于深度学习的推断计算相对训练过程计算量要小很多，但仍涉及到大量的矩阵卷积、非线性变换等运算，需要开发专用工具或框架实现业务部署，提升计算效率。总的来看，推断框架部署环境主要分为两类，一类是在手机终端以及不同嵌入式设备上部署的推断框架，以满足相关业务在限定设备性能及功耗等场景下的实际需求，业界开发了众多开源的推断软件框架供生产使用；一类是在服务器端部署的推断框架。服务器端推断框架受到训练框架软硬件生态影响较大，在技术选项方面有一定的延续性。服务器端推断框架限制条件较终端推断要求相对较少，但对于计算性能、业务实时性等要求更为严格。

TensorFlow Lite 可以运行在 Android 和 iOS 平台，结合 Android 生态的神经网络运行时能够实现较为高效的 AI 移动端应用速度。**Core ML** 是苹果公司开发的 iOS AI 软件框架，能够对接 Caffe、PyTorch、

MXNet、TensorFlow 等绝大部分 AI 模型，并且自身提供了常用的各种手机端 AI 模型组件，目前也汇集了众多开发者及贡献力量。**OpenCV** 也集成了 DNN 推断库，支持 Caffe、TensorFlow 等主流框架 AI 模型格式，并可以自由配置底层运算库（如 openblas，cudnn 等）和编译库，能够适配 GPU、Intel/AMD X86 和 ARM 等多类处理器，通过编译配置能够对云端和终端侧推断均提供支持。另外与 OpenCV 众多的图像处理库相结合，可以很方便实现一体化的图像类 AI 应用。**Paddle-mobile** 是百度自研的移动端深度学习软件框架，支持 PaddlePaddle 模型部署在移动端，拥有极高的性能表现，是一个支持多平台（iOS、Android）、多硬件（CPU、GPU、FPGA）的高性能框架。**NCNN** 是腾讯开源的终端侧 AI 软件框架，支持多种训练软件框架的模型转换，是主要面向 CPU 的 AI 模型应用，无第三方依赖具有较高的通用性，运行速度突出。**Caffe2go** 是最早出现的终端侧推断软件框架，能够让深层神经网络在手机上高效的运行。由于终端侧的 GPU 设备性能有限，Caffe2go 是基于 CPU 的优化进行设计。**TensorRT** 是英伟达（NVIDIA）开发的深度学习推断工具，已经支持 Caffe、Caffe2、TensorFlow、MXNet、PyTorch 等主流深度学习库，其底层针对 NVIDIA 显卡做了多方面的优化，可以和 CUDA 编译器结合使用。

产业界在手机端推断侧应用主要包括自动拍照、AR 手势识别、实时翻译以及目标识别等应用，对于实时性、多硬件平台及终端能耗有着特殊需求。由于端侧推断工具链需要与特定的芯片结合，目前最不完善。在智能手机上，Android 系统可以选择 TensorFlow Lite, Apple

系统可以选择 CoreML。而对于手机之外的端侧系统，目前产业界尚未形成成熟解决方案，需要从硬件加速器到软件工具链重新打磨。

产业界在服务器端推断框架由于训练框架生态影响，同样呈现趋同态势。如 TensorFlow 生态工具链相互搭配使用，能够显著减少模型优化部署等工作，云端训练模型能够快速交付至业务环境进行模型优化，Caffe/Caffe2、MXNet 以及 Keras 等框架也被广泛应用于云端推断。PaddlePaddle 基于云服务能够与硬件系统深度耦合，并且针对 CPU 硬件有专门优化，在如地图服务这种实时性要求较高的服务，能够有效提升推断速度。

当前，云端推断基于 GPU 的计算仍然是主流方案。由于其基于 GPU 提供了优化、编译、执行端到端解决方案，英伟达的 TensorRT 得到广泛使用。选择 TensorRT 的企业主要青睐于英伟达的软硬件生态，其在底层所做的大量性能优化工作能够有效降低单机服务成本，增加单机服务请求量计算。然而虽然该框架优化程度很高，但对算子的支持不够完善，在实际场景中，经常需要用户开发自定义算子。由于 TensorRT 闭源运行，企业开发进度受制于英伟达的进度，并不是一个完美的解决方案。

2. 推断框架滞后于实际需求

由于推断计算面向不同应用的具体要求及限制均不相同，不同应用场景底层硬件环境也千差万别，因此推断框架呈碎片化趋势，具有的共性功能较少，尚未形成业界需要的统一工具集。总体来看，目前推断框架落后于实际业务需求，主要体现在以下几个方面：

一是各推断框架间的兼容性缺失。嵌入式硬件对资源环境要求比较苛刻，训练框架并未关注推断在包括嵌入式场景等平台的实现，因此需要重构开发适应嵌入式场景的轻量级推断框架。**二是**推断框架的集成程度缺失。缺失主要体现在两个方面，一是统一接口适配所有的流行训练框架的接口性缺失；二是其他增强易用性以及可扩展性的工具集成。**三是**对多硬件并行处理方面的支持，如何针对推断业务进行多硬件并行优化尚未得到有效解决。**四是**对端侧不同硬件的优化及支持算子缺失，如 TensorFlow Lite 虽然在端测运行速度快，但是支持算子极少。

对于需要将训练好的神经网络模型部署在终端节点上的场景，神经网络部署/推断阶段，需要使用 AI 加速器硬件，主要有嵌入式 GPU、FPGA、AI 加速芯片三种方案，每一种部署/推断框架生态环境都未完全建成，企业只能选择 AI 加速器硬件厂商提供的配套软件工具，单个厂商的配套工具无法实现对多种训练框架神经网络模型的兼容，企业无法按照业务逻辑开展定制工作，企业只能被迫选择自研 AI 加速器及软件工具，造成研制进度缓慢、成本过高等一系列问题。

（二） 推断框架选型考虑

针对以上产业需求，现就训练框架选型提出以下指标体系供参考。推断框架基本功能应当包括模型加载转换组件、算子运算库和运算库依赖编译器几个部分，其中模型加载转换组件包括了对各类型模型文件的加载和到框架内部统一数据格式的转换，算子运算库包括了算子运算算法和面向硬件的运算优化，运算库依赖编译器主要是支持运算

库运算优化到目标硬件的编译实现。另外推断框架还可包括其他附加功能，如对模型的优化工具等。其中，推断框架中的模型加载转换组件主要体现了该推断框架对不同训练框架生成模型格式支持的广泛程度。算子运算库及其依赖的编译器主要体现了硬件支持类型和推断速度。

整个指标体系纵向分为四个大类，分别从易用性、性能、底层优化以及安全稳定性入手进行了分析，横向分为二级指标进行细化，每级指标是对前一级指标的细化。具体二级指标的细化会在同步开展的《深度学习技术选型评估规范（名称待定）》中做进一步的讨论。深度学习推断框架选型指标体系如表 2 所示。

表格 2 深度学习推断框架选型指标体系

一级指标	二级指标	三级指标
易用性	模型优化功能	支持模型加载
		框架数据格式
	通用模型表示	支持模型种类
	跨平台情况	支持哪些平台
性能	推断速度	计算时延
		实际业务性能
	启动时间	
	系统资源占用	内存、存储占用
底层优化	针对不同底层硬件的支持情况	FPGA/ASIC 支持（终端） GPU（云端）
	指令集优化	专属优化工具集（CPU 等）

		指令集支持（ARM INTEL SIMD 类指令集）
安全稳定性（终端）	模型加密	

易用性主要从三个维度进行描述，其中对于训练好模型的优化功能支持情况是最重要体现，包括模型压缩、加速算法组件以及超参数优化组件等。训练模型迁移至推断端实现涉及到了模型表示的转化，便捷的模型转化以及模型在端侧的便捷部署能够极大降低开发成本。框架在不同底层硬件的兼容可靠使用以及便利部署同样能够节省大量的开发技术门槛及业务开展时间。

端侧推断性能是业务开展的刚性需求，主要从计算推断速度、框架启动时间、系统资源占用以及功耗四个方面进行描述。计算推断速度决定了业务响应时间、业务吞吐等性能表现，不同功耗下推断计算速度是核心指标；框架启动时间对于低延迟业务也有重要影响；系统资源占用对于框架体量以及内存占用等要求严格，终端电池供应也对框架功耗提出了优化要求，需要在性能及资源占用方面找到合理平衡。

底层优化是端侧业务性能的重要保障，包括对于不同底层硬件的支持及提供专属优化工具集，保证相同框架及算法实现在不同硬件底层的性能表现。

在安全稳定性方面，实际业务开展中考虑到企业核心技术的保护，模型加密是重要技术保障，一般用于离线系统场景的部署，也是在实际开展相关业务时需考虑的重要因素。

（三） 产业优秀使用案例

目前产业界已基于开源推断框架开发打造了一系列便于开发者使用的开放能力平台，提升了 AI 应用效率，降低了 AI 部署门槛。

1. 面向移动终端的 HiAI 计算平台

HiAI 是面向移动终端的 AI 计算平台，构建三层 AI 能力开放：服务能力开放、应用能力开放和芯片能力开放。向开发者提供人工智能计算库及其 API，让开发者便捷高效的编写在移动设备上运行的人工智能应用程序。

HiAI Foundation 提供三大引擎包括在线推理、离线推理和端侧训练，满足多应用场景下的灵活性和高性能的不同需求。**易用性方面，**提供包括 Android Studio 插件在内的工具链和集成开发环境，让开发者可以基于现有熟悉的开发环境方便实现算法模型的集成；支持丰富的前端主流 Framework。**生态建设方面，**支持多框架下的主流算子，包括卷积、反卷积、池化、全链接，多种激活等，算子数量不断丰富，超过 140+。**性能方面，**专用神经网络处理单元 NPU 和 AI 指令集，快速转化和迁移已有模型，借助异构调度和 NPU 加速获得最佳性能，在知识模型处理、AI 专用指令集、大规模平行计算方面 NPU 具有显著优势，相比 CPU，有 50 倍效率和 25 倍性能的提升。**安全稳定性方面，**支持神经网络算法模型的加密接口，保护开发者知识产权。

2. 面向工业的轴承故障推断应用

INDICS 平台基于 TensorFlow 框架研发了一套滚动轴承的故障预测算法，通过对轴承设备振动信号进行处理与挖掘，以深度神经网络对滚动轴承的剩余寿命进行预测，该算法在现有设备数据上获得了较

高的准确率。尤其在轴承生命末期，可以提供不超过 2 小时的剩余寿命误差。可以有效的减少因设备损坏导致的非计划停产所带来的经济损失。INDICS 平台采用滚动轴承的振动数据基于 TensorFlow，开发了一套以神经网络进行剩余使用寿命预测和健康评估分析的算法模型。

在完成模型的设计与开发后，可将其部署到 INDICS 云端基于 TensorFlow 框架对其进行训练与预测，并以 API 的方式为用户提供相应的服务。用户可将设备的运转数据实时上传，并在平台 DaaS 层对数据进行相应的清洗、转换和预处理操作。接着数据导入人工智能引擎及 TensorFlow 框架，预测得出结果后为用户提供健康的显示及故障预警。

3. 企业研发助力推断框架性能显著提升

PaddlePaddle 的推断框架可以基于模型的图进行灵活的 fusion 优化，可以扩展优化策略。基于这个扩展，PaddlePaddle 的推断框架可以在几周时间提高模型的推断性能数十倍。

TensorFlow 的推断框架可以基于 TPU 使用低精度的 8-bit 进行高性能，低能耗的推断。相比基于传统 CPU 的 float32 的推断，能耗和性能都有数量级的优势。

四、 深度学习技术生态工具集

在实际工程应用中，人工智能算法可选择多种软件框架实现，训练和开发人工智能模型也可有多种硬件选项，这就开发者带来了不小的挑战。原因一是可移植性问题，各个软件框架的底层实现技术不同，

导致在不同软件框架下开发的模型之间相互转换存在困难；**二是**适应性问题，软件框架开发者和计算芯片厂商需要确保软件框架和底层计算芯片之间良好的适配性。解决以上两个挑战的关键技术之一就是**深度神经网络模型编译器及其上下游的工具集，它在传统编译器功能基础上，通过扩充面向深度学习网络模型计算的专属功能，以解决深度学习模型部署到多种设备时可能存在的适应性和可移植性问题，同时以中间件的方式提供包括模型压缩工具、量化工具、稀疏化工具、转换工具等软件工具。**

1. 深度学习编译中间件

传统编译器缺少对深度学习算法基础算子（卷积、残差网络及全连接计算等）的优化，且对人工智能多种形态的计算芯片适配缺失，针对人工智能底层计算芯片及上层软件框架进行适配优化的编译器需求强烈。目前业界主要采用依托传统编译器架构进行演进升级的方式来解决这个问题。

英伟达通过提供针对 LLVM 内核的 CUDA 源代码及并行线程执行后端打造了 CUDA 编译器。该编译器可支持 C、C++以及 Fortran 语言，能够为运用大规模并行英伟达 GPU 的应用程序加速。英特尔基于 LLVM 架构打造 Intel Inference Engine 计算库，为深度学习提供优化方法，可以处理所有的计算芯片抽象细节，目前已经开发了 TensorFlow/XLA、MXNet 和 ONNX 的软件框架桥梁；华盛顿大学基于 LLVM 架构打造了 NNVM/TVM 编译器，能够直接从多个深度学习前端将工作负载编译成为优化的机器代码。实现端到端的全面优化。

2. 数据及模型表示格式

在工程实践上，统一的中间表示层对模型进行表达及存储，输入数据格式以及模型表示规范也同样是重要的影响因素。

主流软件框架输入数据集格式各有不同。由于在训练中已经过清洗和标注的数据依然面临着多线程读取、对接后端分布式文件系统等实际操作问题，各主流人工智能软件框架均采用了不同的技术和数据集格式来实现此类数据操作。如 TensorFlow 定义了 TFRecord 、MXNet 及 PaddlePaddle 使用的是 RecordIO 等。

深度学习网络模型的表示规范分为两大阵营。**第一阵营**是 Open Neural Network Exchange（ONNX，开放神经网络交换），是一个用于表示深度学习模型的标准，可使模型在不同软件框架之间进行转移。ONNX 由微软和 Facebook 联合发布，该系统支持的软件框架目前主要包括 Caffe2，PyTorch，Cognitive Toolkit 和 MXNet，而谷歌的 TensorFlow 并没有被包含在内。**第二阵营**是 Neural Network Exchange Format（NNEF，神经网络交换格式），是由 Khronos Group 主导的跨厂商神经网络文件格式，计划支持包括 Torch, Caffe, TensorFlow, 等几乎所有人工智能软件框架的模型格式转换，目前已经有 30 多家计算芯片企业参与其中。

3. 深度学习可视化工具

作为提高 AI 开发效率的重要支持，可视化工具已经是 AI 训练中的重要工具主要用于展示训练过程中的统计数据（最值，均值等）变化情况、数据的分布图等。目前产业界主要是以 TensorBoard 提供

最强的可视化工具支持，其他 AI 平台通过社区贡献对接 TensorBoard 功能。百度的 VisualDL 也基本实现了 Tensorborad 类似功能而且兼容 PaddlePaddle, pytorch, mxnet, Caffe2 在内的大部分主流 DNN 平台。在图像数据集管理方面 google 开源了数据集可视化工具 Facets 帮助开发者洞察数据的分布情况。

4. 标准模型算法资源库

各大主流 AI 训练平台为了能吸引更多的开发者，不断推出和完善主流模型的直接调用能力，通常被称为 Model Zoo。TensorFlow 社区推出了一系列围绕 model 的项目，TensorFlow hub 为迁移学习(增量学习)提供前端模型支持、TensorFlow models 提供几十种常用模型的官方支持和社区研究模型关注度非常高、TensorFlow Tensor2Tensor 提供从数据集到训练模型的全流程案例。PyTorch、MXNet、Keras、Gluon、TensorLayer 各层次的平台也都从不同程度的提供主流模型算法的直接支持，使得开发者可以快速的使用。

5. 模型压缩优化工具集

对于训练模型的压缩以及优化的自动流程化操作业界已开展了相关探索，主要包括模型压缩/加速算法组件以及超参数优化组件两个部分。以腾讯发布的 PocketFlow 为例，其主要提供通道剪枝组件、权重稀疏化组件、权重量化组件、网络蒸馏组件、多 GPU 训练组件以及超参数优化组件，通过对这类算法组件的有效结合，能够实现精度损失更小、自动化程度更高的深度学习模型的压缩与加速。

五、 趋势展望

综上分析，未来软件框架开发及使用将主要聚焦以下问题：**一是安全问题**，在使用开源框架过程中无法保证数据的安全使用，需要做第三方的数据安全保密处理工作；**二是资源的共享问题**，一些在已有的开源技术进行封装以后能够有针对性的解决某些问题，但是目前这个封装后的资源由于各种问题无法实现资源的共享；**三是数据前处理**，在进行开源框架调用过程中并不能具直接使用工业数据，需要进行数据的清洗、甚至结构化关联等前期处理工作，但是目前框架不支持这些功能；**四是运算效率问题**，目前的开源框架在工业大数据处理问题上，运算效率偏低，分布式训练线性加速比表现很差，需要大量优化，运行在单机及集群上的相同算法开发原理不同；**五是定制化**，工业方面定制化要求较高，固定的框架结构无法满足众多的需求，同时框架对于自行开发的算法添加至算法库供后续批量使用的支持情况也较差，在工业方面需要具体问题具体分析，再搭建的过橙中需要视情况而定。**六是工程化特性缺失**，实际工程中所需的调测、训练、可视化、推断预测等功能现有框架实现缺失，如：深度学习训练前，进行的数据清洗；“数据集、算法、模型”之间关联关系记录以及模型发布等特性。

在编译器层面，各硬件厂商的中间表示层之争成为技术和产业发展的阻碍。目前业界并没有统一的中间表示层标准，并且模型底层表示、存储及计算优化等方面尚未形成事实标准，导致各硬件厂商解决方案存在一定差异，导致应用模型迁移不畅，提高了应用部署难度。

在实际使用中，传统行业面临开发门槛，图形化开发需求，更简

易 API 提供，更丰富的实际业务部署方式将是未来趋势。传统企业在人工智能技术方面前期积累不足，因此在使用深度学习框架进行深度学习模型训练及应用开发时，陷入无法快速开发产品的困境。在使用深度学习框架前，往往需要对技术人员做相应培训后才能投入开发工作。并且不同产品由于硬件载体限制需要不同语言将程序嵌入，传统行业在计算机基础技术方面也积累不足，虽然有丰富的 API 接口但还是很难完成多种类型开发语言的转化。

六、合作机构

本白皮书主要起草单位：

中国信息通信研究院

本白皮书写作工作中得到了以下单位的支持：

中兴通讯股份有限公司

华为技术有限公司

杭州海康威视数字技术股份有限公司

北京百度网讯科技有限公司

中国移动通信有限公司

中移物联网有限公司

中国电信股份有限公司广州研究院

中国联合网络通信有限公司

中国联通网络技术研究院

航天云网科技发展有限责任公司

中国航天科工集团第三研究院第三总体设计部

小米科技有限责任公司

中国人工智能产业发展联盟

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系人：王蕴韬

联系电话：010-68094605

网址：www.aiiaorg.cn