

AI 产品经理手册

[美] 艾琳·布拉西斯(Irene Bratsis) 著
张玉君 刘璐 译

清华大学出版社

北 京

北京市版权局著作权合同登记号 图字：01-2023-4311

Copyright © Packt Publishing 2023. First published in the English language under the title The AI Product Manager's Handbook: Develop a product that takes advantage of machine learning to solve AI problems (9781804612934).

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

版权所有，侵权必究。举报：010-62782989，beiqinquan@tup.tsinghua.edu.cn。

图书在版编目(CIP)数据

AI 产品经理手册 / (美) 艾琳·布拉西斯

(Irene Bratsis) 著；张玉君，刘璐译. -- 北京：清华大学出版社，2024. 10. -- ISBN 978-7-302-67432-0

I. F49-62

中国国家版本馆 CIP 数据核字第 20241CA344 号

责任编辑：王 军

封面设计：孔祥峰

版式设计：思创景点

责任校对：成凤进

责任印制：丛怀宇

出版发行：清华大学出版社

网 址：<https://www.tup.com.cn>，<https://www.wqxuetang.com>

地 址：北京清华大学学研大厦 A 座 邮 编：100084

社 总 机：010-83470000 邮 购：010-62786544

投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn

质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 装 者：定州启航印刷有限公司

经 销：全国新华书店

开 本：148mm×210mm 印 张：8.25 字 数：236 千字

版 次：2024 年 11 月第 1 版 印 次：2024 年 11 月第 1 次印刷

定 价：59.80 元

产品编号：103768-01

谨以此书献给那些有勇气追求并实现梦想的人……愿你们永葆此心！

—Irene Bratsis

译者序

嗨，亲爱的读者！

很高兴为大家带来这本《AI 产品经理手册》。AI 将颠覆所有行业，越来越多的企业开始拥抱 AI。AI 是 IT 从业者的必经之路，我们务必把握先机。

虽然 AI 在高速发展，但企业对 AI 的认知和对 AI 产品构建的认识仍然非常有限。对此，本书简单明了地介绍 AI 技术的基础知识，并从具体应用场景出发，讲解 AI 产品构建方法以及 AI 产品开发过程中的团队合作。本书适合 AI 领域的产品人员、运营人员、跨界者和创业者阅读，帮助他们应用 AI、发挥资源优势，并掌握 AI 赋能的实际场景。

能够参与本书的翻译工作，我深感荣幸。我先后从事过大数据与推荐系统、企业智能化转型、SaaS 智能化升级等工作，算是 AI 领域发展的一个见证人。本书内容和我的工作经历非常吻合。我希望通过我的努力，将作者的著作精华准确地传达给中文读者，并为大家提供一份关于 AI 产品经理的全面的、有价值的学习资料。同时，我也希望读者能够在阅读本书的过程中，深入理解 AI 产品的核心价值和前景，从而更好地为自己的职业生涯做出规划和决策。

我要感谢所有为《AI 产品经理手册》付出努力的人，包括出版社、编辑、校对和排版人员，他们的辛勤工作和专业精神，使本书得以顺利出版。同时，我也要感谢本书的另一位译者刘璐，她为本书的翻译付出了非常大的努力。最后，我要感谢我的家人们，能够理解和支持我，能够接受我将部分家庭生活时间分配到本书的翻译

工作中。

希望本书能够为你们带来启发和帮助，让我们一起加入 AI 的行列，创造更加美好的未来！

张玉君

关于作者

Irene Bratsis(艾琳·布拉西斯)是国际 WELL 建筑研究所(International WELL Building Institute, IWBI)的数字产品和数据主管。她拥有经济学学士学位，在学习数据科学和大数据分析方面的慕课(MOOC)后，还在 Thinkful 上学习了一门数据科学的课程。在加入 IWBI 前，Irene 曾担任特斯拉的运营分析师、Gesture 的数据科学家、Beekin 的数据产品经理、Tenacity 的产品主管。Irene 作为《纽约公约》的志愿者，担任“Women in Data”分会的联合负责人，积极投身于各种志愿者活动。她曾策划并组织过多个 AI 加速器项目，多次主持以“WaiTalk”(Women in AI)为主题的系列演讲活动。此外，她还每月组织一次关于数据和 AI 书籍的读书会。

关于审稿人

Akshat Gurnani 是一位在计算机科学和机器学习领域背景深厚的高级人才。他拥有计算机科学硕士学位，对各种机器学习技术和算法有深入的研究，拥有与自然语言处理、计算机视觉和深度学习相关的各种项目的工作经验。他在顶级期刊和会议上发表了多篇研究论文，并在该领域拥有良好的业绩。他对领域的最新发展保持浓厚的兴趣，并渴望继续研究 AI，为 AI 的发展做出贡献。

前言

现在，人们对 AI 充满了兴趣和看法。这些年，我亲身经历了 AI 的感受和认识的此起彼伏。我还是学生时，就对 AI 以及伴随而来的第四次工业革命感到无比激动和期待。然而，当我开始组织读书会，每月阅读有关 AI 的书籍，了解到对 AI 的偏见和依赖如何以或明显或隐蔽的方式威胁着我们的生活时，这份热情很快冷却下来。后来，我开始主持活动，邀请来自 AI 和机器学习领域的各方人士，他们不仅分享了如何在自己的工作中运用这项技术，还表达了关于 AI 如何影响人类未来的看法。

这让人回想起：每当科技发生飞跃式进步时，我们总会陷入一个重大争议。在了解了其中的风险后，我们是否敢于采用强大的技术？在我看来，我们别无选择，争议只是自欺欺人。AI 已经到来，悲观担忧并不能保护我们免受潜在的危害。潘多拉的盒子已经打开，当我们审视其中的内容时，会发现希望永不止息。

AI 会如实地反映出社会的偏见和不平等，而目前这种情况并不是喜闻乐见的。本书希望大家能够学会如何负责任地采用 AI，减少其可能带来的伤害，并使其最大限度地造福现代社会。我撰写这本关于 AI 产品管理的书，是为了帮助产品经理将模糊的想法变成真实的产品。在书中，我将尽力详细介绍如何以诚信的方式构思、构建、管理和维护 AI 产品，这是我目前对这个领域做出的最大努力。能够撰写本书也是我的荣幸。

本书读者对象

本书适合想要成为 AI 产品经理、AI 技术人员和企业家的读者，或者致力于将 AI 产品落地的读者。如果你已经在从事产品管理，并对构建 AI 产品感兴趣，那么本书应该对你有所帮助。如果你已经在某种程度上从事 AI 开发工作，并希望将这些概念引入产品管理，扮演商业化的角色，那么本书也适合你。虽然书中的某些章节更侧重于技术，但书中所有技术内容都是入门级的，适合所有人阅读。

本书内容

第 1 章“构建 AI 产品所需要的基础设施和工具”：概述管理 AI 产品的基本概念和基础设施。

第 2 章“AI 产品的模型开发和维护”：深入探讨模型开发和维护的细节。

第 3 章“机器学习和深度学习深入剖析”：详细讨论传统机器学习和深度学习算法之间的差异及其用例。

第 4 章“AI 产品的商业化”：讨论了在市场上 AI 产品的不同领域，以及有助于商业化的伦理和关键因素。

第 5 章“AI 转型及其对产品管理的影响”：探讨未来 AI 应用融入主要市场领域的方式。

第 6 章“了解 AI 原生产品”：概述打造 AI 原生产品所需要的战略、流程和团队建设。

第 7 章“机器学习服务产品化”：探讨从零开始构建 AI 产品时可能遇到的困难和挑战。

第 8 章“面向垂直领域、客户和同行群体的定制化”：讨论 AI

产品在不同垂直领域、客户类型和同行群体中的变化和发展。

第 9 章“产品的宏观 AI 和微观 AI”：概述利用 AI 的各种大大小小的方式，以及一些最成功案例和常见错误。

第 10 章“性能基准、增长策略和成本”：解释在产品层面而非模型性能层面衡量产品成功的标杆。

第 11 章“AI 的浪潮”：重新审视第四次工业革命的概念，并为目前尚未采用 AI 的产品提供蓝图。

第 12 章“行业发展趋势与洞察”：深入探讨 AI 在不同行业的发展趋势，及知名研究机构的研究成果。

第 13 章“将产品演进为 AI 产品”：本章是一个实用指南，介绍如何提供 AI 功能，并优化现有产品的逻辑，以成功地将产品升级为具有商业价值的 AI 产品。

参考文献扫描封底二维码下载。

目 录

第 I 部分 AI 的基础：术语、基础设施、AI 类型以及 AI 产品案例

第 1 章	构建 AI 产品所需要的基础设施和工具	3
1.1	定义：什么是 AI，什么不是 AI	4
1.2	机器学习与深度学习的区别	6
1.2.1	机器学习	7
1.2.2	深度学习	7
1.3	机器学习的学习类型	9
1.3.1	监督学习	9
1.3.2	无监督学习	11
1.3.3	半监督学习	12
1.3.4	强化学习	13
1.4	流程顺序：最佳流程及其过程	13
1.4.1	步骤 1：数据可用性和集中化	14
1.4.2	步骤 2：持续维护	14
1.5	数据库基础：数据库、数据仓库、数据湖和湖仓	15
1.5.1	数据库	16
1.5.2	数据仓库	16
1.5.3	数据湖(和湖仓)	17
1.5.4	数据流水线	17
1.6	项目管理：IaaS	18

1.7	部署策略：部署与应用模型	19
1.7.1	影子部署策略	20
1.7.2	A/B 测试模型部署策略	20
1.7.3	金丝雀部署策略	21
1.8	AI 领域的成功案例：构建基础设施的成功案例	21
1.9	AI 的潜力：AI 的发展方向	23
1.10	本章小结	24
第 2 章	AI 产品的模型开发和维护	27
2.1	了解 NPD 的各个阶段	28
2.1.1	阶段 1：发现	28
2.1.2	阶段 2：定义	28
2.1.3	阶段 3：设计	29
2.1.4	阶段 4：实施	29
2.1.5	阶段 5：市场营销	30
2.1.6	阶段 6：培训	30
2.1.7	阶段 7：发布	31
2.2	模型类型：从线性回归到神经网络	31
2.3	模型训练：为上线做准备	33
2.4	模型部署：交付研发结果	37
2.5	模型测试和故障排除	39
2.6	模型刷新：模型更新频率的伦理规范	41
2.7	本章小结	44
第 3 章	机器学习和深度学习深入剖析	47
3.1	传统的 AI：机器学习	48
3.2	新兴的 AI：深度学习	49
3.2.1	隐藏的影响	51
3.2.2	深度学习简史	52

3.2.3 神经网络的类型·····	54
3.3 新兴技术：相关的辅助技术·····	61
3.4 可解释性：伦理、注意事项和责任·····	62
3.5 准确性：为成功做准备·····	63
3.6 本章小结·····	64
第 4 章 AI 产品的商业化·····	67
4.1 成功的 B2B 产品案例·····	68
4.2 成功的 B2C 产品案例·····	70
4.3 蓝海产品案例·····	71
4.4 红海产品案例·····	73
4.5 差异化、颠覆性和主导性战略产品案例·····	75
4.5.1 主导性战略·····	76
4.5.2 颠覆性战略·····	77
4.5.3 差异化战略·····	77
4.6 本章小结·····	79
第 5 章 AI 转型及其对产品管理的影响·····	81
5.1 财富和价值：AI 革新经济体系·····	83
5.2 商品和服务：商业 MVP 的增长·····	85
5.3 政府和自治：AI 塑造社会的边界和自由·····	87
5.4 疾病和健康：AI 和纳米技术在医疗领域的应用·····	90
5.5 基本需求：AI 向善·····	92
5.6 本章小结·····	93

第 II 部分 构建 AI 原生产品

第 6 章 了解 AI 原生产品·····	97
6.1 AI 产品开发的阶段·····	98
6.1.1 阶段 1：创意·····	98

6.1.2	阶段 2：数据管理	99
6.1.3	阶段 3：研发	100
6.1.4	阶段 4：部署	101
6.2	AI/ML 产品团队的最佳组合	102
6.2.1	AI 产品经理	102
6.2.2	AI/ML/data 策略师	103
6.2.3	数据工程师	103
6.2.4	数据分析师	103
6.2.5	数据科学家	104
6.2.6	机器学习工程师	104
6.2.7	前端/后端/全栈工程师	105
6.2.8	UX 设计师/研究员	105
6.2.9	客户成功	106
6.2.10	市场/销售/市场推广团队	106
6.3	技术栈投资	107
6.4	AI 服务产品化：AI 产品管理的不同之处	108
6.5	AI 定制化：针对行业和客户群体的考虑	109
6.6	销售 AI：产品管理与销售	111
6.7	本章小结	112
第 7 章	机器学习服务产品化	113
7.1	AI 产品与传统软件产品的差异	113
7.1.1	相似之处	114
7.1.2	差异之处	115
7.2	B2B 与 B2C：产品化的商业模式	121
7.2.1	领域知识：了解市场需求	121
7.2.2	实验：探索群体的需求	123
7.3	一致性和 AIOps/MLOps：信赖与信任	125

7.4	性能评估：测试、重新训练和超参数调整	126
7.5	反馈循环：建立关系	127
7.6	本章小结	128
第 8 章	面向垂直领域、客户和同行群体的定制化	129
8.1	特定领域的 AI 定制化	130
8.1.1	了解市场	132
8.1.2	产品设计与市场服务	133
8.1.3	制定 AI 产品战略	134
8.2	AI 产品高度渗透的垂直领域	137
8.2.1	金融科技	137
8.2.2	医疗保健	139
8.2.3	网络安全	140
8.3	用户行为分析	141
8.4	AI 产品的价值指标	141
8.4.1	OKR	142
8.4.2	KPI	142
8.4.3	技术指标	144
8.5	思想引领：向同行学习	144
8.6	本章小结	145
第 9 章	产品的宏观 AI 和微观 AI	147
9.1	宏观 AI：基础和范畴	148
9.1.1	机器学习	149
9.1.2	计算机视觉	151
9.1.3	自然语言处理	151
9.1.4	深度学习	152
9.1.5	机器人技术	153
9.1.6	专家系统	155

9.1.7	模糊逻辑/模糊匹配·····	156
9.2	微观 AI：功能层面·····	156
9.2.1	机器学习(传统机器学习/深度学习/计算机视觉/自然语言处理)·····	157
9.2.2	机器人技术·····	158
9.2.3	专家系统·····	159
9.2.4	模糊逻辑/模糊匹配·····	160
9.3	成功案例：振奋人心的示例·····	161
9.3.1	Lensa ·····	161
9.3.2	PeriGen·····	162
9.4	挑战：常见的陷阱·····	163
9.4.1	伦理·····	163
9.4.2	性能·····	165
9.4.3	安全·····	165
9.5	本章小结·····	167
第 10 章	性能基准、增长策略和成本·····	169
10.1	价值指标：北极星指标、KPI 和 OKR 的指南·····	170
10.1.1	北极星指标 ·····	171
10.1.2	KPI 和其他指标标准·····	175
10.1.3	OKR 和产品策略 ·····	177
10.2	增长黑客：以产品为导向的增长·····	178
10.3	技术栈：及时反馈·····	180
10.3.1	客户数据平台(CDP)·····	181
10.3.2	客户参与平台(CEP)·····	182
10.3.3	产品分析工具 ·····	183
10.3.4	A/B 测试工具·····	184
10.3.5	数据仓库 ·····	185

10.3.6	商业智能(BI)工具	185
10.3.7	增长黑客工具	186
10.4	成本管理和定价: AI 是昂贵的	187
10.5	本章小结	188

第Ⅲ部分 在现有产品中融入 AI

第 11 章	AI 的浪潮	193
11.1	演进或淘汰: 变化是唯一不变的	194
11.2	第四次工业革命: 技术的进步和变迁	197
11.2.1	与咨询顾问合作	199
11.2.2	与第三方合作	199
11.2.3	首次招聘	200
11.2.4	第一个 AI 团队	201
11.2.5	无代码工具	201
11.3	摆脱恐惧: 收获大于代价	202
11.4	本章小结	206
第 12 章	行业发展趋势与洞察	207
12.1	最具增长潜力的领域: Forrester、Gartner 和麦肯锡的研究	208
12.1.1	嵌入型 AI: 应用和整合案例	208
12.1.2	伦理型 AI: 责任和隐私	210
12.1.3	创作型 AI: 生成和沉浸式应用	211
12.1.4	自主 AI 开发: 图灵机器人	212
12.2	AI 采用的趋势: 让数据说话	213
12.2.1	整体趋势	214
12.2.2	嵌入型 AI: 应用和集成的用例	215
12.2.3	伦理型 AI: 责任与隐私	216

12.2.4	创作型 AI：生成和沉浸式应用	217
12.2.5	自主 AI 开发：图灵机器人	217
12.3	最容易实现的目标：快速实现 AI 的成功	218
12.4	本章小结	220
第 13 章	将产品演进为 AI 产品	221
13.1	韦恩图：可能性和概率	222
13.1.1	清单 1：价值	223
13.1.2	清单 2：范围	224
13.1.3	清单 3：影响范围	226
13.2	数据为王：公司的血液	227
13.2.1	准备和研究	228
13.2.2	良好的合作关系	228
13.2.3	基准测试	229
13.2.4	数据团队	230
13.2.5	定义成功	231
13.3	竞品分析：关注竞争对手	232
13.4	产品战略：建立适合组织的蓝图	233
13.4.1	产品战略	234
13.4.2	产品路线图	237
13.5	红旗和绿旗：要注意和警惕的事项	239
13.5.1	红旗：警告信号	239
13.5.2	绿旗：积极信号	240
13.6	本章小结	242
	参考文献(扫描封底二维码下载)	243

第 I 部分

AI 的基础：术语、基础设施、AI 类型以及 AI 产品案例

如果 AI 产品经理想要将产品商业化，他们需要对 AI 以及所有 AI 成功落地所需要的各种组件有全面的了解。

本书的第 I 部分由五章组成，包括 AI 的定义和相关术语，以及如何在组织中构建基础设施来支持 AI 成功落地。本部分还介绍如何从维护的角度支持 AI 项目，如何在机器学习(Machine Learning, ML)和深度学习(Deep Learning, DL)领域选择最佳路径，以及如何了解当前和未来 AI 产品的发展。

通过本部分的学习，可以了解 AI 的相关术语和组成要素，从投资的角度了解 AI 实施的意义，了解如何可持续地维护 AI 产品，以及如何选择最适合产品和市场的 AI 类型。此外，还可以学习如何理解构思和构建最小可行产品(Minimal Viable Product, MVP)的成功因素，以及如何打造真正能满足市场需求的产品。

本部分包括以下各章。

- 第 1 章：构建 AI 产品所需要的基础设施和工具

- 第 2 章：AI 产品的模型开发和维护
- 第 3 章：机器学习和深度学习深入剖析
- 第 4 章：AI 产品的商业化
- 第 5 章：AI 转型及其对产品管理的影响

第1章

构建AI产品所需要的基础设施和工具

随着对新的产品概念、组织方式和行业发展的深入探索，AI的发展速度也在不断加快。我们生活的方方面面都将以某种方式受到 AI 的影响。希望通过阅读本书，读者对于在正在支持的或将要构建的产品中采用 AI，能有更多的了解和信心。

本书的第 I 部分将对整个 AI 领域进行概述，并介绍 AI 相关术语、基础设施、各种 AI 算法和成功的产品案例。阅读本部分的内容，可以了解在制定 AI 战略时需要考虑的各种因素，无论创建一个 AI 原生产品还是为现有产品添加 AI 功能。

管理 AI 产品是一个高度迭代的过程，产品经理的工作是帮助组织发现基础设施、训练和部署工作流的最佳组合，以在目标市场上取得最大成功。AI 产品的性能和成功的关键在于管理 AI 流程所需要的基础设施，需要充分理解，才能将其输出集成到产品中。本章将介绍数据库、工作台、部署策略和AI项目的管理工具等，以及如何评估产品的效能。

本章对第 I 部分中的后续各章提供整体的概览，更重要的是对一些术语的定义进行解释。在当今的竞争环境中，都以 AI 为主要营销卖点，很少使用这些术语。如今，几乎每个产品都标榜自己是 AI 产品，导致 AI 这个词也被滥用并变得含糊不清。虽然这种情况短期内不会改变，但随着消费者和客户越来越了解 AI、机器学习和数据科学的能力与具体细节，我们可以更清楚地看到这些产品是如何构建和优化的。无论你是想要从 0 到 1 创建一个 AI 产品，还是想要将 AI 应用到现有产品，理解 AI 的背景知识都非常重要。

本章主要介绍以下主题。

- 定义：什么是 AI，什么不是 AI
- 机器学习与深度学习的区别
- 机器学习中的学习类型
- 流程顺序：最佳流程及其过程
- 数据库基础：数据库、数据仓库、数据湖和湖仓
- 项目管理：IaaS(基础设施即服务)
- 部署策略：部署与应用模型
- AI 的成功案例：构建基础设施的成功案例
- AI 的潜力：AI 的发展方向

1.1 定义：什么是 AI，什么不是 AI

1950 年，数学家艾伦·图灵(Alan Turing)在他的论文“Computing Machinery and Intelligence-Can machines think?”中提出了一个问题：机器能思考吗？至今，人们仍在探讨这个问题。根据不同的观点，AI 可以有許多不同的定义。在互联网中，AI 的应用领域非常广泛，从医疗保健和金融领域使用的专家系统，到人脸识别、自然语言处理和回归模型等。本章将介绍市场上一些新兴产品中的 AI 应用。

为了使 AI 应用在各行各业的产品中，本书将主要关注机器学

习和深度学习模型的使用。这些模型在实际生产中经常使用，几乎覆盖了所有市面上的 AI 产品。我们使用 AI/ML 作为总称，涵盖一系列机器学习应用，并将介绍大多数人了解的机器学习的主要领域，如深度学习、计算机视觉、自然语言处理和人脸识别。这些应用是 AI 领域中最常见的应用方式，熟悉这些应用对于即将进入 AI 领域的产品经理来说非常有帮助。如果你希望从其他产品管理背景进入 AI 领域，希望本书能帮你选择最适合自己的 AI 领域。

本章还会解释什么是机器学习，什么不是机器学习。简而言之：如果一台机器通过学习以往的行为提高其准确率，那就是机器学习！学习是其中的核心要素。虽然没有哪个模型是完美的，但模型可通过学习获得很多能力。每个模型都需要调优超参数(hyperparameter tuning)，每个模型的使用都有一定的性能范围。数据科学家和机器学习工程师在研究这些模型时，可以对基准性能进行评估，并研究如何改善性能。如果机器的内核是固定的硬编码的规则，就不能算是机器学习。

AI 是计算机科学的一个分支。程序员所做的实际上是给计算机设定一系列指令，让它按照指令的要求执行。如果程序只是按照预先设定的指令执行，不能从过去的经验中学习，就不能称为机器学习。在过去，规则引擎或专家系统等程序也被认为是 AI 的一种形式，但它们并非机器学习，因为它们仅仅是在模仿人的工作，本身并没有自主学习或改变的能力。

我们现在处于一个 AI 采用的困惑时期。一方面，AI 尚未普及，关于什么样的产品才能称为 AI 没有明确的定义；而在市场上还没有对 AI 的明确解释的情况下，营销人员纷纷给产品贴上 AI 标签。这让消费者和技术人员都感到困惑。相信在看到 AI 产品的广告时，你也有这种感觉。

另一方面，对于大多数人来说，一提到 AI，就会联想到 20 世纪 80 年代的《终结者》系列电影以及其他描述科技灭世的未来主义作品。虽然 AI 确实可能会带来许多危害，但这种描绘所代表的

是强人工智能或**通用人工智能(Artificial General Intelligence, AGI)**。而目前的 AI 是人工狭窄智能或**狭义人工智能(Artificial Narrow Intelligence, ANI)**，离实现 AGI 还有很长的路要走。

ANI 通常被称为弱人工智能，现在看到的、带有 AI 的产品，一般指的就是 ANI。顾名思义，ANI 是 AI 的狭窄应用。它可能擅长与你对话、预测未来价值或组织事务。它也许是某些领域的专家，但它的专长无法延伸到其他领域。如果能够延伸，它就不仅仅是 ANI 了。与人类智能相比，这些 AI 的主要领域被称为强人工智能和弱人工智能。即使是目前最具代表性的对话型 AI，看起来非常逼真，实际上也只是一种虚拟的智能。事实上，目前存在的所有 AI 都属于弱人工智能或者 ANI。《终结者》离我们仍然很遥远，也许永远无法实现。

网上经常可以看到关于 AI 具有意识或对人类怀有敌意的帖子，本书想要明确表明以下观点：AGI 并不存在，没有所谓有意识的 AI。不过，这并不意味着 AI 在现实中不会对人类造成伤害。注意，不合乎伦理、草率地采用 AI 已经给人们的生活带来了或多或少的不便或困扰。符合伦理并负责任地构建 AI 仍然任重而道远。虽然 AI 系统不会有意地破坏人类社会，但如果没有经过充分测试、适当管理和偏见审查，ANI 应用有可能对人们的生活造成真正的伤害。

目前，机器能像人类一样思考吗？还不能。将来会吗？我们希望不会。我个人认为，通过 AI，人类所面临的痛苦和困扰将在我们这一代结束。我们深信：无论是我们生活中最严重的问题，还是我们最疯狂的好奇心，都将因 AI 和机器学习得到显著改变。

1.2 机器学习与深度学习的区别

作为产品经理，需要与技术团队建立牢固的信任关系，这样才能一起打造一款出色的产品，才能在技术上和功能上达到最佳水平。阅读本书时，你可能已经了解过机器学习和深度学习这些词。接下

来将介绍一些机器学习与深度学习的基础知识，并在第 3 章更详细地解释这些概念。

1.2.1 机器学习

机器学习(ML)主要由两个关键部分组成：所使用的模型和用于学习的训练数据。这些数据是历史数据点，能够为机器提供一个学习的基础。理论上，每次重新训练模型时，模型的性能都会有所提升。如何选择、构建、调整和维护这些模型以实现最佳性能，是数据科学家和机器学习工程师的工作任务。产品经理的任务是将这些符合性能的成果用于优化产品体验。AI 产品管理中，产品经理需要与数据科学家和机器学习团队密切合作。

作为 AI 产品经理，需要与不同的团队合作。根据组织的结构，可能会与数据科学家和开发人员合作，一起部署机器学习；或者与机器学习工程师合作，他们既能训练和维护模型，又能将其应用到实际生产中。总之，你必须与所有这些团队以及 DevOps 保持密切的合作关系。

所有机器学习模型都可以分为以下四种主要的学习类型：

- 监督学习
- 无监督学习
- 半监督学习
- 强化学习

这是机器学习的四个主要类型，每个类型都有其特定的模型和算法，并通过不同的方式使用。学习类型与数据是否被标注以及对表现良好的模型的奖励方法有关。这些学习类型适用于所有机器学习模型和深度学习模型。在接下来的章节中，将更深入地探讨机器学习中的学习类型。

1.2.2 深度学习

深度学习(DL)是机器学习的一个分支，但这两个术语通常被当

作几乎完全不同的概念。原因是深度学习基于神经网络算法，机器学习则通常基于神经网络外的其他算法。在前面介绍机器学习的内容中，讨论了如何处理数据，使用数据来训练模型，并预测未来数据。每次使用模型时，都可以通过它与正确答案的差异来评估模型的准确性，并反复迭代，直到获得足够好的模型。每次迭代，都基于具有某些模式或特征的数据构建和训练模型。

在深度学习中，处理数据的过程与机器学习类似，但深度学习的关键不同之处在于，它基于分层系统，通过**特征学习(feature learning)**或**特征工程(feature engineering)**提取和学习数据中的模式或特征。接下来的内容中，将详细介绍深度学习使用的各种算法，以及它们之间的差别。在深入了解不同类型的机器学习的同时，也可以了解构成 AI(机器学习和深度学习)的主要领域的各种模型的分类方式。出于营销的目的，对于深度学习算法，也会使用机器学习、深度学习/神经网络或者 AI 这个总括性概念表述。

产品经理需要理解这些术语在实践和模型层面上的实际意义及两者的区别，并且能够以通俗易懂的方式向非技术人员解释。产品经理的工作是在工程团队的构建内容和营销团队传达的信息之间建立联系。听到**黑匣子模型(black box model)**这个术语时，它指的是神经网络模型，即深度学习。原因是深度学习工程师通常无法确定其模型是如何得出某些结论的，从而导致模型的运作方式变得不透明。这种不透明性是双面的，既存在于工程师和技术人员本身，也存在于下游的客户和用户，他们在无法理解模型如何做出决策的情况下，明显感受到模型带来的影响。这正是因为深度学习神经网络模拟了人类思维方式中多层神经网络的结构。

对于产品经理来说，深度学习可解释性方面的问题在于我们几乎无法理解模型为何以及如何得出结论，而且根据产品的具体情境，可解释性的侧重点可能有所不同。另一个困难在于，这些模型本质上是自主学习的，不需要工程师选择最相关的特征数据；神经网络本身会进行特征选择。它几乎不需要工程师的干预就能学习。机器

学习模型可以理解为“做什么”，而学习类型就是“怎么做”的。提醒一下，接下来将介绍的学习类型(无论是监督学习、无监督学习、半监督学习还是强化学习)适用于深度学习和传统机器学习模型。

1.3 节将介绍机器学习中的不同学习类型。

1.3 机器学习的学习类型

本节将介绍监督学习、无监督学习、半监督学习和强化学习之间的区别，以及如何应用这些学习类型。同样，学习类型主要与是否对数据进行标注以及模型奖励的方法有关。模型选型的最终目标是能够为产品提供所需要的性能和可解释性。

1.3.1 监督学习

如果数据是由人工标记的，并且机器也在试图正确地标注当前或未来的数据点，那么这就是监督学习。在监督学习中，我们知道正确答案，因此可以看到它们与正确答案的差距，并且我们不断地训练或重新训练模型，直到达到令人满意的准确度水平。

监督学习模型的应用包括：分类模型，例如像垃圾邮件过滤器一样对数据进行分类；回归模型，寻找变量之间的关系以预测未来事件和发现趋势。记住，所有模型都只能在一定程度上发挥作用，因此需要不断地训练和更新模型，而 AI 团队通常会使用集成建模或尝试各种模型并选择性能最佳的模型。无论采用哪种方式，模型都不是完美的。但只要通过足够的引导，它会逐渐接近你想要的效果。

以下是在生产过程中可能会使用的、常见的监督学习模型/算法。

- **朴素贝叶斯分类器(Naive Bayes Classifier):** 该算法将数据集中的每个特征都作为其独立变量，从而试图在没有关于数据的任何假设的情况下通过概率找到关联性。它是最简单

的算法之一，其简单性实际上正是使它在分类中如此成功的原因。它通常用于二进制值，例如尝试判断某个邮件是否为垃圾邮件。

- **支持向量机(Support Vector Machine, SVM):** 该算法也主要用于分类问题，并将尝试将数据集分为两类，以便你可以使用它对数据进行分组，并尝试预测未来数据点将落在哪个分类中。如果没有看到数据之间的明显分组，则可以添加更多维度直到明显地看到分组。
- **线性回归模型(Linear Regression Models):** 这种模型自 20 世纪 50 年代以来就存在了，是用于回归问题(如预测未来数据点)的最简单模型。它们基本上使用数据集中的一个或多个变量来预测因变量。该模型的线性部分试图找到最佳直线来拟合数据，这条直线是用来做预测的。在这里，同样看到相对简单的模型因其多功能性和可靠性而被广泛使用。
- **逻辑回归(Logistic Regression):** 该模型的工作方式类似于线性回归，包含自变量和因变量，但它不是预测数值，而是预测未来的二元分类状态，例如某人未来是否可能贷款违约。
- **决策树(Decision Trees):** 该算法既适用于预测分类变量，也适用于预测数值变量，因此可用于预测未来状态或未来价格等各种机器学习问题。由于这种独特的灵活性，决策树通常用于解决各种问题，这也是其受欢迎的原因之一。之所以称之为“树”，是因为其中的节点和分支结构就像树一样，它们可以起到流程图的作用。决策树通过学习过去数据流转状态来预测未来值。
- **随机森林(Random Forest):** 该算法是在之前的决策树基础上构建的，也用于解决分类和数值问题。其工作方式是将数据集分成不同的随机样本集合，为每个样本集合创建决策树，然后对其预测取平均值或按多数表决(取决于你是将其

用于分类还是数值预测)。随机森林的决策过程比较难理解，因此如果对可解释性没有特别要求，可以使用。

- **K 近邻算法(K-Nearest Neighbors, KNN):** 该算法专门处理分类和数值预测，因此它寻找未来状态并以组的形式提供结果。模型的工作原理是对数据进行分组，确定数据与其邻近组共享的特征，并根据这些邻近组为未来值提供最佳预测值，而组中数据点的数量由工程师/数据科学家设置。

现在已经介绍了监督学习，接下来介绍无监督学习。

1.3.2 无监督学习

在数据没有标记的情况下，使用机器对数据进行标记并查找尚未发现的模式，就是无监督学习。实际中，要么知道正确答案，要么不知道，这也是区分机器学习算法所属的学习类型的方法。可以想象，无监督学习模型的结果会让人有一定的疑虑，因为它可能找到的分类方式并不一定有用或准确。同时，无监督学习模型还需要大量的数据来训练，因为如果在小数据样本中找出模式，可能会极不准确。随着它训练的数据越来越多，其性能会改善，但再次强调，这里没有标准答案。

无监督学习模型的应用包括聚类和降维。聚类模型将数据分成不同的组别或类别。这种模型可以用于医学试验或药物研发等领域，通过寻找数据中的模式和关联，发现可能隐藏的信息。而降维则是简化数据集，去除对性能贡献较小的特征，从而将有用的信号与噪声区分开，使最重要的特征能够更好地提升性能。

以下是在生产过程中可能会使用的、常见的无监督学习模型/算法的列表。

- **K-means 聚类:** 这种算法将数据点分组在一起，以更好地看到模式(或簇)，但它也寻找最优的簇数量。这是一种无监督学习，因此模型寻找可以从中学到的模式，因为它没有从

使用它的工程师那里得到任何信息(或监督)。此外，簇数量是一个超参数，你需要选择最佳的簇数量。

- **主成分分析(Principal Component Analysis, PCA)**: 使用无监督学习处理大数据集的最大问题往往是有太多不相关的数据，以至于无法找到有意义的模式。这就是人们经常使用 PCA 的原因，因为它是一种很好的降维方法，可以在不丢失或不丢弃有用信息的情况下减少维度。这对于大规模数据集特别有用，例如在基因组测序或药物发现试验中寻找模式。

接下来，介绍半监督学习。

1.3.3 半监督学习

在理想的情况下，我们将拥有大规模的标记良好的数据集，用来创建最优模型，而不会出现过拟合的情况。过拟合(Overfitting)指的是创建和调整的模型对目前拥有的数据集过度贴合，即它在当前特定数据集上进行了过度优化，反而导致在未来不同的数据上表现不佳。这是数据科学中的常见问题。然而，在现实世界中，常常面临标记数据不足或完全没有足够数据的情况。这时，半监督学习就派上了用场。通过提供一些标记的数据集，并加入一些未标记的数据集，可以引导模型朝着正确的方向努力寻找模式。

半监督学习虽然无法像监督学习那样具有非常准确的结果，但为模型提供了一些有用的线索，帮助模型组织结果，使其更容易找到通向正确答案的路径。

假设你需要一个能够有效检测照片或语音中的模式的模型。你可以对其中一部分样本数据进行标记，然后观察随着未标记样本的增加性能如何变化。在半监督学习中，可以使用多个模型。这个过程类似监督学习，监督学习通过标记的数据集进行学习，以便准确知道它与正确答案的偏差。监督学习和半监督学习的主要区别在于，半监督学习要预测一部分新的未标记数据，然后基于标记数据检查

其准确性。将未标记的新数据点添加到训练集中，可以使模型在已经正确识别的数据上进一步训练。

最后，简要介绍一下强化学习。

1.3.4 强化学习

在机器学习中，有一种通过不断试错来学习的方法，称为强化学习(Reinforcement Learning)。强化学习从过去的经验中学习，并根据自身的表现不断调整策略，以达到最佳效果。强化学习可以类比为根据权重和奖励强化正确结果的一种系统。模型会尝试优化奖励，并随着时间的推移逐渐提升其性能。在实际应用中，强化学习在机器人领域得到广泛应用，例如训练机器人理解如何操作并适应现实中各种不可预测的情况。

现在，已经讨论并了解了不同类型的机器学习类型，接下来继续介绍机器学习过程的最佳流程。

1.4 流程顺序：最佳流程及其过程

与犹豫不决的竞争对手相比，致力于通过 AI 和机器学习创造价值的公司可以获得很多收益。麦肯锡全球研究所预测：“到 2025 年，完全将 AI 纳入价值创造工作流程中的公司，现金流增长率将超过 120%，并主导 2030 年的全球经济。”但是，拥抱 AI 并将其应用于产品或企业内部是一项非常复杂、技术债务重、成本很高的任务。一旦确定了模型和应用场景，将 AI 真正应用到生产环境中会遇到种种困难，这是许多企业面临的挑战，尤其是对于那些本身并非科技行业但要拥抱 AI 的企业。实现流程运营、更新模型、保持数据的新鲜和清洁、组织实验、进行验证、进行测试和相应的存储等，都是复杂而关键的步骤。克服这些挑战，AI 才能成功应用到业务中。

整个流程存在着不同层次的复杂性，但基本组成部分相同。为

为了更好地理解整个过程，我们将按如下步骤介绍。一旦你完成基础工作，并确定最适合你的用例的模型和算法，就可以开始完善 AI 系统的管理流程了。

1.4.1 步骤 1：数据可用性和集中化

首先，需要一个中央存储位置，用来存储 AI/ML 模型和算法训练学习所需要的数据。根据你投入的数据库或所使用的现有系统，你可能需要一个 ETL 流水线和数据工程来处理数据，确保各层级的数据和元数据可供生产中的 AI/ML 模型使用，并从中获得有价值的洞察。

这相当于创建为 AI/ML 系统提供数据的流水线。

AI 依赖于数据，如果数据传输过程繁琐或缓慢，那么在后续的生产过程中就会遇到问题。选择合适的数据存储方式本身就有一定难度。随着规模的扩大，无法预知技术框架会如何演变，因此选择一种性价比高且可靠的解决方案本身就是一项挑战。我们曾在一家网络安全公司工作，随着客户数量的增加，我们注意到某些面向客户的仪表盘的加载速度明显变慢。其中一部分原因是客户数量的增加及元数据过多，超出了原本的数据流水线的承载能力。

1.4.2 步骤 2：持续维护

现在，你已经拥有了模型和算法，并选择了一个数据传输系统供它们使用。你需要持续维护这个系统。在 DevOps 中，这被称为持续集成(Continuous Integration, CI)/持续交付(Continuous Delivery, CD)。稍后将介绍 AI 运营(AI Operation, AIOps)的概念，但现在先介绍一些专门针对持续维护 AI 流水线的几个阶段。以下是持续维护过程的四个主要组成部分。

- 持续集成(CI)：测试、验证代码和组件、数据、数据模式和模型。

- 持续交付(CD): 持续将代码更改或更新传递给模型, 一旦进行了更改, 模型就可以部署到测试环境, 然后进入生产环境, 不需要中断。
- 持续训练(Continuous Training, CT): 前面提到了持续学习对于机器学习的重要性, 而持续训练则使这个过程产品化。当数据源不断更新时, 模型也自动进行训练学习, 并不断从新数据中学习。
- 持续监控(Continuously Monitoring, CM): 持续监控 AI/ML 模型的运行情况非常重要, 以确保没有出现严重问题。

如果你想负责任地管理 AI 项目, 那就必须不断地对其进行改进和迭代。当迭代过程停滞不前时, 模型和超参数会过时, 数据也会陈旧, AI 将失去效果。性能是需要时刻关注的, 因为性能不足是显而易见的问题, 无论是面向客户还是内部使用。AI 也可能出错。例如, 性能滞后或模型更新频率低可能导致人们失去工作、无法获得有竞争力的贷款利率, 或者受到不公平的判决。模型维护不当, 可能会导致一系列严重后果。

1.5 数据库基础: 数据库、数据仓库、数据湖和湖仓

AI/ML 产品依赖于数据。其存储数据的方式和位置是一个重要的考虑因素, 会影响 AI/ML 的性能。本节将介绍一些最常用的数据存储方式。选择最佳的存储、访问和训练数据的方式是一项专业的工作, 但如果你从事 AI 产品管理, 你最终需要了解构建 AI 产品的基本要素。简而言之, 数据是 AI 的关键。

因为 AI 需要大量数据, 所以数据库的选择是产品和业务的重要战略性决策。如果没有一个良好运作的数据存储系统, 你会遇到许多问题, 这些问题将影响模型性能, 进而影响产品本身。作为产品经理, 了解对于产品来说最具成本效益和性能驱动的解决方案,

并在各个方面找到平衡，将有助于产品的成功。当然，对于这些决策，主要依赖技术执行人员，但产品经理需要参与其中，因此需要有所了解。

现在，看一些为 AI/ML 产品存储数据的可选项。

1.5.1 数据库

根据组织的目标和预算，可以将数据以某种方式集中存储，如数据湖、数据库和数据仓库，甚至可能考虑一种新的选择——数据湖仓。如果你刚开始接触这个领域，可以将数据存储的关系型数据库中，以便轻松访问和查询数据。如果需求相对简单，那么关系型数据库是一个很好的选择。在使用关系型数据库时，需要遵循特定的模式(schema)，如果希望将这些数据与其他数据库中的数据合并，可能会遇到模式对齐的问题。

如果你的数据库主要用于查询数据、获取公司数据的特定子集以进行常规的趋势分析，那么关系型数据库可能足够了。如果你希望将来自业务不同领域的各种数据集合并，并且希望实现更高级的分析、仪表盘或 AI/ML 功能，则可以继续阅读以下内容。

1.5.2 数据仓库

如果你希望将数据汇总到一个地方进行集中管理，并且有大量结构化数据输入，那么数据仓库(data warehouse)更为合适。实际上，这是走向成熟的第一步，因为它能够快速整合各个业务部门的洞察和趋势。如果需要以不同方式利用 AI/ML，而不只是某种特定的方式，则数据仓库非常适合。

假设要基于现有产品在人力资源功能中添加 AI 功能。你可以利用客户数据为客户提供基于同行绩效表现的趋势或预测，并使用 AI/ML 为内部员工提供预测或优化。这两种用例都可以通过数据仓库实现。

然而，数据仓库的创建需要一些前期投资，包括制订计划和设

计数据结构。此外，它们的投资成本较高，因为它们能够按需提供分析所需的数据，所以需要支付较高的成本来保持数据的即时可用性。根据内部用户的技术水平，你可以选择更便宜的选项，但对于大多数业务用户来说，他们更希望使用简单易懂的方式分析数据。无论采取哪种方式，数据仓库都能够为内部用户和利益相关团队创建仪表盘。

1.5.3 数据湖(和湖仓)

如果你有大量原始的、非结构化的数据，并且想要一个更高性价比的存储位置，可以考虑数据湖(data lake)。通过它，可以存储非结构化、半结构化及结构化数据，技术人员可以轻松访问这些数据。例如，数据科学家和机器学习工程师可以使用这些数据，因为他们可以创建自己的数据模型来实时转换和分析数据，但大多数公司并非如此。

如果你拥有大量的数据，而业务用户不需要立即使用这些数据，可以选择将数据存储和数据湖中，但不能完全用数据湖替代数据仓库或数据库。数据湖是一个“有备无患”的方案。如果你已经有一个庞大的历史数据湖，希望将来用于分析，则需要考虑另一种数据存储方式以便进行洞察。

你或许听过“湖仓”(lakehouse)这个术语。市面上有许多数据库、数据仓库和数据湖。“湖仓”是由 Databricks 公司提出的，它提供了类似于数据湖的功能，但又具备数据仓库的一些功能，即展示数据、使其对内部的非技术用户可用和可读取，并创建仪表盘。湖仓的最大优势在于可以预先存储数据并支付存储费用，然后可以在下游访问和操作数据。

1.5.4 数据流水线

无论使用何种技术维护和存储数据，都需要建立数据流水线，以确保数据的流动通畅，这样仪表盘可以按照业务需求同步更新，并确保数据按照所需要的方式流动。处理和传递数据也有多种方式。

可以批量处理(批处理)大量数据，定期移动数据，或者使用实时流水线，以便在数据生成后可以实时获取数据。如果想进行预测分析、报告生成，或者建立一个能够移动、处理和存储数据的系统，数据流水线或许已经足够了。然而，根据数据处理的任务和转换量的规模，你可能需要同时使用数据流水线和 ETL 流水线。

ETL 代表抽取(Extract)、转换(Transform)和加载(Load)，数据工程师可以为更高级的系统创建特定的流水线，例如将所有数据集中到一个地方，插入数据或更新数据增强，将数据与客户关系管理(Customer Relationship Management, CRM)工具连接，甚至在系统之间对数据进行转换和格式化。这是在使用数据仓库或数据库时不可或缺的步骤。只要使用数据湖，你就会拥有所需要的所有元数据，按你喜欢的方式进行分析并获取洞察。在大多数情况下，如果正在构建 AI/ML 产品，你将与数据工程师合作，他将为数据流提供支持，确保产品正常运行，其中往往需要同时使用关系型数据库和数据仓库。实现 AI/ML 功能所需要的分析大多由专门负责 ETL 流水线的数据工程师完成。

管理和维护这个系统也是数据工程师的工作，产品经理需要与数据工程师保持密切的合作关系。上述两种流水线方式之间的一个关键区别是，ETL 流水线通常是批量更新，而不是实时更新。例如，如果使用 ETL 流水线更新客户使用产品的日志信息，以提供关于客户的洞察，最佳方式是每天更新两次。然而，如果内部业务用户需要使用实时仪表盘以获得洞察，并且他们依赖这些数据进行日常决策，那么可能需要使用连续更新的数据流水线。

现在，了解了存储数据的不同可用选项以及如何选择适合业务的正确选项，接下来讨论如何进行项目管理。

1.6 项目管理：IaaS

在组织中创建一个 AI/ML 系统时，需要将其视为一个独立的生

态系统，并持续维护。这就是 MLOps 和 AIOps 需要与 DevOps 团队密切合作的原因。越来越多的公司开始提供托管服务和基础设施即服务(Infrastructure-as-a-Service, IaaS)。行业也在发展，Determined AI 和 Google 等公司的 AI 平台流水线工具开始根据市场的需求提供解决方案。这样的需求背后的核心是，对于那些刚开始使用 AI 系统处理庞大任务的公司，减少它们的困惑，减轻其负担。

经过几十年的试错，DevOps 团队在大规模软件开发中越来越常见，MLOps 和 AIOps 也有类似的趋势。开发解决方案和将其投入运营是两个不同但需要合作的领域。对于 AI/ML 系统来说尤其如此。现在的趋势是 IaaS。这是一个重要的概念，因为刚接触 AI 的公司通常对 AI 所需要的成本、存储、计算能力和投资并不了解，特别是对于需要大量数据进行训练的深度学习 AI 项目，更缺乏了解。

目前，大多数公司才刚开始运行 AI/ML 程序，甚至没有专门的团队。像 MAANG(Meta、Amazon、Apple、Netflix、Google)这样的科技公司正在引领管理 AI/ML 的文化规范，但大多数需要拥抱 AI 的公司并非科技公司，并且在技术债务方面准备不充分，将给工程团队带来管理上的挑战。

如果为了推进 AI 计划而走捷径，会导致日后需要重构代码或者更改数据的存储和管理方式。因此，制定采用 AI 的策略和计划至关重要。IaaS 解决方案的出现可以帮助工程团队保持灵活性，以应对未来的变更需要。随着时间的推移，保持 AI 团队运行所需要的基础设施也会发生变化，使用 IaaS 提供商的优势在于可以运行所有项目，并且只需要支付 AI 开发人员实际使用数据进行模型训练的时间费用。

1.7 部署策略：部署与应用模型

当选择了合适的模型(包括其性能和错误率)，并且建立好产品

和所选 AI 模型用例的基础设施时，就可以进入流程的最后一步：将代码部署到生产环境中。正如 1.6 节介绍的，在持续维护工作中，确保采用适合产品和组织的部署策略非常重要。同时，需要考虑重新训练模型和刷新训练数据的频率，以防止模型性能下降和数据漂移。此外，还需要一个系统来持续监控模型的性能。这个过程，不同的产品和业务会有所差异，特别是因为在重新训练期间系统需要一些停机时间。

部署是一个动态过程，由于模型主要用于对真实世界的数据进行预测，因此根据真实数据的变化，你需要或多或少地关注部署。例如，在为一家机器学习房地产科技公司工作期间，房地产数据由于疫情导致的移民数据和房价数据的快速变化而出现巨大偏差，我们几乎每天都在更新、重新训练和重新部署模型。如果模型未经检查，而且未经工程师或业务领导人在产品客户端上进行检验，我们可能无法发现模型基于非典型数据，从而做出明显错误的决策。

此外，还需要了解许多众所周知的部署策略。我们将在下面的内容中进行讨论。

1.7.1 影子部署策略

在影子部署策略中，同时部署一个新模型和一个已经存在的模型，新模型有新的特性。然而，新模型只是作为当前正在使用的模型的影子存在。新模型将与现有模型一样处理所有请求，但不会显示模型的结果。这种策略可在不中断实际生产中的模型的情况下，观察影子模型在相同的真实数据上是否表现更好。一旦确认新模型的性能更好，并且没有运行问题，它就将成为主导模型，并替换原始模型，完全部署在生产环境中。

1.7.2 A/B 测试模型部署策略

采用 A/B 测试模型部署策略，实际上是在同时运行两个略有不

同的模型。两个模型具有不同的特性，这使它们在生产环境中的运行情况和性能也有差异。这两个模型同时设置，并通过优化性能提升转化率。可以将其看作一项实验，比较两个模型的结果，并且根据某种假设或期望来判断哪个模型的性能更好，然后进行验证。不过，模型之间的差异必须足够小，因为如果两个模型的特性差异太大，就无法确定什么因素起到了最重要的作用。

1.7.3 金丝雀部署策略

在金丝雀(canary)部署策略中，采用了渐进方式进行系统部署。具体而言，将用户分成不同的子群体，然后逐渐增加体验新模型部署的用户数量。这样做的好处是可以给不同用户群体设置缓冲时间，以观察他们对新模型的反应和使用情况。实质上，在发布到新批次之前，将不同用户分组作为测试者，以便逐步发现错误和修复可能存在的问题。这个过程较为缓慢，但会带来可观的回报，需要足够的耐心和勇气。

还有更多的策略可供选择，但要记住，选择什么策略取决于多个因素，包括产品的性质、客户/用户需求、预算限制、指标和性能监控、技术能力和知识、时间安排等。在部署之外，还需要帮助业务部门了解代码重构和分支操作的频率。

现在已经讨论了不同的部署策略，接下来看看在 AI 领域的成功案例。

1.8 AI 领域的成功案例：构建基础设施的成功案例

针对机器学习系统的复杂性，许多大型科技公司都专门建立了团队和平台，致力于构建、训练、部署和维护机器学习模型。以下是构建 AI/ML 程序时的几种选择。

- Databricks 的 MLflow——MLflow 是由 Databricks 公司开发的开源平台，旨在帮助企业管理机器学习的全生命周期。

它允许运行实验，并使用各种库、框架或语言。其主要优点包括实验跟踪(观察不同实验之间模型的表现)、模型管理(管理团队间的所有模型版本)和模型部署(快速查看部署情况)。

- Google 的 TensorFlow Extended(TFX)——这是 Google 公司基于 TensorFlow 开发的最新产品，是一个端到端的平台，用于部署生产级别的机器学习流水线。它允许团队内部和团队之间进行协作，并提供强大的功能，以支持可扩展、高性能的环境。
- Uber 的 Michelangelo——Uber 公司是一个很好的示例，它们自主研发了机器学习管理工具 Michelangelo，用于团队协作和模型部署。在使用 Michelangelo 之前，Uber 公司使用的是不同的编程语言、模型和算法，并且团队之间存在信息孤岛。在实施了 Michelangelo 后，成功地将不同技能和能力整合到一个系统中。它们需要一个可靠、可复制、标准化的流水线，以便大规模地创建、管理、预测和部署数据。
- Meta 的 FBLearner Flow——为管理其众多的 AI 项目，Meta 公司自己开发了该系统。由于机器学习是其产品的基础部分，因此 Meta 公司需要平台，该平台能够实现以下功能。
 - 实现的每个机器学习算法都能够在以后被其他人重复使用。
 - 每个工程师都能够编写可重复使用的训练流水线。
 - 使模型训练变得简单和自动化。
 - 每个人都能够轻松地检索过去的项目和实验。

实际上，Facebook 创建了易于使用的知识库和 workflows，以集中管理其所有的机器学习操作。

- Amazon 的 SageMaker——这是 Amazon 公司的一款产品，提供一套完全托管的基础设施工具和工作流程，以构建、

训练和部署机器学习模型和程序。这个产品的理念是满足其客户的需求，提供低代码或无代码的 UI(User Interface, 用户界面)，无论是机器学习工程师还是业务分析师都可以使用。如果你已经在使用 Amazon 的服务作为云基础设施，那么就可以方便地使用 SageMaker 的基础设施，以进一步自动化和标准化大规模的 AI/ML 程序和操作。

- Airbnb 的 Bighead——为了实现其 AI/ML 组织之间的标准化和集中化，Airbnb 公司创建了自己的机器学习基础设施 Bighead。它们使用了一系列工具，如 Zipline、Redspot 和 DeepThought，来协调其机器学习平台，以达到与 Facebook 和 Uber 一样的目标：减少错误和差异，并最小化重复性的工作。

如上所述，有多个平台可以用于创建、训练和部署机器学习模型。最后，探讨一下 AI 的未来。

1.9 AI 的潜力：AI 的发展方向

那么，AI 实施将会带领我们走向何方？它对所有行业意味着什么？目前，AI 是一个受到地缘政治影响的行业，AI 技术的采用伴随着大量的责任、成本和机会。只要公司和产品经理意识到妥善管理 AI 项目所涉及的风险、成本和投资程度，将其视为一种探索，并将 AI/ML 应用于容易取得成果的项目，并在此基础上持续发展，那么投资于 AI 的人将会体验到 AI 的潜力。这个潜力源于可量化的预测和优化的能力。例如，Highmark 公司在 2019 年通过使用机器学习进行诈骗检测，节省了超过 2.6 亿美元；GE 公司通过预测性维护帮助客户节省了 16 亿美元；而 Amazon 公司通过其推荐引擎创造了 35% 销售额。

当业务收入中有 1/3 来自 AI 算法时，AI 的重要性将毫无争议。不管对 AI/ML 投资多少，一定要通过适当的规划和战略来确保充分

发挥其最大效果。同时，物色了解这个领域和潜在风险的人才，并选择适合的可扩展基础设施来减少系统重构的成本。

如果你负责监督这些项目，只要 AI/ML 项目能够直接影响成本节约或收入增长，你很有可能在职业生涯中获得成功。本章详细介绍了维护 AI 程序的许多方面以及潜在的障碍，因此有一个明智的策略，即从小规模着手，将 AI 应用于明确的业务目标，跟踪目标的实现，并展示其有效性。如果你能向最犹豫的高管清晰地传达 AI 的优势和潜力，就能更好地解释需要投入的时间、人力和基础设施费用所对应的价值。

这对于技术资源(数据科学家、数据工程师和机器学习工程师)与业务利益相关者也非常重要。了解你将使用的机器学习算法或者获得一些建议来更好地存储数据只是一个方面，如果你不能迭代项目，并积累对最佳实践的理解和直觉，就无法成为组织内的真正变革推动者。我们在项目中不断迭代学习，并在成功完成任务的过程中建立信心。作为产品经理，同样如此。

在前面的示例中，GE 公司帮助其客户节约了成本，Highmark 公司通过预测欺诈行为预防未来的瓶颈，Amazon 公司通过机器学习增加了收入。当我们还在思考 AI 的潜力以及它将带领我们走向何方时，这些示例表明 AI 是最新工业革命的核心。AI 不仅仅为公司带来好处，还对每个人都有好处。当然，利益的分配可能并不完全平等，因为投资 AI 的公司在投资这项技术，它们会优先追求最高的回报。但重要的是，消费者和企业都将从 AI 中获益。

1.10 本章小结

本章介绍了很多内容，其中许多概念将在后续章节进一步讨论。毫不夸张地说，基础设施对实现 AI/ML 至关重要，因为性能很大程度上取决于如何传递数据和管理部署。本章介绍了机器学习和深度学习的基本定义，以及它们所能应用的学习类型。本章还介绍了设

置和维护 AI 流水线的基础知识，并提供了一些其他公司管理此类操作的示例。

构建利用 AI/ML 的产品是一项雄心勃勃的事业，作为本书的第 1 章，本章旨在为建立整个 AI 项目的过程提供足够的基础，以便在后续章节中能够在该过程的各个方面深入讨论，而不必在后期引入过多新概念。如果你感到不知所措，那意味着你正在理解构建 AI 所需要的规模。这是一件好事！在第 2 章，将深入具体地介绍本章提到的机器学习模型的使用和维护。