



人工智能赋能的智能环境及其应用创新模式

北京大学 信息工程学院

朱跃生

2022 年 11月 19日

北京大学



朱跃生 教授/博士生导师

工学学士 (华南理工大学)
工学硕士 (华南理工大学)
博士 (香港城市大学)

大陆 - 香港 - 新西兰 - 美国 - 大陆

北京大学、华南理工大学
香港城市大学、香港理工大学、
新西兰Otago大学AI Lab (NLP)、
Auckland理工大学AI Lab (NLP)，
美国硅谷教育及高科技界

从事通信信号处理、编码理论与应用，人
工智能安全、网络与信息安全的教学校研
及标准化工作





Email: zhuys@pku.edu.cn, Office: 6号楼1502

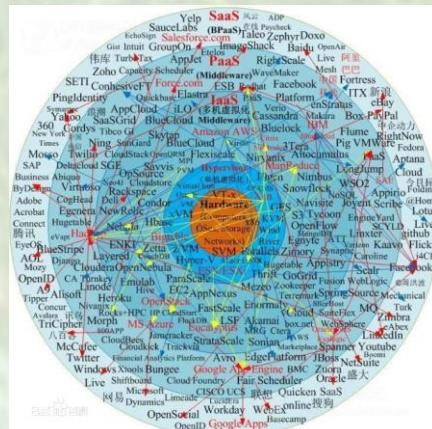


Teaching Assistant: 张扬, 干皓丞



教学大纲-系列专题

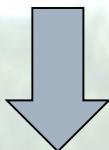
- 智能环境下“人工智能+与“互联网+”的发展模式与机遇
- 智能环境下新型智慧城市的建设与管理模式
- 智能环境下新一代无线通信网络技术（5G）及“物联网+”产业发展机遇与创新模式
- 智能环境下金融行业面临的挑战及创新模式
- 智能环境下大健康产业发展趋势与创新模式
- 智能环境下数据安全与应用创新模式
- 智能环境下电子政务/电子商务的发展趋势与管理模式



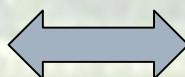
北京大学

当下世界形势变化面临的挑战与机遇

- “疫情时期”
- “国际关系变化”

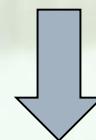


- “人口众多”



应用场景丰富

- “地缘广大”



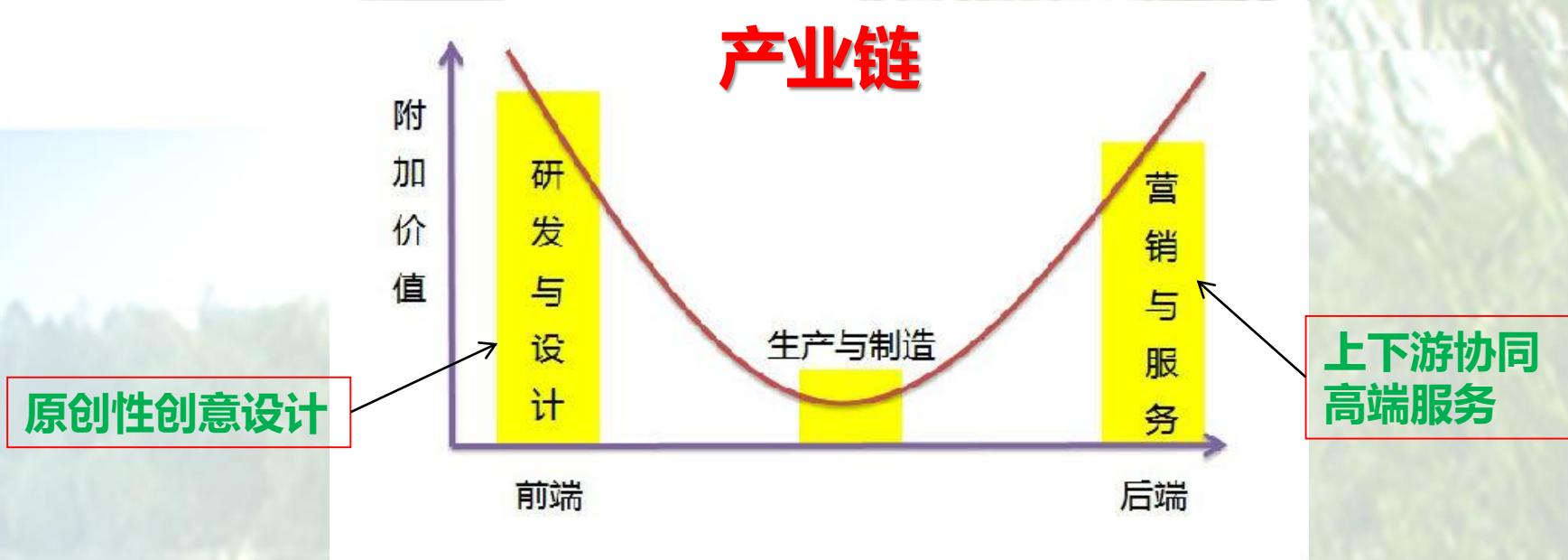
持续健康的社会发展

丰富的应用场景



- 基本原理 → 关键技术 → 应用场景 → 解决方案
- 应用场景 → 关键技术
痛点/难点 → 解决方案 → 商业模式

“微笑曲线”

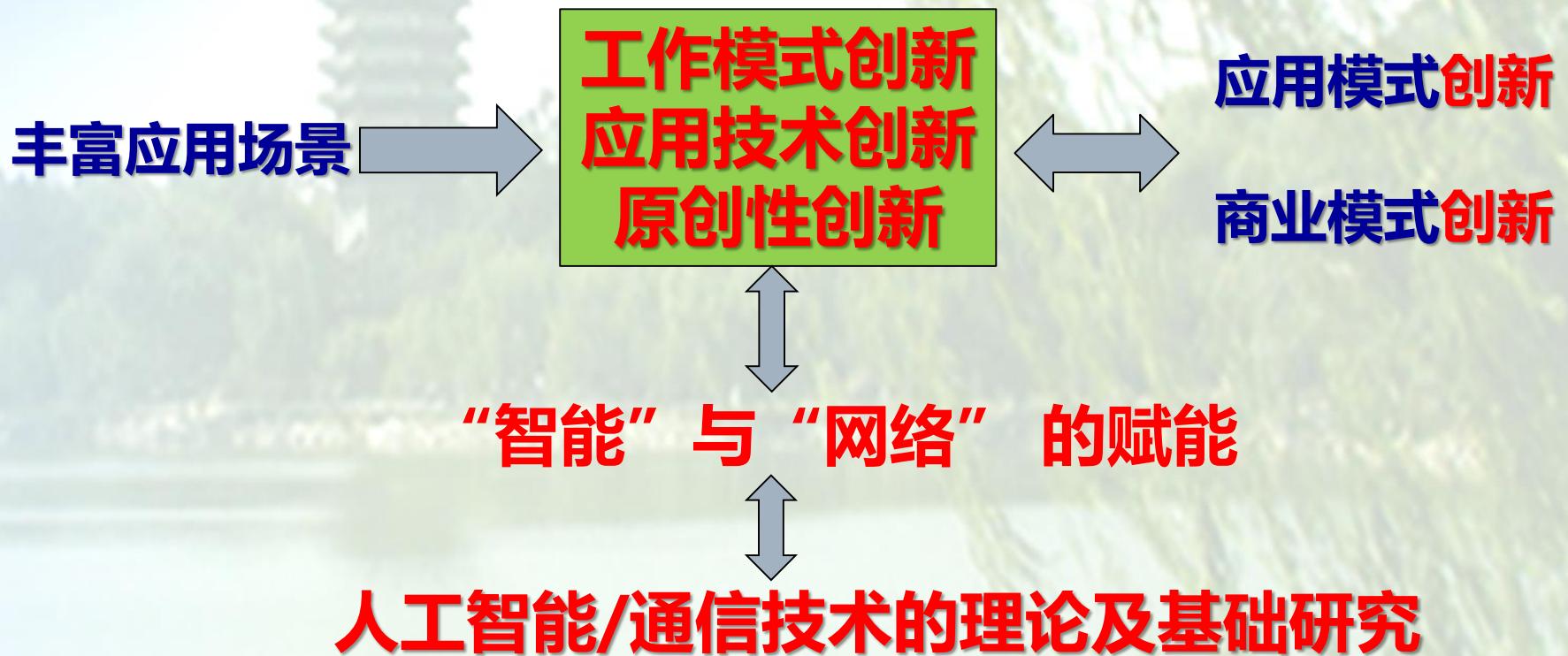


附加值体现在两端，处于中间环节的生产与制造附加值最低

制造大国：处于“微笑曲线”中间区域的生产与制造环节，投入大量的劳动力，但获取的利润少



(一) 智能环境下“人工智能+ 与“互联网+” 的发展模式与机遇

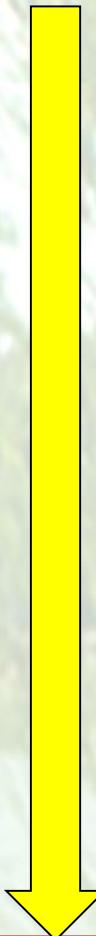




互联网时代：

互联网服务和商业模式演进带来的思考

- ✓ 互联网门户时代
Yahoo!
- ✓ 搜索时代
Google, 百度
- ✓ 移动互联网时代
Apple, 华为, 三星, 小米等智能终端
- ✓ 社交网络时代
微信, Facebook, Twitter
- ✓ 互联网消费时代
亚马逊, eBay, 淘宝, 京东…



丰富的应用场景



- 基本原理 → 关键技术 → 应用场景 → 解决方案
- 应用场景 → 关键技术
痛点/难点 → 解决方案 → 商业模式



移动互联网关键点

- 终端移动性
“随时、随地、随心” 接入使用互联网
- 业务多样性-更具个性化
 - QoS** (服务质量, 客观)
 - QoE** (用户体验, 主观)
 - 灵活的电子商务应用模式
- 安全性
 - 移动互联支付
 - 信息安全与隐私保护



移动社会及影响 Mobile Society

转变：工作方式，学习方式，生产方式，思维方式，管理方式
交往方式，生活方式

- ✓ 移动交互 **Mobile Interaction**
- ✓ 移动工作 **Mobile Working**
- ✓ 移动医疗 **Mobile Medicine**
- ✓ 移动娱乐 **Mobile Entertainment**
- ✓ 移动政务 **Mobile Government**
- ✓ 移动商务 **Mobile Commerce**
- ✓ 移动教育 **Mobile Education**

⋮



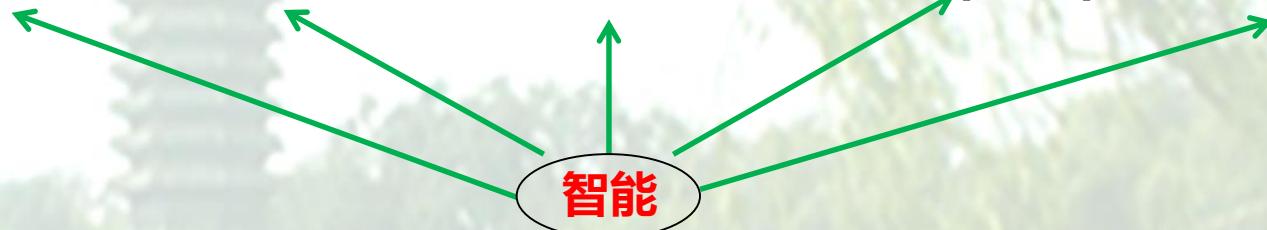
北京大学



互联网及应用发展

- ✓ 通过互联网媒体属性及产业属性

知情 → 交换信息 → 动态交互 → 消费(支付) → 产业(生产)



- 我国互联网及产业蓬勃发展

如：互联网BAT：百度（B）、阿里巴巴（A）和腾讯（T）
在搜索、电商和社交领域促进了消费/产业互联网发展

- ✓ 2014年我国互联网经济已占GDP达7%，首次超过美国；
- ✓ 目前：网络零售交易额规模跃居全球第一



万联网 (IoE)

✓ 互联网- Internet



物联网 - Internet of Things (IoT)

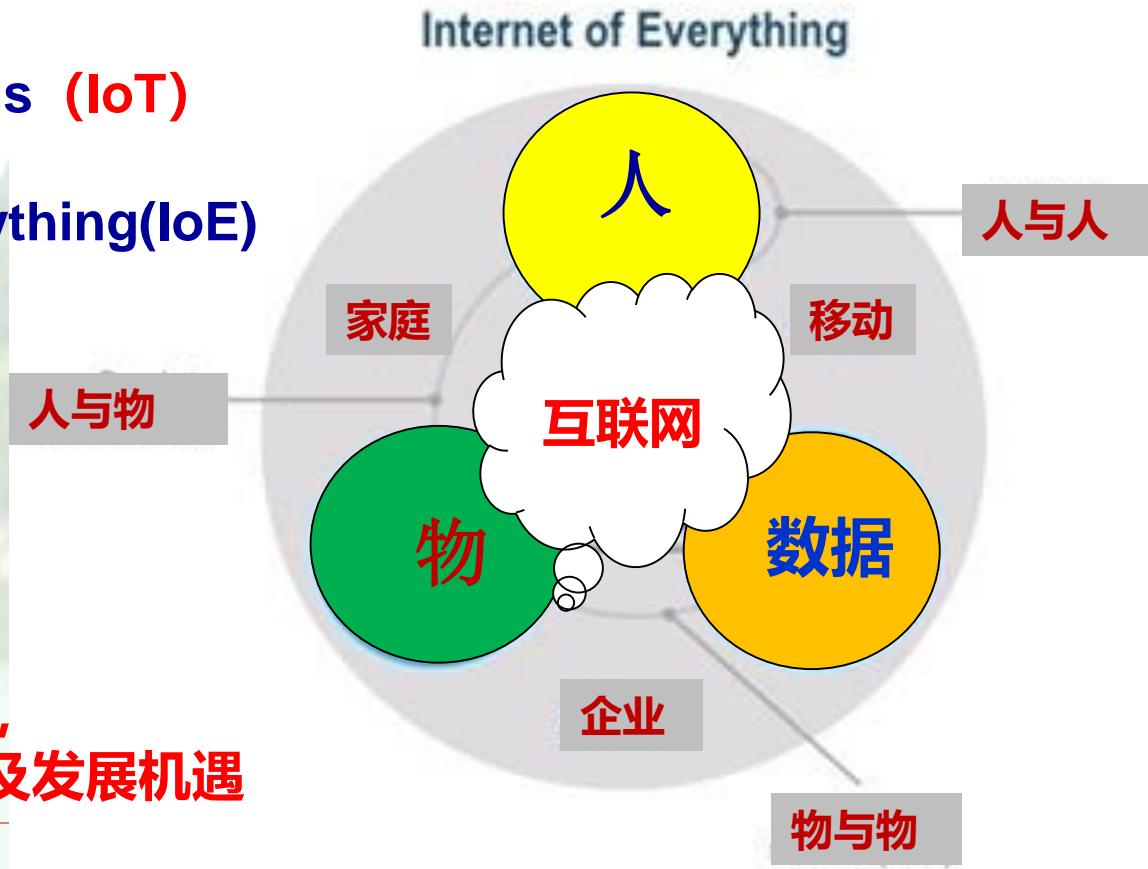


万联网 – Internet of everything(IoE)

➤ Things 事件

联人、联物、联数据
高效和融合

➤ 利用网络/数据/信息给企业，
可为个人和社会带来创新及发展机遇



融合先进信息技术的万物互联智能生态环境

- 物联网 (IoT)
- 移动计算 Mobile Communication & Computing,
元宇宙 (Metaverse)
- 人工智能 (AI)
- 区块链 (Block Chain)
- 云计算 (Cloud)
- 大数据 (Data Science)
- 边缘计算 (Edge Computing)
- 扩展现实 (XR, Extended Reality)
- 信息安全 (Security)

I M A B C D E X S

I M A B C D E X S

AI 赋能创新

integration innovation and supporting technology



IoT感知场景

Perceptual scenario

Secured AI-
Networking

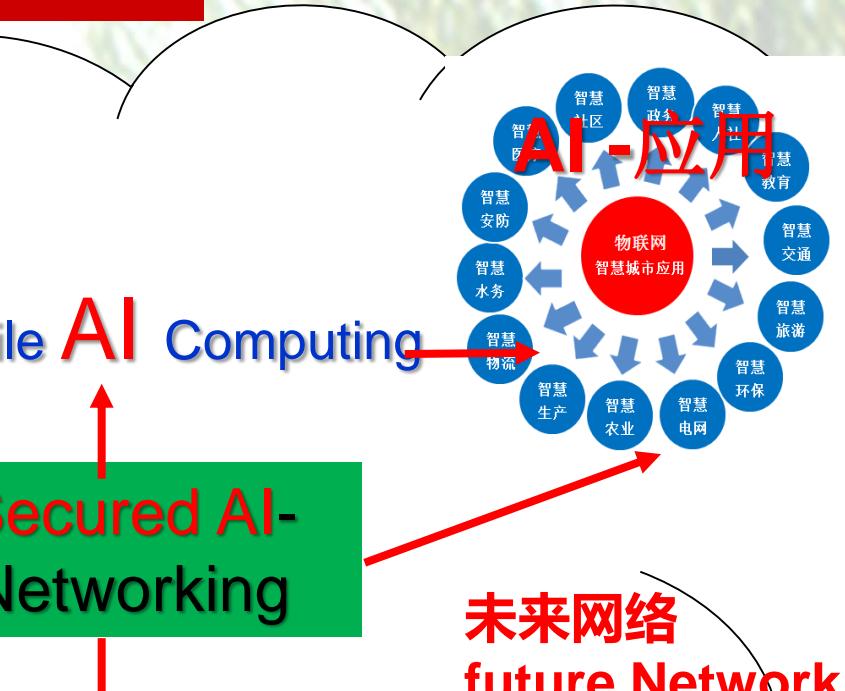
AI Cloud

A Block Chain Data Science

Mobile AI Computing

未来网络
future Network

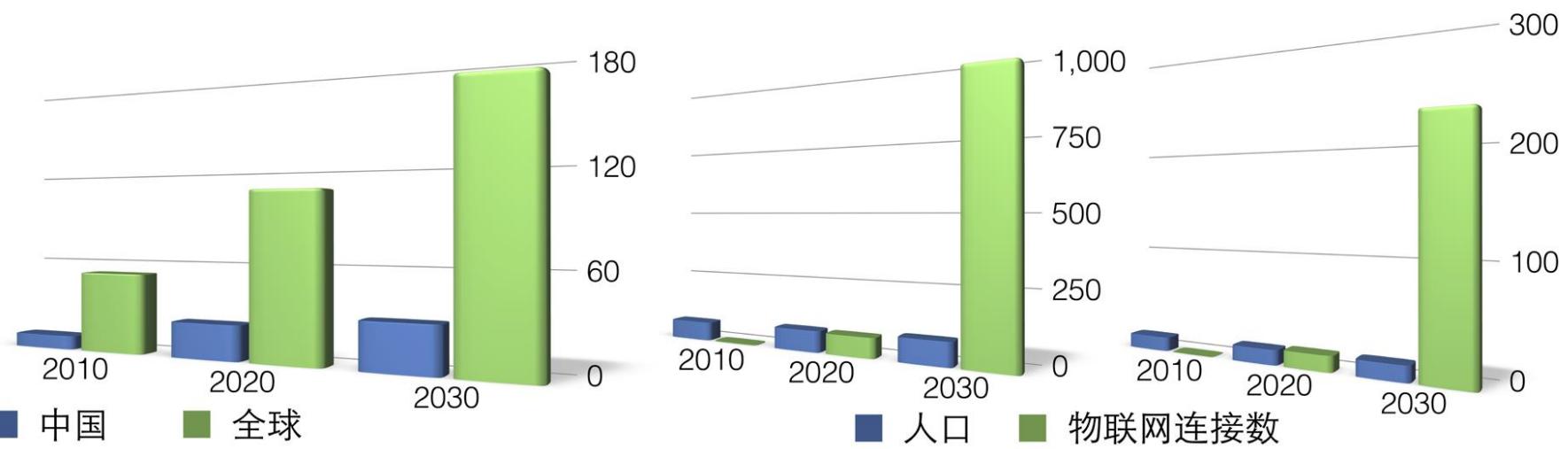
AI-应用



丰富的应用场景



2010-2030年全球和中国 移动终端及物联网连接数增长趋势



我国网络规模及大数据形成

截至2022年6月，我国网民规模为10.51亿，互联网普及率达74.4%
截至2021 年12 月，手机网民达 10.29亿，网民用手机上网比例为 99.7%

□ 每天产生巨大数据

- 互联网（社交、搜索、电商、微信微博）、物联网（传感器，智慧地球）、车联网、GPS、医学影像、安全监控、金融（银行、股市、保险）、电信（通话/短信）每天都在疯狂产生着数据



图 22 手机网民规模及其占网民比例



- IDC 预测，全球产生的数据量呈指数级增长，近两年产生的数据量相当于之前产生数据总量

大数据 (big data)

✓ 定义

数据量大到超出目前**传统**数据库软体工具，在合理时间内达到获取、管理、处理、并分析整理成可说明决策信息的**能力**

"Big data refers to data sets whose size is **beyond the ability** of typical database software tools to capture, store, manage and analyze."

- *The McKinsey Global Institute, 2011*



时空大数据



大数据包括了那些数据量很大，导致常用的数据软件工具无法在合理时间内获取、组织、管理和处理的数据集



主要特点-5V

➤ Volume (量大)

ZB级，非结构化数据大规模增长，
占总量80%，比结构化数据增长快10-50倍

➤ Velocity (变化快)

实时，监控

➤ Variety (种类多)

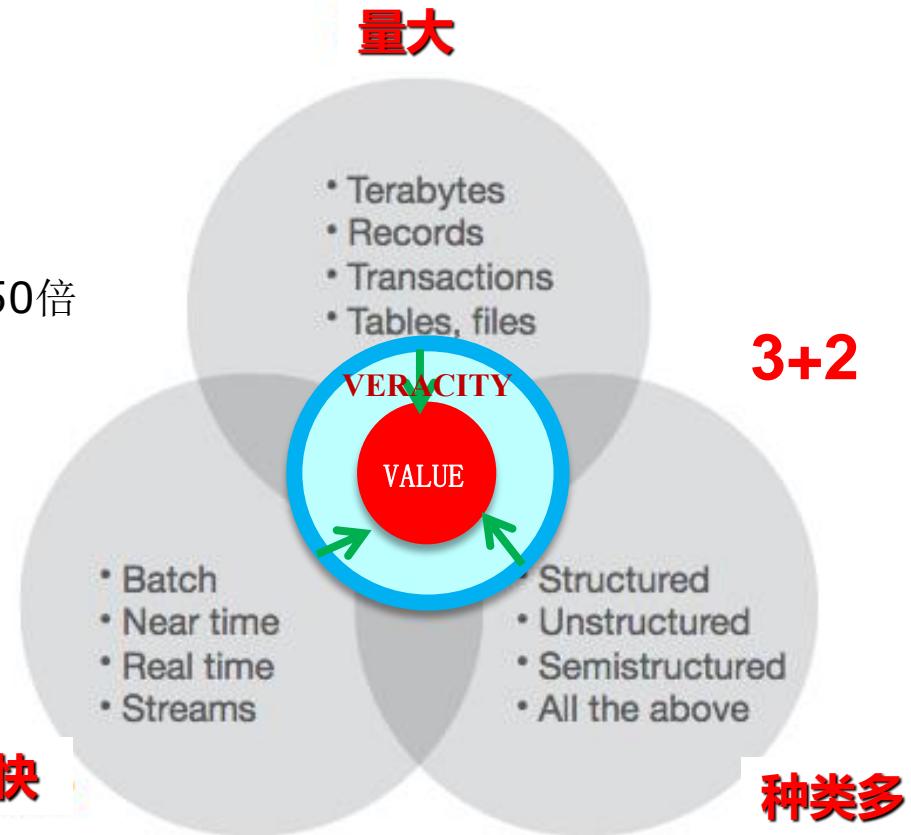
文本、图像、视频、机器数据

➤ Veracity (提取精准性)

完整性、模糊 / 隐性 → 关联一致性

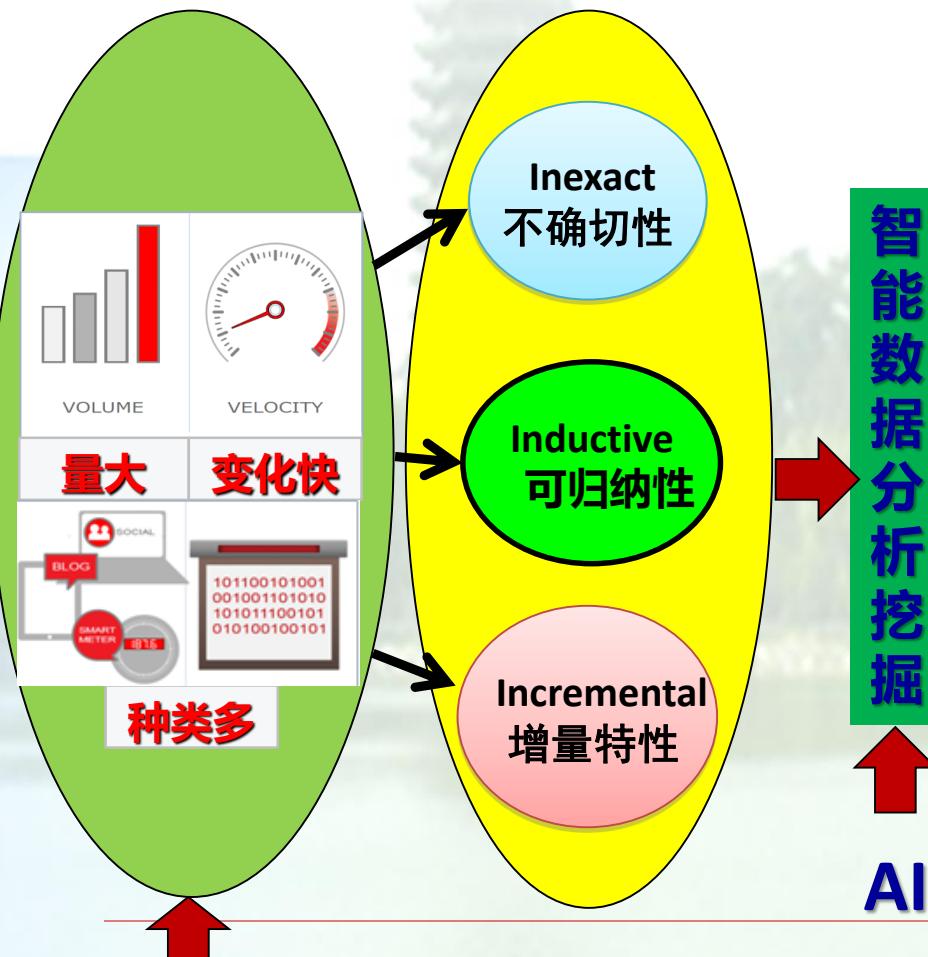
➤ Value (价值)

挖掘 → 预测，咨询，报告 → 经济及社会效益



大数据与智能分析

Big data and Intelligent Analysis



客观特点

北京大学

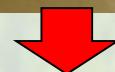
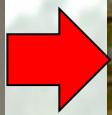
大数据与数据统计

□ 数据统计 ≠ 大数据分析

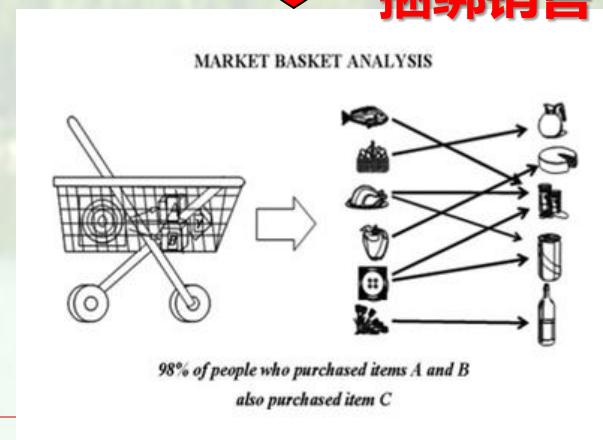
- ✓ 大量的数据并非一定具有“价值”
- ✓ 大数据分析和数据统计的区别在于“智能分析”



实例：“啤酒+尿片”关联的启示



捆绑销售



但商品的关联
因地域不同
季节不同
文化不同

而不同！！！

“网络”与“智能”的赋能

- 创造新的发展生态圈
 - ✓ 新的社会形态
 - ✓ 新的先进生产力
- ◆ 充分发挥互联网在社会资源配置中的优化和集成作用
- ◆ 将互联网/**智能技术**创新成果深度融合于经济、社会各领域中
- ◆ 提升全社会创新力和生产力，形成更广泛经济发展新态势



物联网 (IoT, Internet of Things)

在互联网基础上延伸扩展起来的网络

利用传感设备及网络技术，通过感知、识别、以及网络连接

物物相连：在物与物间进行通信和信息交换，**事物：联人，联物，联事件，联数据**

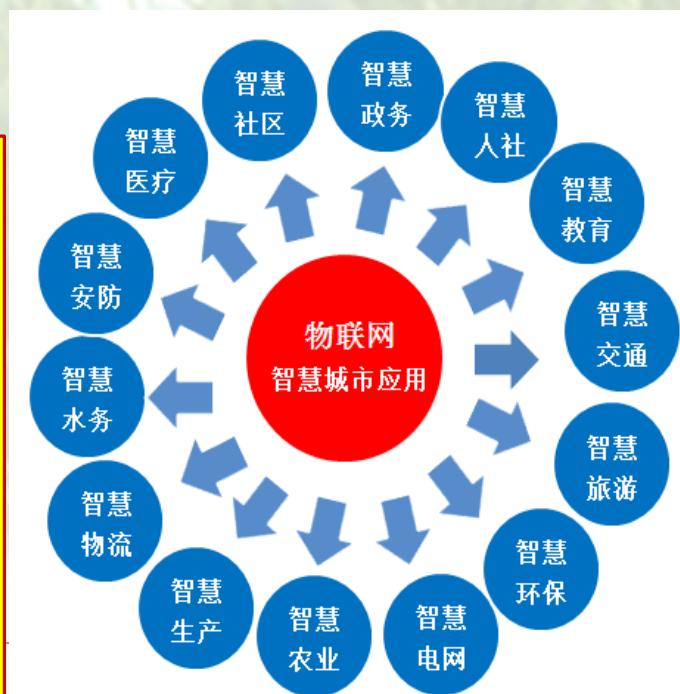
利用智能技术，实现智能化识别、定位、跟踪、监控和**安全管理**

物联网分为三个层次

感知层：利用传感设备，如传感器、二维码、RFID标签、摄像头、支撑技术包括GPS、北斗以及WiFi、智能蓝牙、NFC/RFID和ZigBee/Z-Wave等技术，自动识别并获取物体的信息；

网络层：通过各种网络与互联网的融合，将感知到的信息进行标准化封装，实时准确地传递到信息处理中心；

应用层：对感知到的信息进行处理，进行智能分析处理、实现精准监控和有效管理等各种实际应用



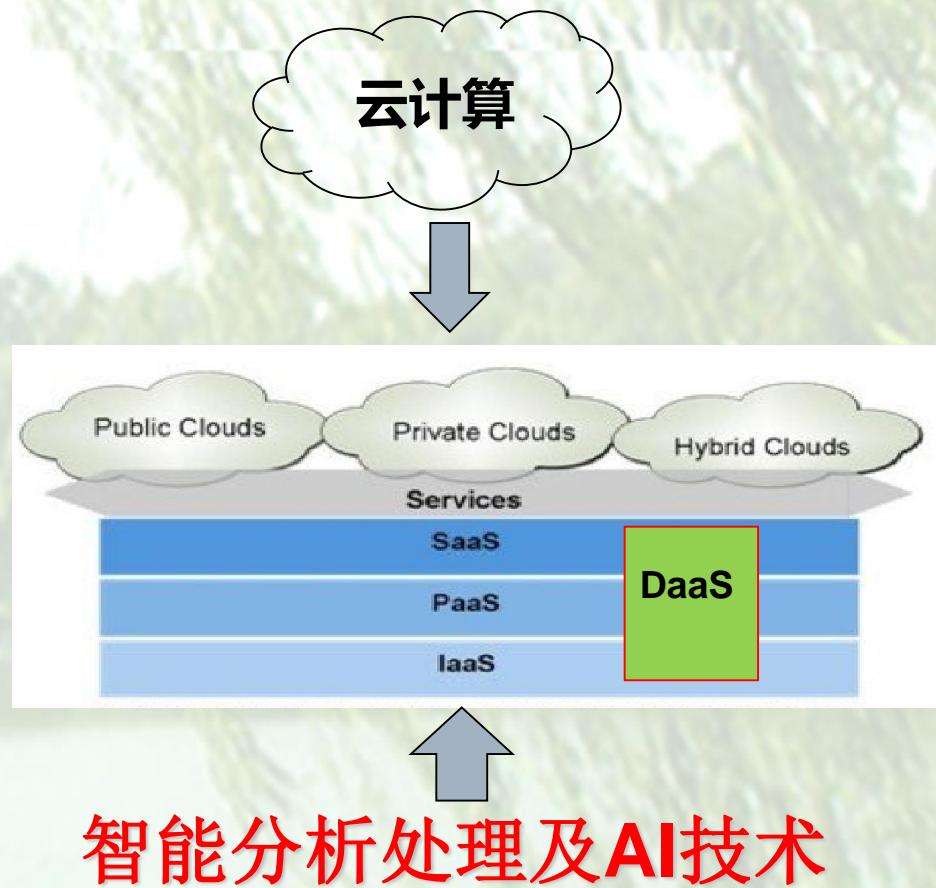
云计算与“互联网+”

- 为资产提供存储、访问和计算环境
- 提供云服务

基础实施即服务 (IaaS)
平台即服务 (PaaS)
软件即服务 (SaaS)
数据即服务 (DaaS)

海量存储和计算，如视频智慧监控

- 挖掘价值性信息和预测性分析
- 政府、企业、个人决策和服务



人工智能 AI

Artificial Intelligence

➤ 模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的技术科学

✓ 研究使计算机来模拟人的某些思维过程和智能行为（如学习、推理、思考、规划等）的学科

✓ 人工智能涉及计算机科学、心理学、哲学和语言学等学科

✓ 弱人工智能

在特定领域、有限规则内类比和延伸人的智慧（目前）

✓ 强人工智能

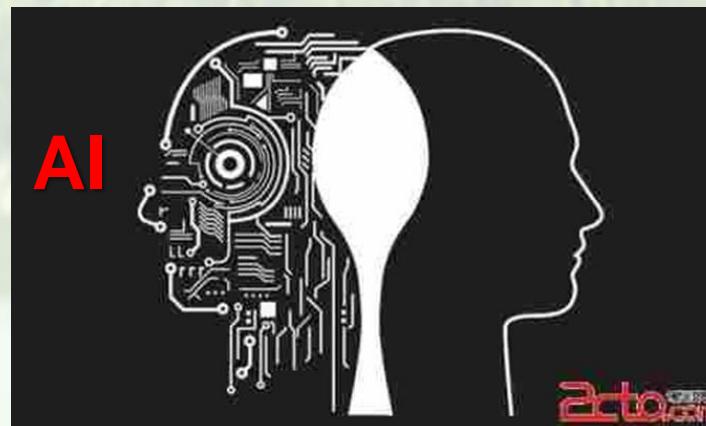
具意识、自我和创新思维，进行思考、计划、解决问题
抽象思维、理解复杂理念、快速学习和从经验中学习等
人类级别智能

✓ 超人工智能

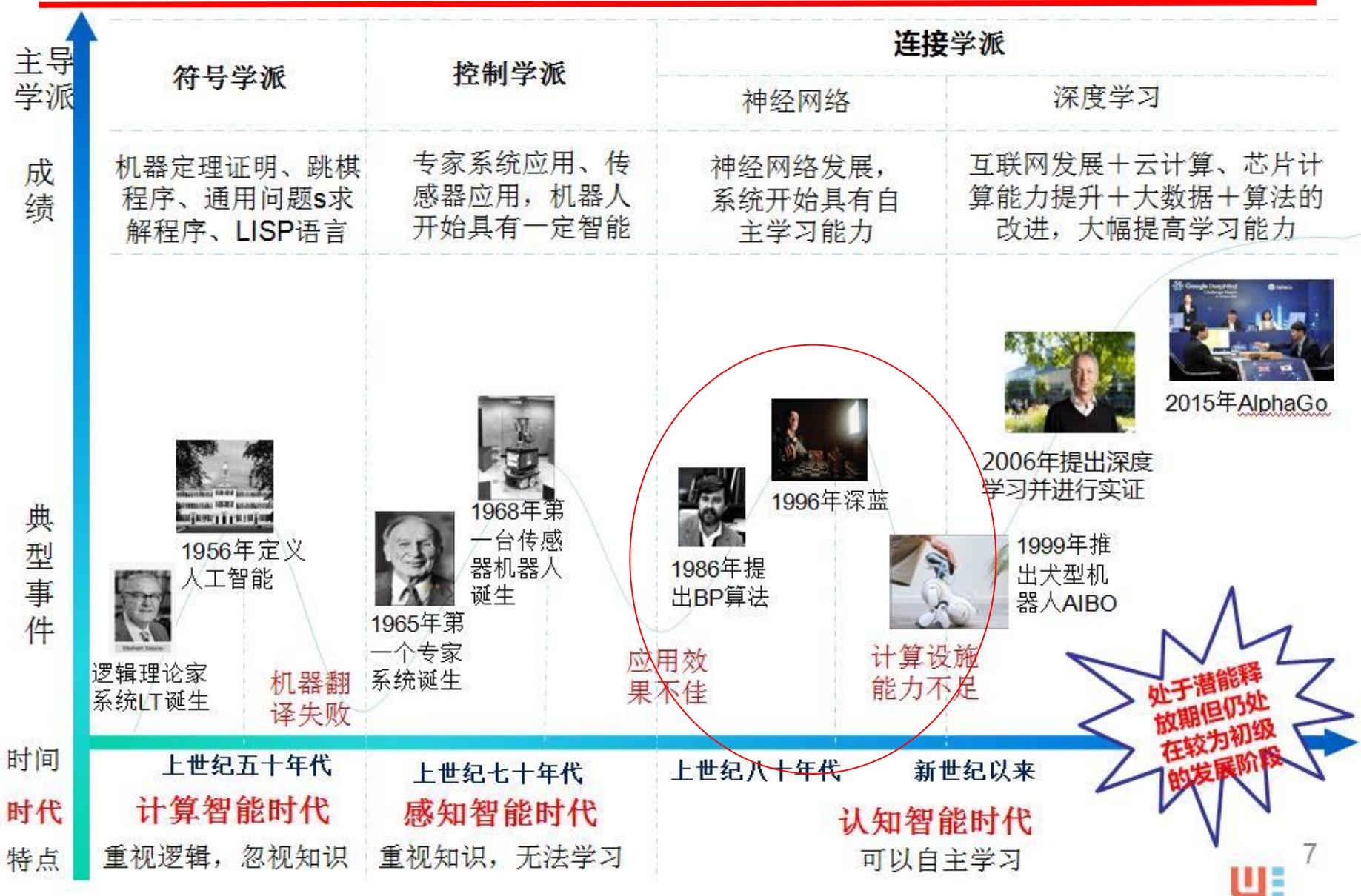
大幅超越人类智能



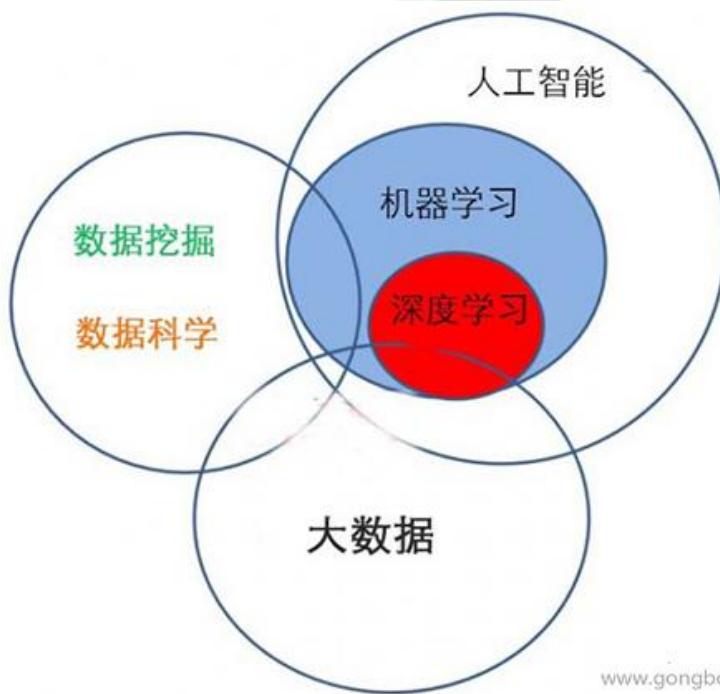
由人类制作的机器/软件
展示的智能



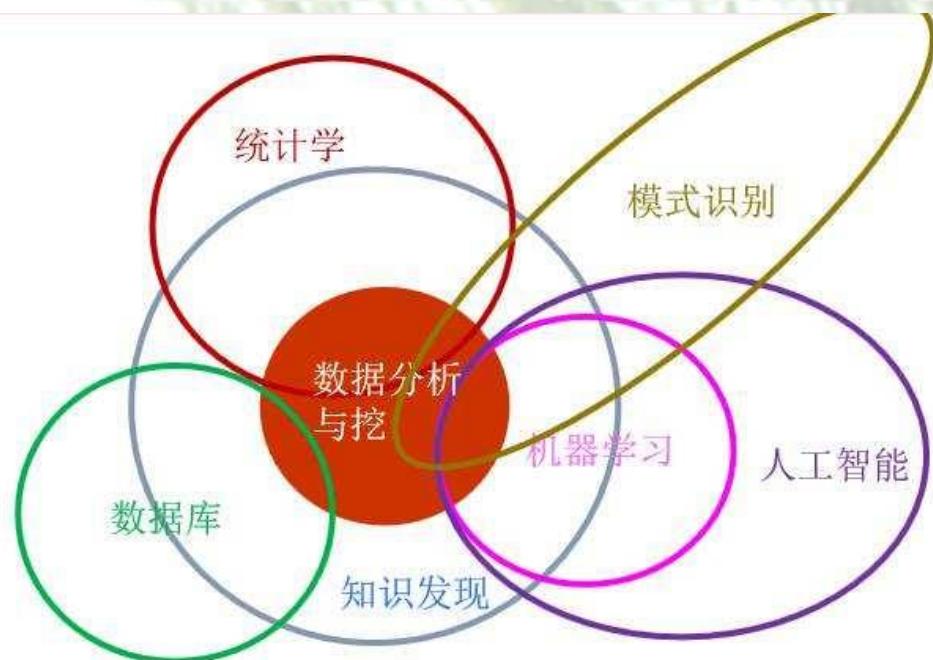
人工智能开始进入第四次发展浪潮



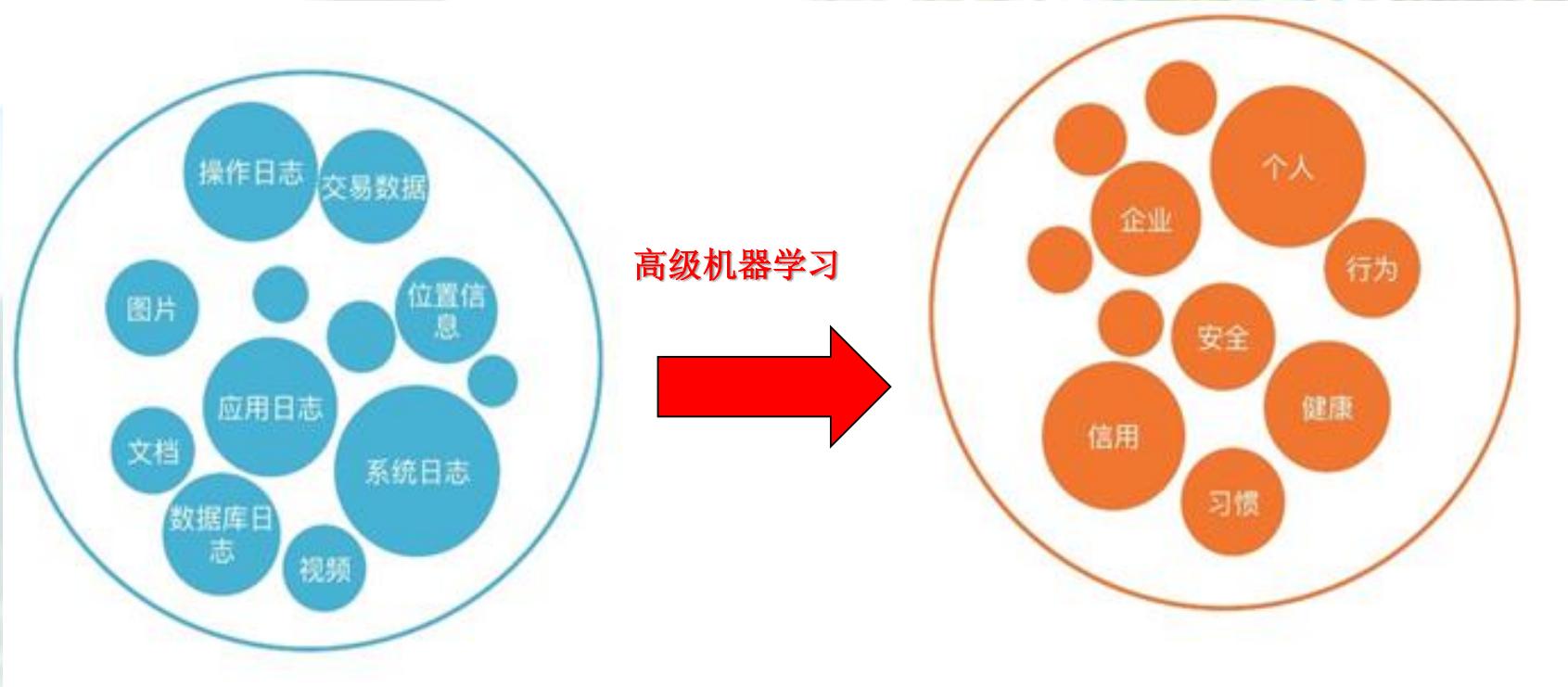
大数据与人工智能



www.gongboshi.com



大数据的分析与理解需要人工智能



区块链 Blockchain

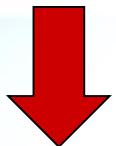
- 2008年，中本聪 《Bitcoin: a peer-to-peer electronic cash system》
 - 设计了一种可解决重复支付问题的P2P电子收银系统——比特币系统
 - 区块链用于记录比特币交易的账目历史
- ✓ 多方共同维护
- ✓ 使用密码学保证传输和访问安全
- ✓ 数据一致存储、难以篡改、防止抵赖的记账技术，也称分布式账本技术





创新模式与挑战

区块链多种技术的集成创新



点对点网络
密码学
共识机制
智能合约



提供一个在不可信网络中
进行信息与价值传递交换的
可信通道

在不可信的竞争环境低成本建立信任



跨链、隐私保护、安全监管等

区块链应用前景

1

需求：

金融、医疗、公证、通信、供应链、域名、投票等领域都在尝试利用区块链技术

2

投资：

风投热情高，投资密度大，资金供给逐步上升，充足资金有望推动技术发展

3

应用：

一种市场工具，帮助节约交易成本、管理成本，提高安全性，去除中间机构，公司业务模式转移

4

技术：

促进数据记录、数据传播、数据存储方式转型，有望改变互联网底层基础协议

5

社会结构变迁：

可融合经济和法律，改变社会监管模式及社会组织形态，走入分布式自治社会

区块链行业应用

类型	政府	金融	工业	医疗	法律	版权
价值转移		数字票据 跨境支付 应收账款 供应链金融	能源交易	医疗保险		
存证	电子发票 电子证照 精准扶贫	现钞冠字号 溯源 供应链金融	防伪溯源	电子病历 药品追溯	公证 电子存证 网络仲裁	版权确权
授权管理	政府数据 共享	征信		健康数据 共享		版权管理



数据科学(Data Science)

➤ 一门研究和探索数据的理论、方法、技术及其应用的学科

包括数据获取、数据存储与管理、数据安全、数据分析、可视化的基础理论和技术，形成新的科学研究方法，以及专门领域的数据学，
如：行为数据学、生命数据学、脑数据学、气象数据学、金融数据学、地理数据学

- ✓ 研究数据内涵及规律和现象
- ✓ 为自然科学和社会科学研究提供新方法，揭示自然界和人类行为现象和规律
- ✓ 对社会及产业发展提供预测依据



大数据的处理



➤ 现有及历史数据的处理

存储, 格式转化, 分析, 描述, 挖掘, 检索, 查询, 安全

➤ 正在采集的数据处理

传输, QoS, 存储, 格式化, 分析, 描述, 挖掘, 归档, 检索, 查询, 安全

➤ 未来产生数据的处理

预测, 传输, QoS, 存储, 格式化, 分析, 描述, 挖掘, 检索, 查询, 安全



大数据处理的分类处理

➤ 结构化数据

在数据库中，可用二维表结构来逻辑表达实现的数据

➤ 半结构化数据

不用数据库二维逻辑表来表现的数据，如XML、HTML、各类报表等

➤ 非结构化数据

字段长度可变，如文本、图像、音视频等数据



大数据处理的理论基础

✓ 北京大学 数学学院 教授 鄂维南 (E Weinan) 院士 :

“数据科学所依赖的两个因素是数据的**广泛性和多样性**，以及数据研究的**共性**”

“数据科学主要包括两个方面：用**数据的方法来研究科学**和用**科学的方法来研究数据**”

➤ **用数据的方法来研究科学**

生物数据学、天体数据学、数字地球等领域

➤ **用科学的方法来研究数据**

数据的获取，存储，和数据的分析

✓ **涉及领域**

数字信号处理、通信技术、计算数学、计算机科学、统计学、机器学习、
人工智能、数据采集、数据库等

北京大学



数据科学的知识体系

➤ 数学基础知识

三大基础：微积分、线性代数和概率论
随机过程、函数逼近论、图论、拓扑学、几何、变分法、群论等

➤ 计算科学基本知识

计算语言、数据库、数据结构、可视化技术等

➤ 算法基本知识

数值代数、函数逼近、优化方法、机器学习、计算几何等

➤ 数据模型

回归、分类、聚类、参数估计等

➤ 专业课程

信号理论、数字信号处理、时间序列分析、图像处理、视频处理、编码理论、自然语言处理
、文本处理、语言识别、通信系统、信息安全、网络技术、移动计算、云计算等

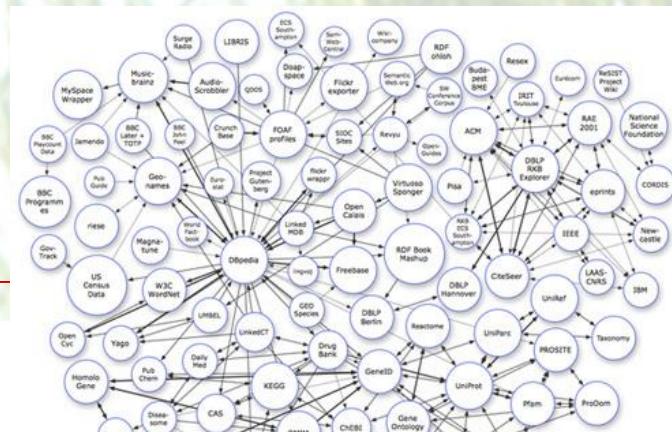
➤ 其它应用专业

生物信息学、地理信息学、金融数据，计算广告学、推荐系统等

- 1, 大数据基础知识
- 2, 统计学
- 3, 程序设计
- 4, 机器学习
- 5, 文本挖掘/自然语言处理
- 6, 可视化
- 7, 大数据和云计算
- 8, 数据获取
- 9, 数据再处理
- 10, 工具

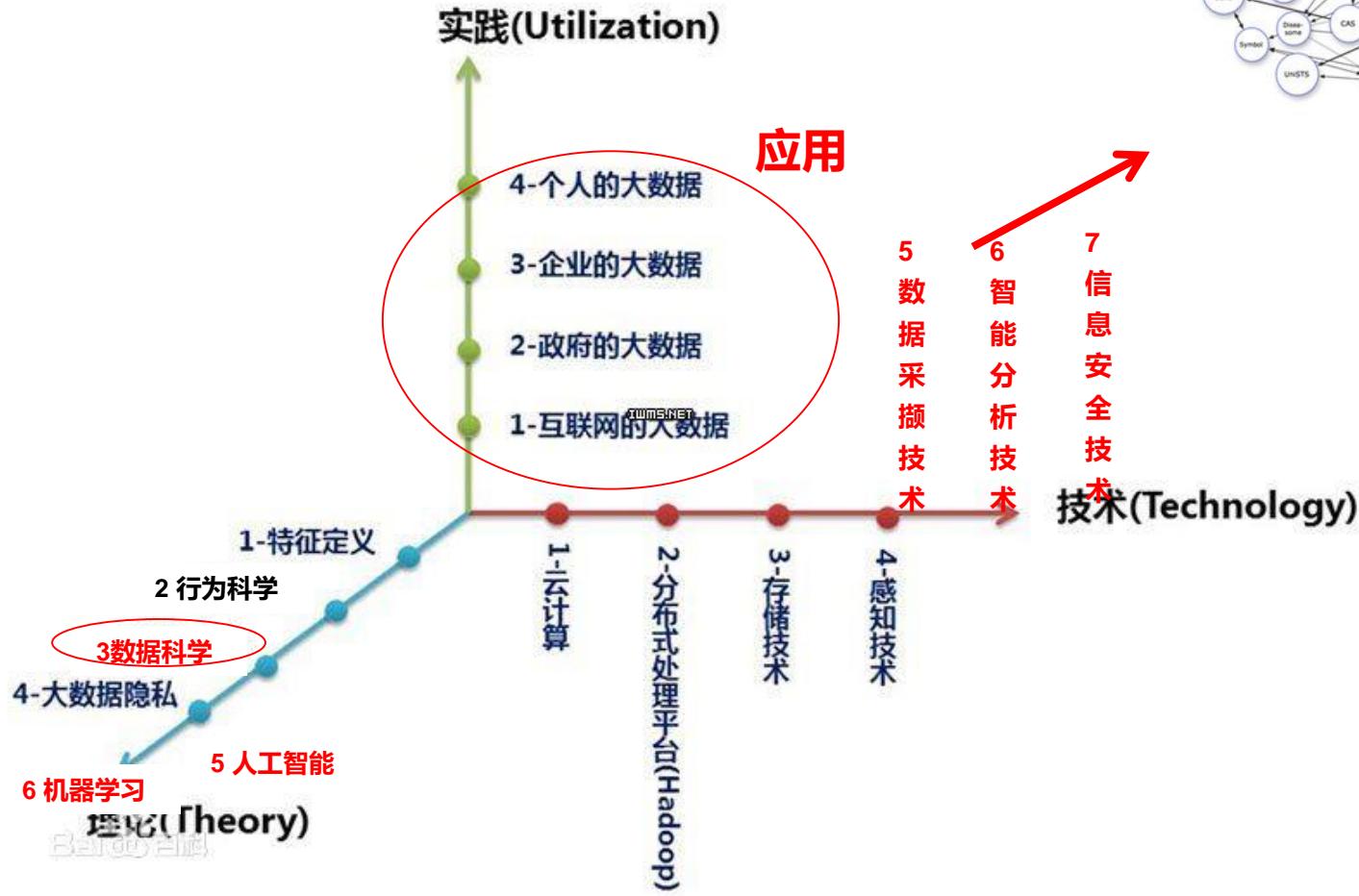
北京大学

大数据的理论与实践



IT专家网
Ciochina.com.cn

关联性



北京大学

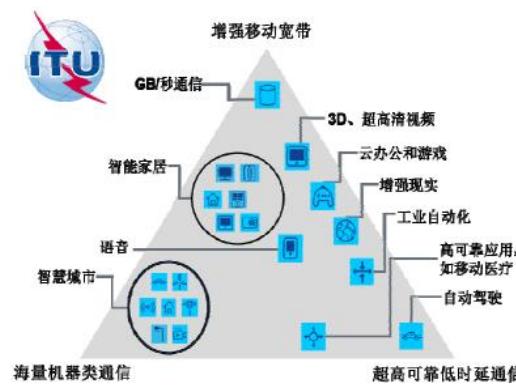
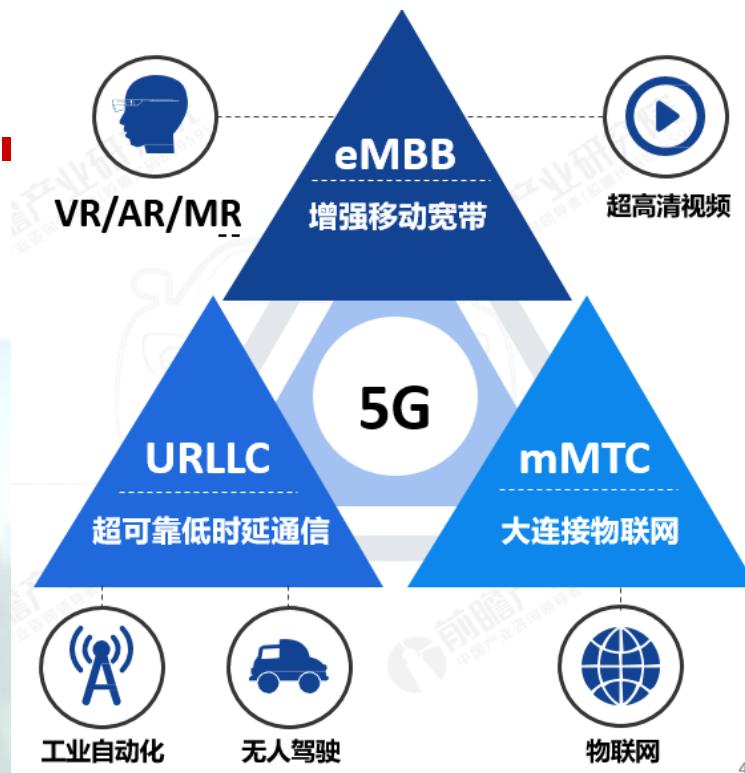
大数据处理架构



网络与信息
安全保障

北京大学

5G应用场景



移动互联网

1、连续广域覆盖场景



移动物联网

1、低时延高可靠场景



2、热点高容量场景



2、低功耗大连接场景



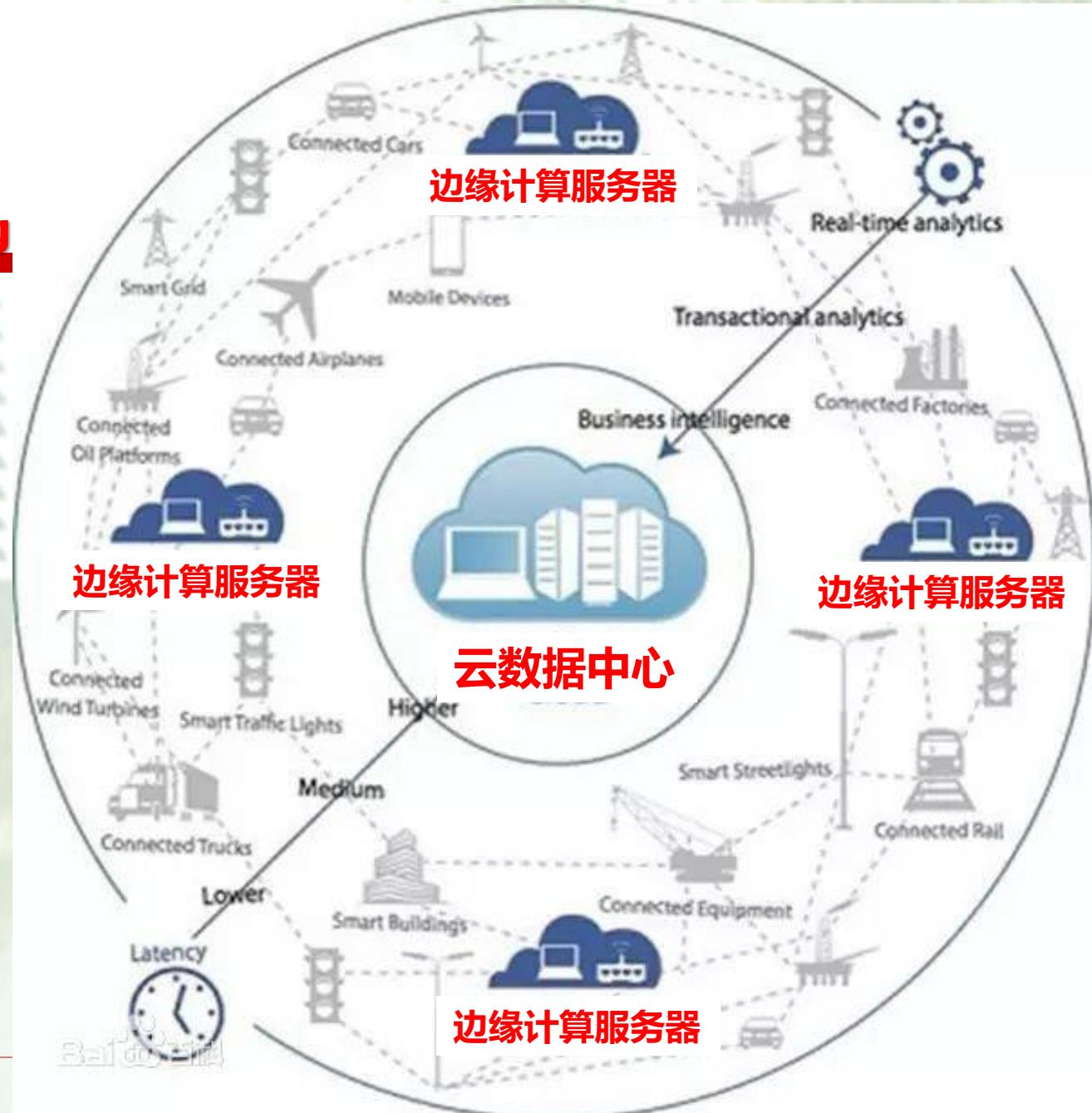
边缘计算/云计算与高带宽/低时延



边缘计算

Edge Computing

- 边缘服务器靠近终端用户，提供快速响应/计算，终端与边缘服务器交互模式
- ✓ 集支撑网络、计算、存储、应用能力为一体的服务器，就近提供最近端服务
- ✓ 快速服务响应，满足实时业务、智能应用及安全与隐私保护等需求。



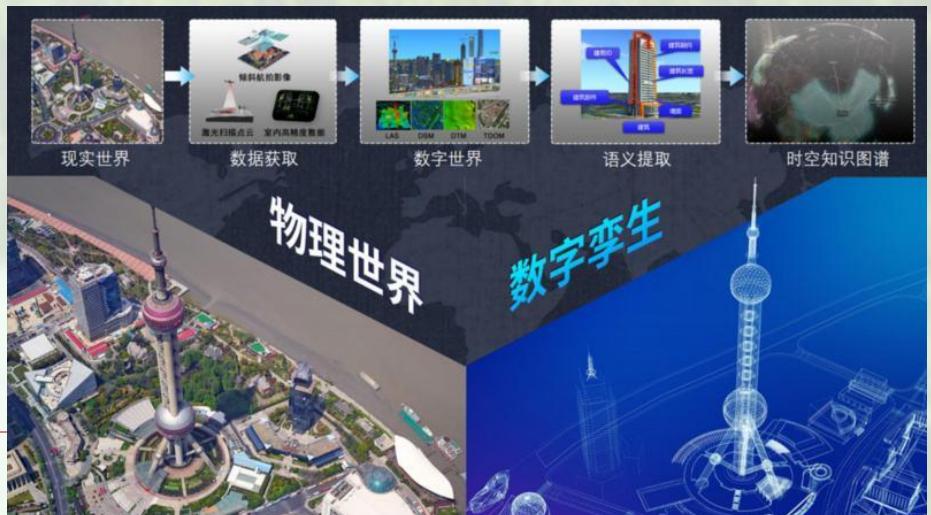
XR (扩展现实)

- 包含AR(增强现实)、VR(虚拟现实)、MR(混合现实),利用软硬件设备结合IMABCDE手段, 将虚拟内容和真实场景进行融合



数字孪生 (Digital Twins)

- 利用物理模型、传感器、运行历史等数据, 集成多参量、多尺度的仿真过程, 并映射到虚拟空间, 实现反映及展示相对应的实体的全生命周期过程



元宇宙 Metaverse



□ 时空性

空间上虚拟，时间上真实的数字世界；

□ 真实性

有现实世界的数字化复制物，也有虚拟世界的创造物；

□ 独立性

与外部真实世界既紧密相连，又高度独立的平行空间；

□ 连接性

由网络、硬件终端和用户整合的一个虚拟现实系统

➤ 由 **IMABCDEX** 及数字孪生提供融合支撑



智能环境下“人工智能+与 “互联网+”的发展模式与挑战

智能的计算能力提升



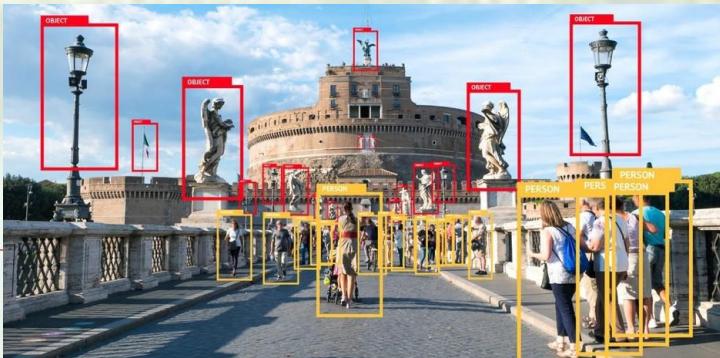
斯坦福大学和麦肯锡（McKinsey）公司报告

人工智能的计算能力每三个月左右翻一番

例子：

18个月中，在云基础架构上训练监督图像识别的网络所需的时间

2017年10月的大约3个小时 ↓ 减少到2019年7月的大约88秒





智能数据分析核心问题

- 各种数据的信号/信息空间建模；
- 时空特征度量与评测准则，为数据特征智能提取、分析聚类给出精准的科学依据；
- 权衡深度神经网络神经元层与计算复杂度的关系，优化特征提取和分类预测流程，寻求低计算复杂度的快速算法；
- 数据特征分析挖掘与敏感信息安全矛盾关系

非结构化大数据管理技术

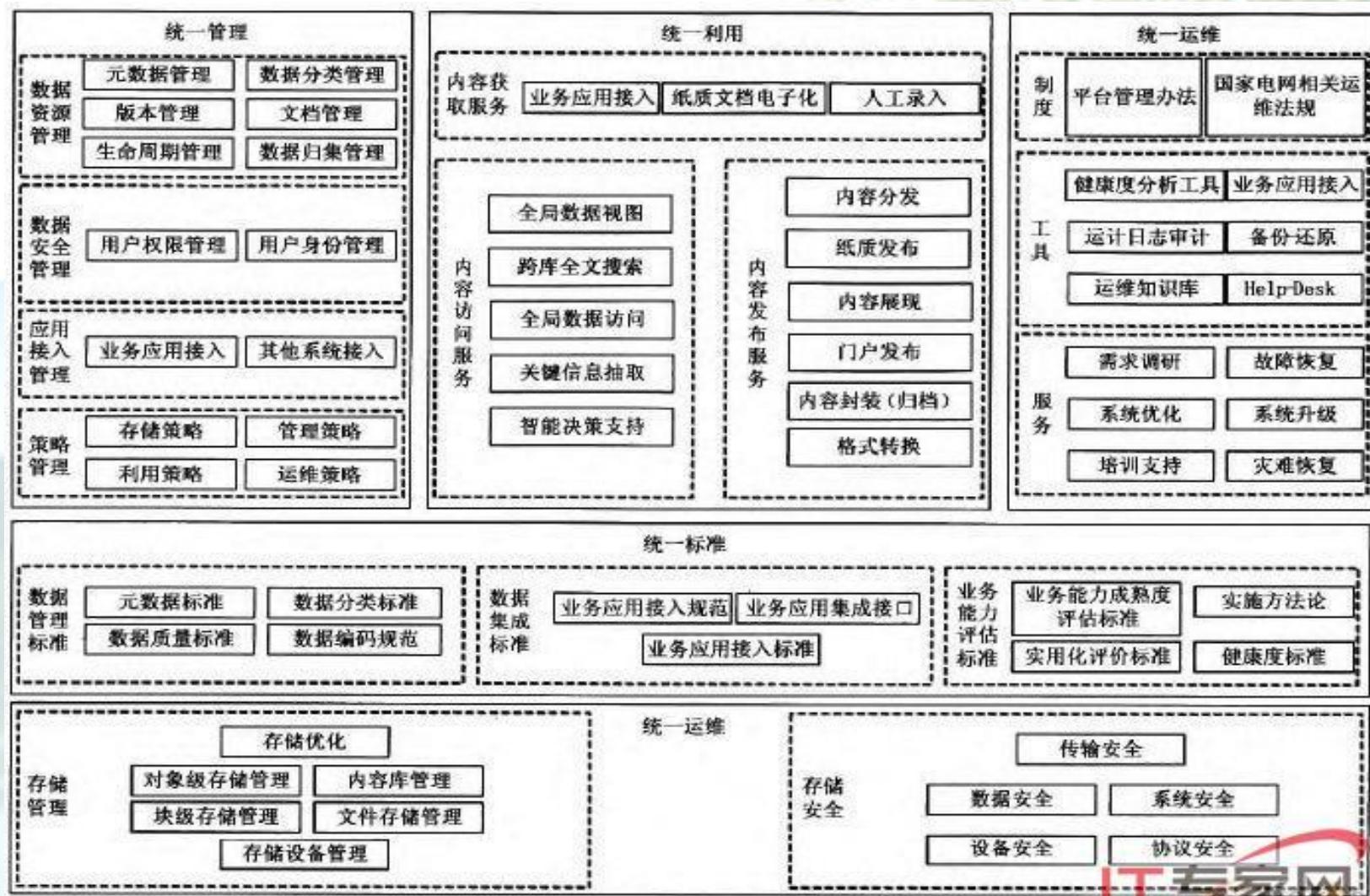
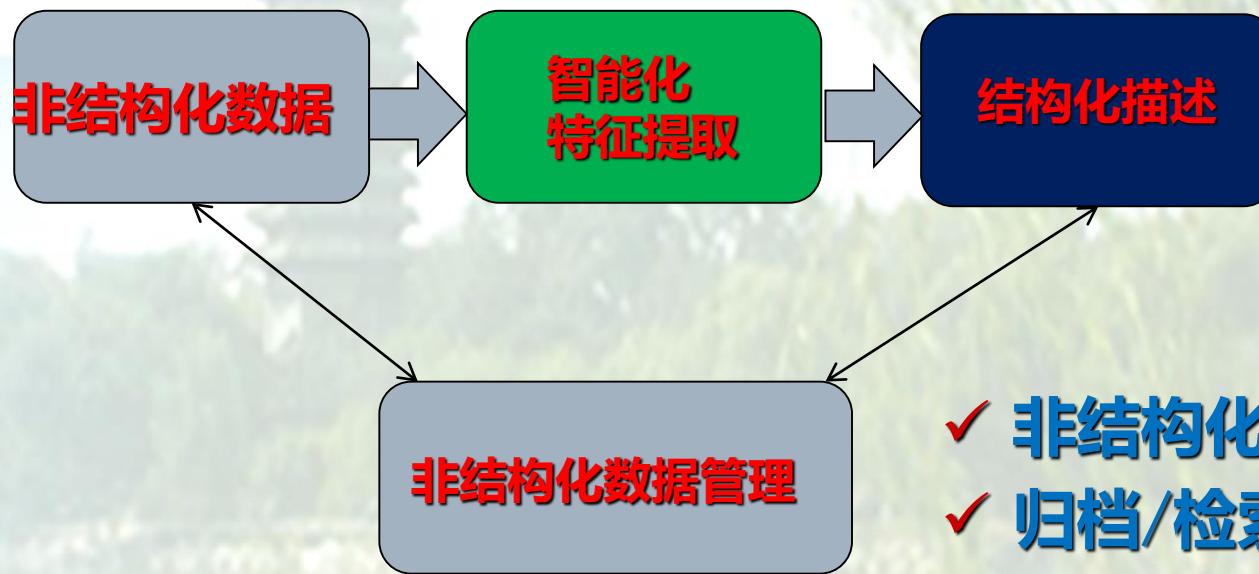


图 1 非结构化数据管理平台业务架构



非结构化大数据的结构化描述

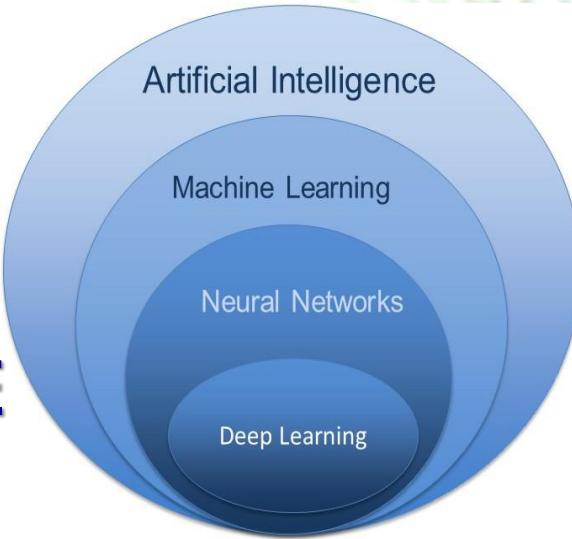
化解为结构化数据



- ✓ 非结构化数据处理引擎
- ✓ 归档/检索引擎
- ✓ 描述与分类与聚类

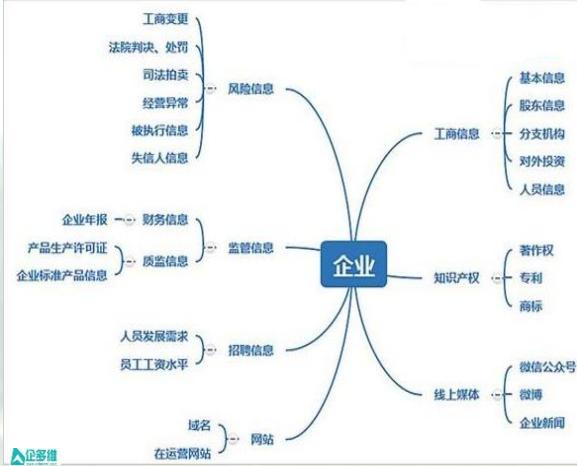
算力提升了 人工智能能力

➤ 分析及提取大数据特征

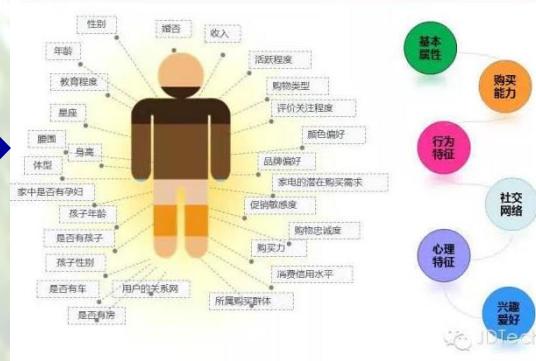


➤ 事件本质理解

企业画像



用户画像



智能物联画像



物体属性

国家新一代人工智能开放创新平台

(2017年11月至今)

- 依托百度：“自动驾驶”
- 依托阿里云：“城市大脑”
- 依托腾讯：“医疗影像”
- 依托科大讯飞：“智能语音”

- 依托商汤：“智能视觉”

- 依托上海依图：“视觉计算”
- 依托明略科技：“营销智能”
- 依托华为：“基础软硬件”
- 依托中国平安：“普惠金融”
- 依托海康威视：“视频感知”
- 依托京东：“智能供应链”
- 依托旷视：“图像感知”
- 依托360：“安全大脑”
- 依托好未来：“智慧教育”
- 依托小米：“智能家居”



智能型机器人

机器人（Robot）：分一般机器人和智能型机器人

娱乐机器人，服务机器人，产业机器人，特种机器人



可信智能交互处理

云计算/边缘计算融合模式

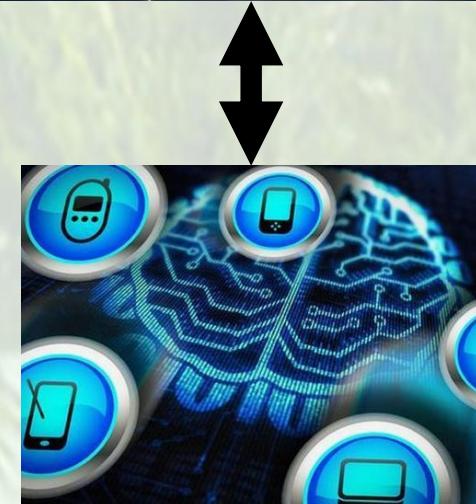
基于AI的智能生产/交互模式

✓ 大脑 - 可信云脑
智能化智慧处理中心

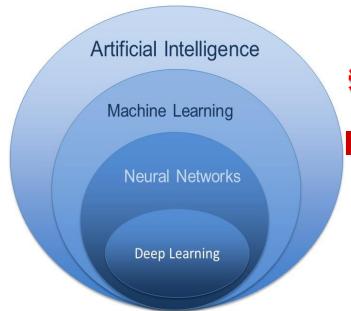
云安全常态化
智能化安全运营和管控
提供安全AI云服务

✓ 小脑 - 可信智能终端-边缘

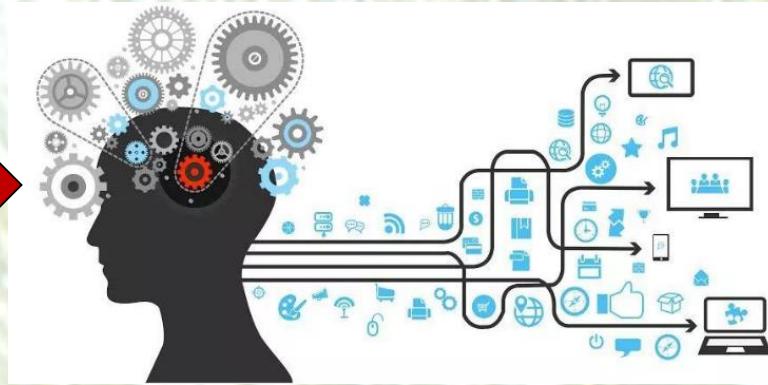
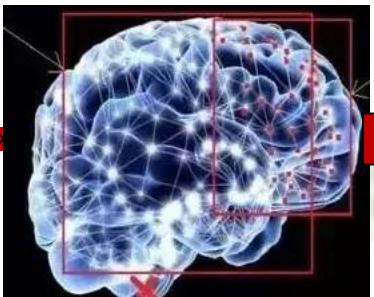
前端快速响应及安全操作



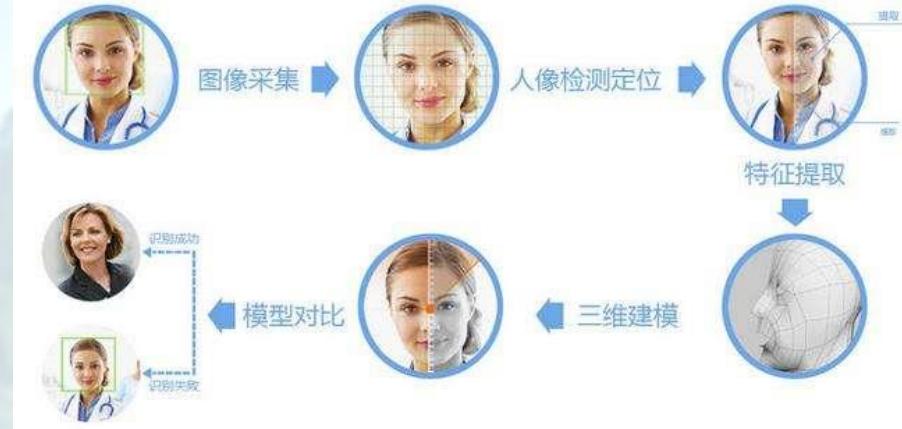
智能识别



智能 (AI)



人脸识别



刷脸门禁/安检



霍金对AI发展的忧虑

“人工智能也有可能是人类文明史的终结，除非我们学会如何避免危险。我曾经说过，人工智能的全方位发展可能招致人类的灭亡，比如最大化使用智能性自主武器。”



——物理学家 霍金

人工智能安全问题

□ “骗人”

□ “吓人”

□ “杀人”



□ AI防御

□ AI入侵

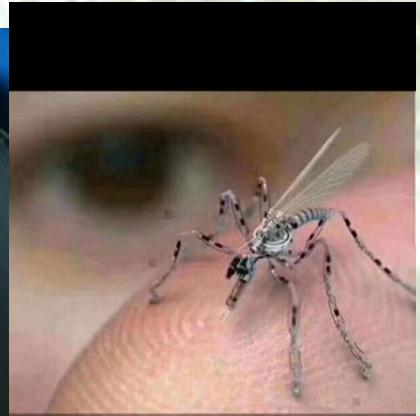
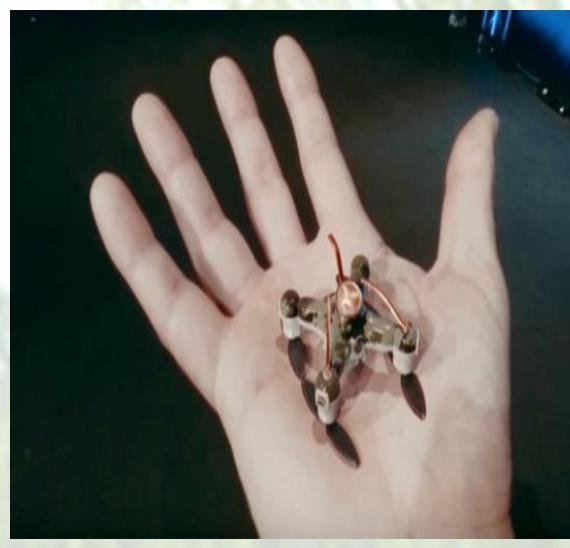
□ AI对抗

□ AI威胁

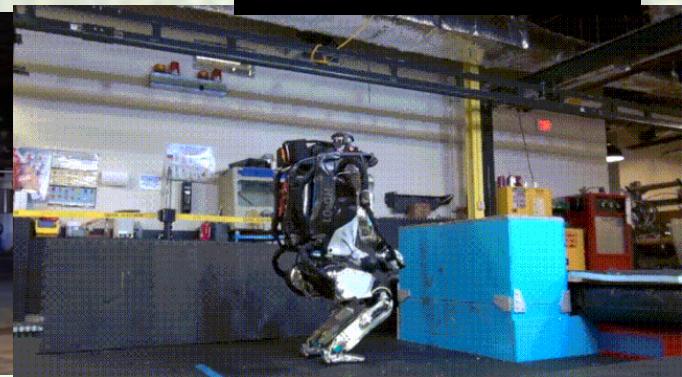
智能机器人安全？

- 很小型的智慧无人机，跟蜜蜂一样大，其处理器比人类快100倍，可躲避人类各种追踪
它的装备：广角摄像头、传感器、面部识别。只要把目标图像信息输给它，它能精准找到打击对象，戴口罩、伪装统统没用，识别率高达99.99！
- 波士顿动力(Boston Dynamics) 机器人

智能功能研制与保护?
防止受入侵攻击?



這是蚊子嗎？
不是的。這是一個針對城市地區的昆蟲間諜無人機，已經投入生產，由美國政府資助。它可以遠程控制，並配有攝像頭和麥克風。它可以降落在你身上，它可能有可能採取DNA樣品或將RFID 跟踪納米技術留在你的皮膚上。它可以通过敞開的窗戶飛過，也可以附著在你的衣服上，直到你把它放在家中。



安全?

3D打印人脸套



DeepFake



- 多模态/多因子信息的安全识别与鉴别
- 智能化(AI)主动安全防御机制

AI安全攻击(AI Security Attack)

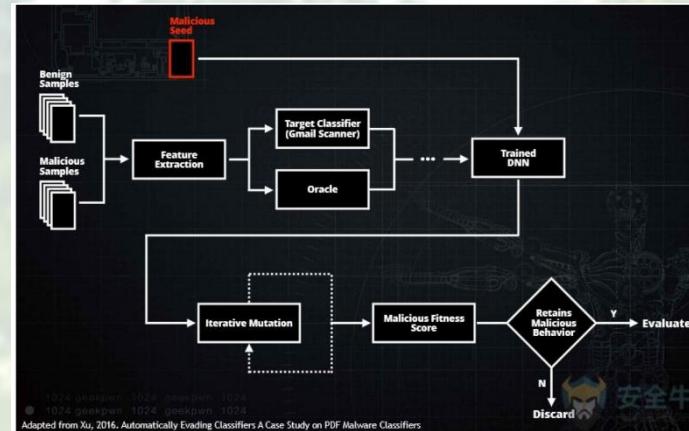
➤ AI破解人脸识别系统

攻击者通过入侵并控制该系统管理端，利用其操作系统漏洞和应用层逻辑漏洞，基于AI修改人脸识别参数，使门禁失控

➤ AI模型攻击

➤ 数据投毒

➤ 对抗式攻击



➤ 使用AI技术进行图形或者语音验证码的破解



“愚弄”机器视觉

数据安全与隐私保护挑战

Challenges of Data Security and Privacy Protection

□ 数据采集中的隐私侵犯

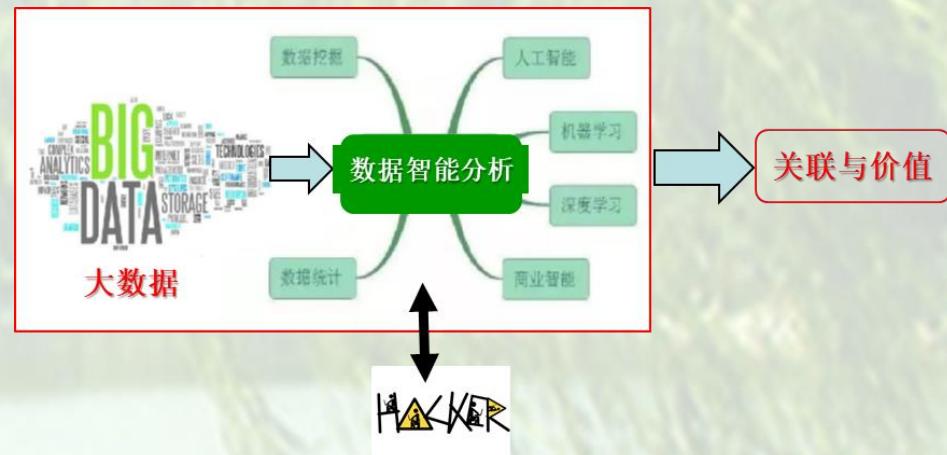
非法使用某些私人信息，就会造成隐私侵犯

□ 云计算中的隐私风险

□ 云端隐私保护问题

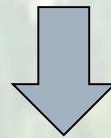
□ 知识抽取中的隐私问题

个性化定制过程又伴随着对个人隐私的发现和
曝光



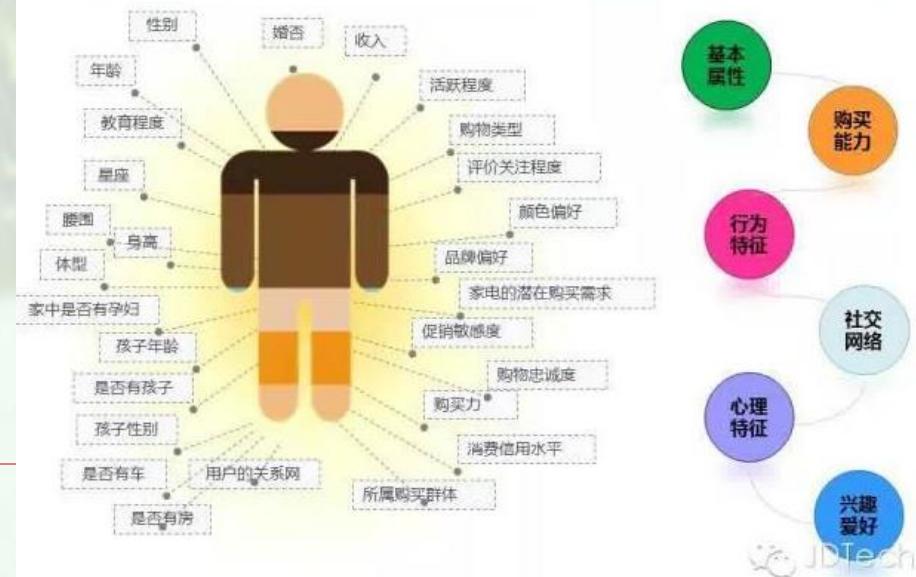
智能数据分析挖掘的安全与隐私-例子

将某人在网上浏览记录、聊天内容、购物过程、好友群和其他记录数据关联在一起，就可分析出其阅读及消费偏好和习惯，商家利用这些关联信息可预测出其潜在的消费需求，提前为其提供必要的信息、产品或服务，如果再将其个人信息以及移动接入网络的信息，包括手机号码、智能终端的硬件标识信息关联起来，就能勾画出某人的个人综合信息及行为轨迹，形成其个人画像



伴随着个人隐私的发现和曝光，带来安全威胁及风险。黑客也可拥有数据分析技术，分析挖掘所需的关联信息，对其带来安全隐患和威胁

用户画像



人工智能带来的安全挑战

➤ 技术滥用引发的安全威胁

- 通过智能方法发起网络攻击，智能化网络攻击软件能自我学习，模仿系统中用户的行为，并不断改变方法；
 - 利用人工智能技术非法窃取私人信息；
 - 通过定制化不同用户阅读到的网络内容，AI技术被用来左右和控制公众的认知和判断。
-

人工智能带来的安全挑战

➤ 技术或管理缺陷导致的安全问题

□ 某些技术缺陷，使人工智能系统出现安全隐患，

如，机器人、无人智能系统的设计、生产不当会导致运行异常等。

无人驾驶汽车、机器人和其他人工智能装置可能受到非法入侵和控制，有可能按照犯罪分子的指令，对人类产生威胁。



人工智能带来的安全挑战-攻与防

➤ DDoS网络攻击趋向于智能化

攻击者改变单一确定的顺序执行攻击步骤，能根据环境自适应地选择或预先定义决定策略路径，改变对攻击模式和行为

➤ 智能化恶意软件和勒索软件的攻击

勒索软件即服务（RaaS, Ransomware-as-a-Service）

数据绑架：攻击者通过加密受害者的数据，要求受害者为解密密钥支付费用。

➤ 勒索软件是一种木马，通过骚扰、恐吓甚至采用绑架用户文件等方式，使“用户数据资产”或“计算资源”无法正常使用，以此为条件向用户勒索
“用户数据资产”包括文档、邮件、数据库、源代码、图片、压缩文件等

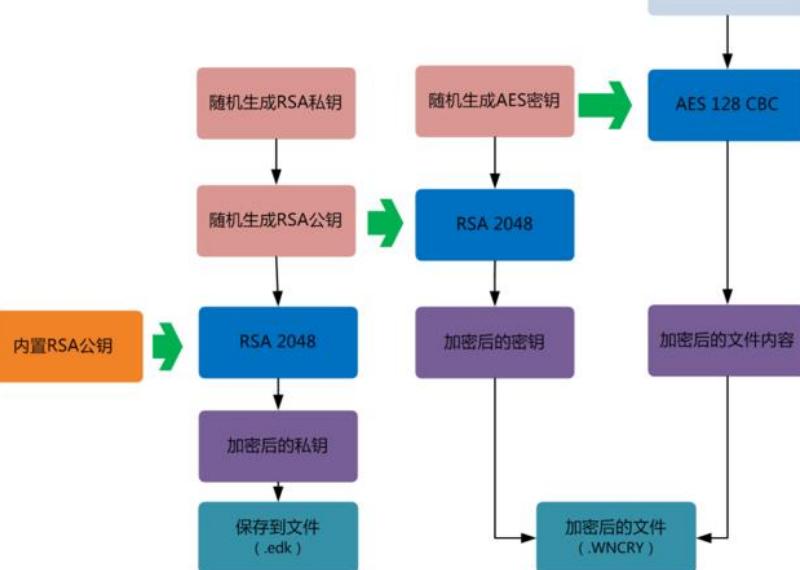
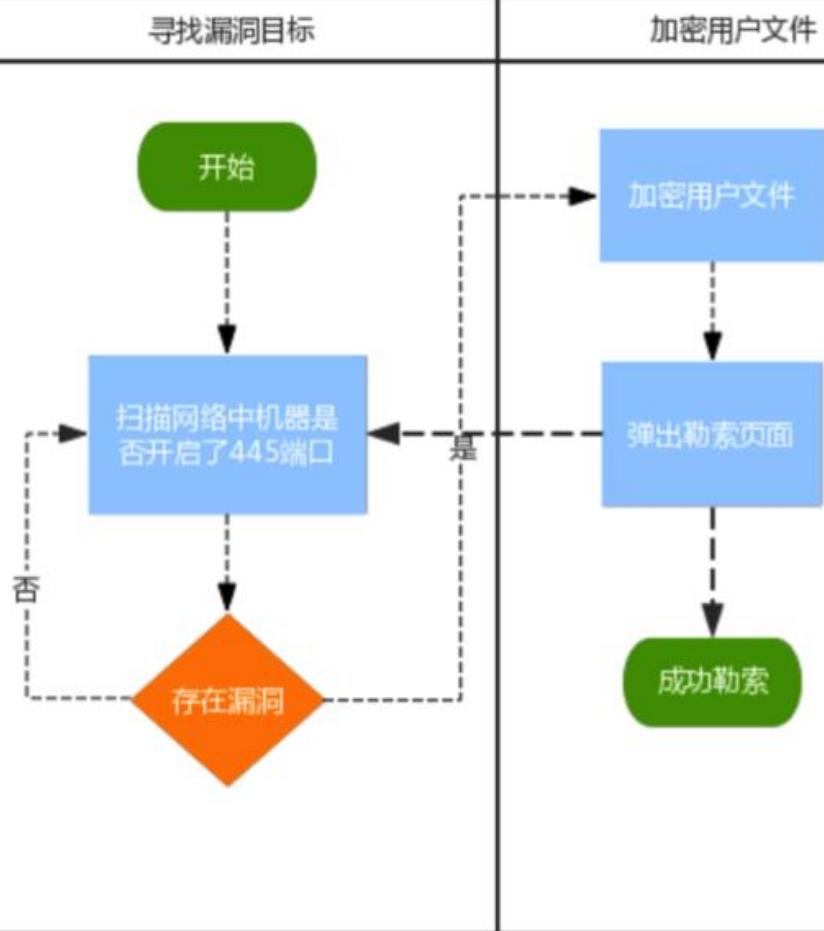
➤ 勒索形式：包括真实货币、比特币或其它虚拟货币。

设定一个支付时限，赎金数目会随着时间推移而上涨；
即使用户支付了赎金，还是无法还原被加密的文件。

基于RSA非对称加密算法的RaaS

2017年5月 “WannaCry” 的勒索病毒网络攻击席卷全球

WannaCryptor攻击流程



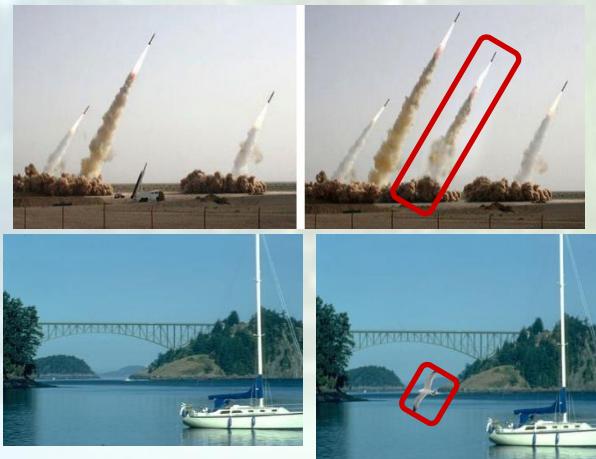
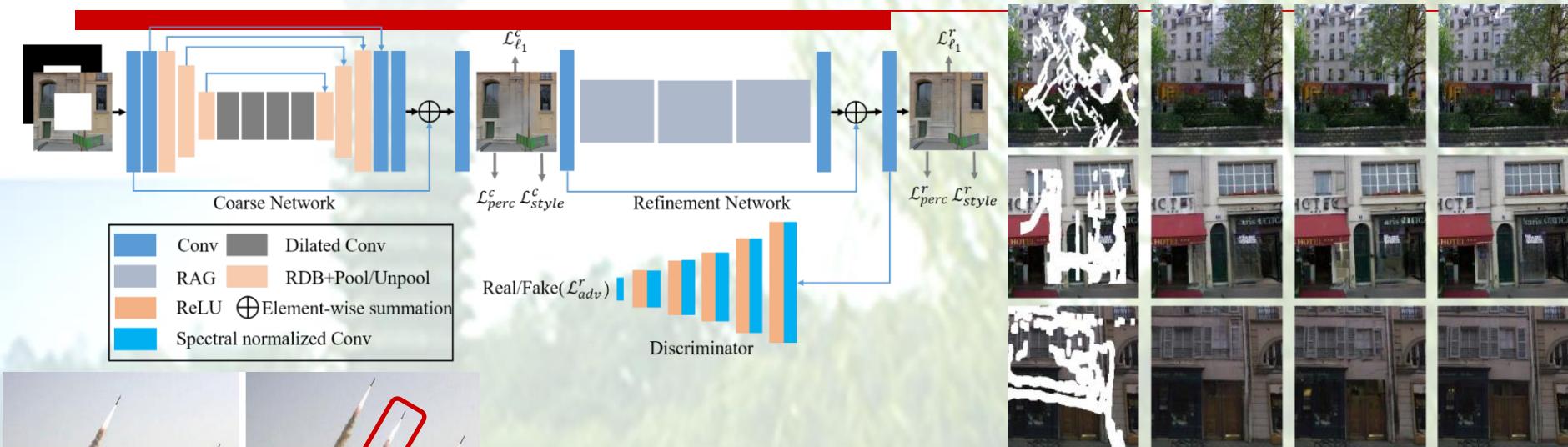
RSA-2048位：

- 1) 随机生成AES密钥
- 2) 使用AES-128-CBC方法对文件进行加密
- 3) 将对应的AES密钥通过RSA-2048加密
- 4) 将RSA加密后的密钥和AES加密过的文件写入到.WNCRY文件中

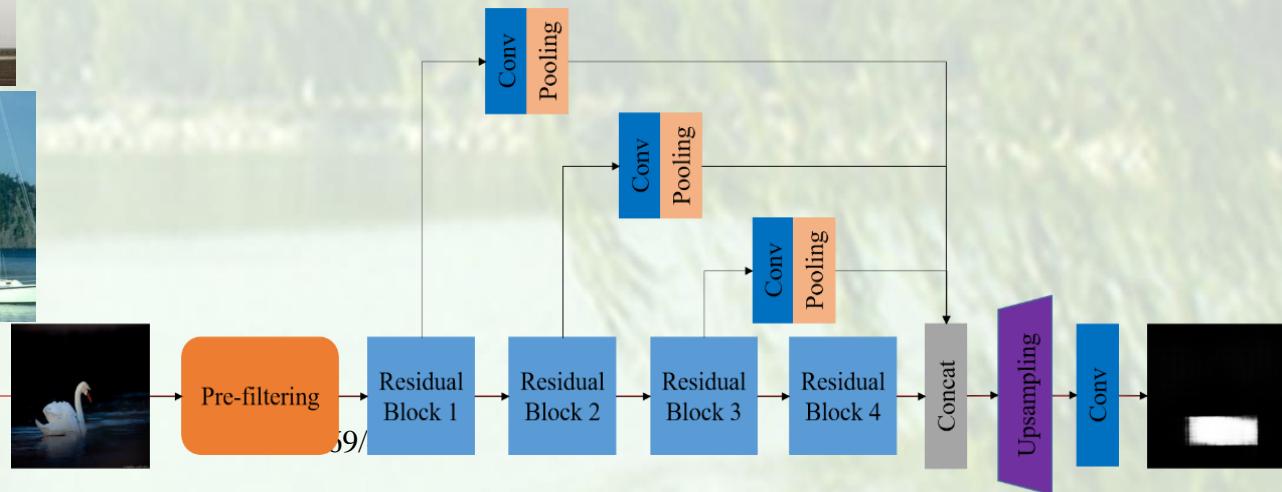
黑客利用勒索软件攻擊模式



图像修复及深度修复区域检测方法 (矛与盾的研究)



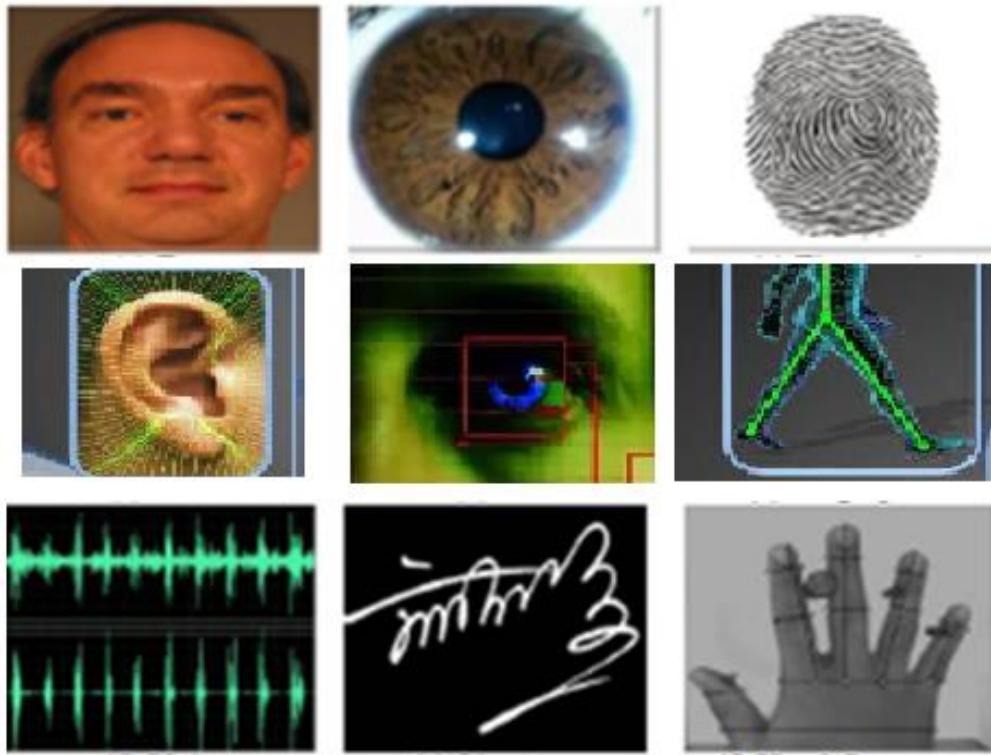
图像篡改
(Image tampering)



视频篡改(Video tampering)与检测



基于多模态多因子的身份安全识别与鉴别



生物特征识别

A Robust Single-sensor Face and Iris Biometric Identification System based on Multimodal Feature Extraction Network

Zhengding Luo, Qinghua Gu, Yueming Zhu, Zhiqiang Bai
Communication and Information Security Lab
Shenzhen Graduate School, Peking University, China
Emails: {luozd, guqh, zhuys, baizq}@pku.edu.cn

Abstract—Joint face-iris identification can integrate complementary information from face and iris to fulfill the requirement of performance improvement and security. However, most of the current face-iris multimodal biometric systems acquire face and iris with different sensors which brings about the increase of capturing complexity and device cost. Besides, they are limited by the identification performance degradation under non-ideal scenarios. In order to address these problems, a robust single-sensor face and iris biometric identification system based on multimodal feature extraction (MFE) network is proposed. Only a single sensor is needed to obtain face and iris images in the proposed system, with the goal of improving recognition performance while minimizing sensor cost and acquisition time. The MFE network is designed as a general network module to extract both face and iris features and it is trained with a triplet framework to reduce intra-class variations and enlarge inter-class variations. Our experimental results on CASIA-4-distance and FRGC v2.0 non-ideal datasets show that the proposed system achieves better identification performance in terms of Equal Error Rate (EER) and False Reject Rate (FRR), etc. compared with other unimodal and multimodal biometric systems.

Index Terms—multimodal biometrics, face and iris recognition, non-ideal biometrics, deep learning, a single sensor

I. INTRODUCTION

Traditional identification techniques include password-based schemes and token-based schemes. However, these schemes are vulnerable to attacks when the passwords are divulged or the tokens are stolen. Biometric recognition refers to automatic identification using certain physiological or behavioral traits associated with an individual. These biometric traits include face, fingerprint, iris, palmprint and voice, etc. which have an edge over traditional identification approaches because they cannot be stolen or shared [1]. But unimodal biometric systems are limited by some inherent drawbacks such as lack of uniqueness, restricted degrees of freedom, non-universality, sensitivity to noisy data, vulnerability to spoofing and unacceptable error rates [2]. Multimodal biometrics can fuse information from multiple modalities to overcome the limitations of single modality and enhance discriminant ability [3]. Apart from that, multi-biometric systems increase the resistance to spoofing attacks by making it difficult to spoof multiple modalities simultaneously [4].

Among biometric traits, face and iris have received significant attention because of many outstanding characteristics.

Face recognition is the most natural and acceptable way in biometric recognition, whereas photographs, videos, 3D masks and other spoofing ways make face recognition less reliable [5] [6]. Iris is one of the most promising biometric traits due to its unique textures, which is stable until the end of human life unless there are accidents [7]. Iris images are usually acquired within a short distance under near-infrared illumination [8]. However, iris recognition may suffer from identification performance degradation when image acquisition is not constrained strictly. Therefore, the pros and cons of face and iris can complement each other to enhance the overall recognition performance and security [9].

While research into face-iris multimodal biometrics has received a large increase over recent years, many related experiments are based on **chimeric datasets** (i.e. face modality and paired iris modality come from different users) due to a lack of real-user datasets (i.e. face modality and corresponding iris modality come from the same person) [10]. The independent acquisition of each modality from different sensors may increase sensor cost, data acquisition time and the risk of spoofing in chimeric datasets. It is much more desirable to acquire multiple modalities from a single sensor for security and usability reasons in practice [11], [12]. In addition, since iris images can be extracted from face images without incurring additional hardware cost as shown in Fig. 1, it is economical and convenient to obtain face and iris samples using a single sensor device.

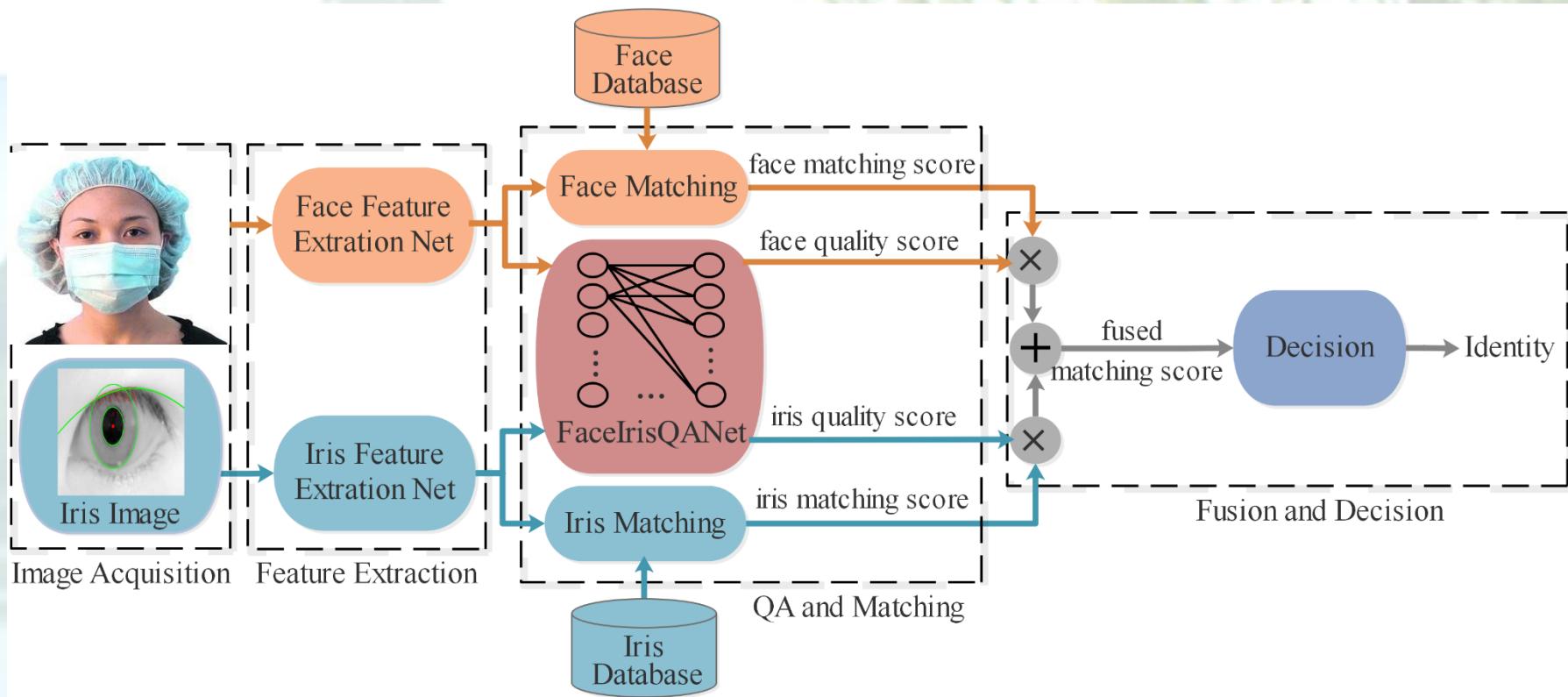
It is common and unavoidable to deal with some noisy factors such as off-angles, reflections, illumination changes and blurred images under less-constrained or non-ideal scenarios. These noisy factors result in the recognition performance drop and lack of security in face-iris multimodal biometric systems. Therefore, development of a robust face-iris multimodal biometric system is highly desirable. The key contributions of this paper are summarized as follows: (1) We propose a face-iris multimodal biometric system combining information from face and iris to enhance the limited discriminant ability of unimodal biometrics. Besides, the proposed system exhibits superior robustness under non-cooperative environments. (2) A **multimodal feature extraction (MFE)** network is developed to extract face and iris features in our system. The MFE network is a modality-general network and it is trained with a triplet

疫情场景：口罩



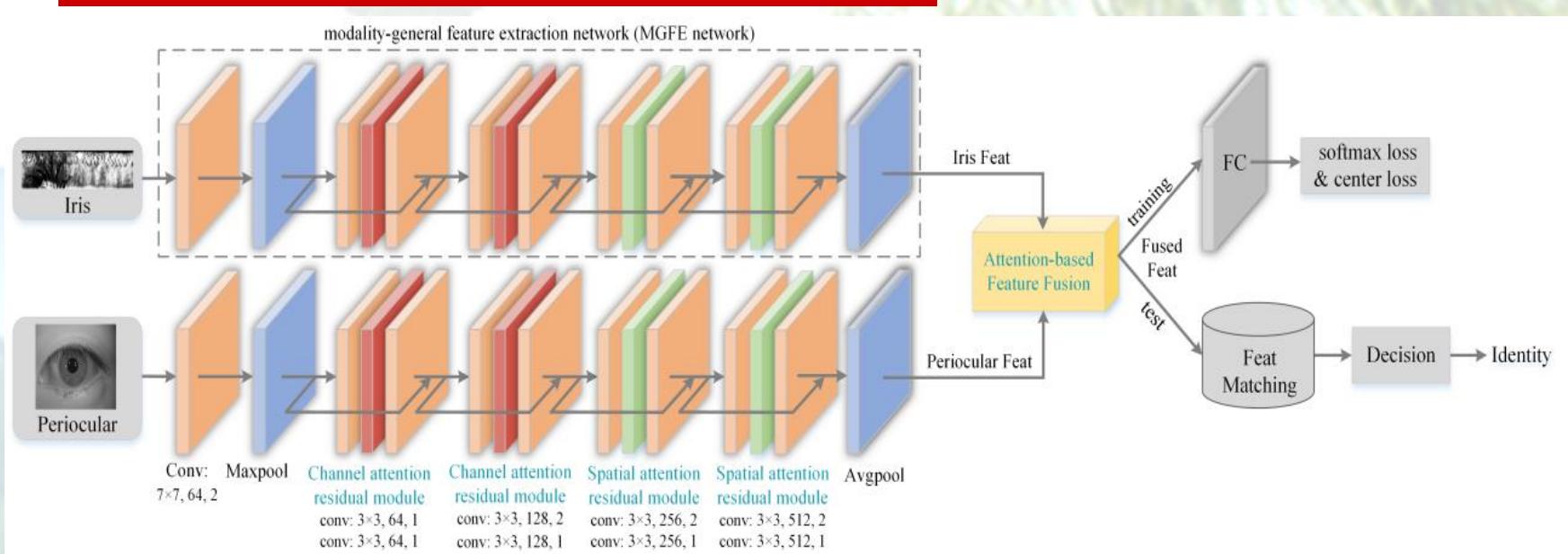
疫情场景下的智能安全

虹膜/人脸/人耳/形态等特征融合安全识别与鉴别



虹膜与眼周融合安全识别与鉴别

基于注意力机制的虹膜-眼周特征层融合



由特征提取网络（MGFE network）和基于注意力的特征融合模块组成。既可提取虹膜也可提取眼周特征。MGFE网络包括卷积层、最大池化层、四个残差模块和平均池化层

Luo, Z., Zhu, Y., et al. "An Efficient Deep Learning Framework based on Multiple Attention Mechanisms for Joint Iris-Periocular Biometric Recognition", IEEE Signal Processing Letters, Vol 28, pp.1060-1064, 2021.

面向难区分及可形变微小动物的 多目标跟踪算法研究

➤ 生命科学领域的重要分支
➤ 疫苗、药物的研发，基因研究

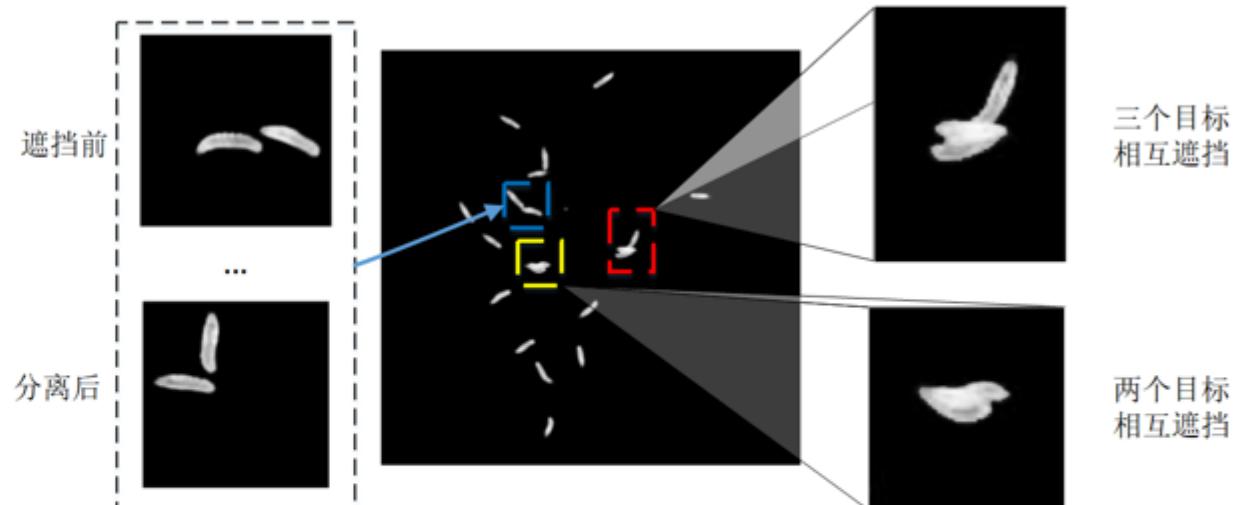
□ 难区分及可形变的微小动物多目标跟踪难点

多个目标相互遮挡时

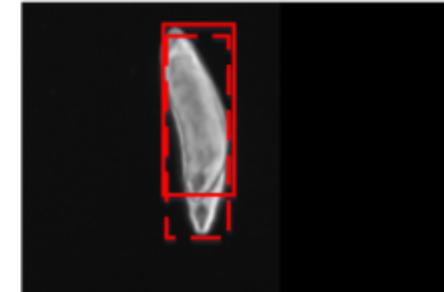
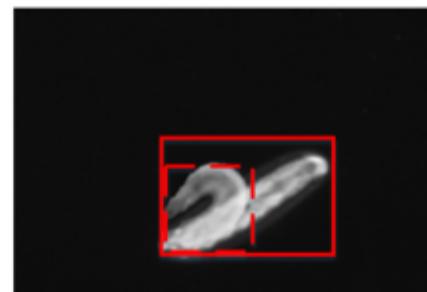
● 难区分性

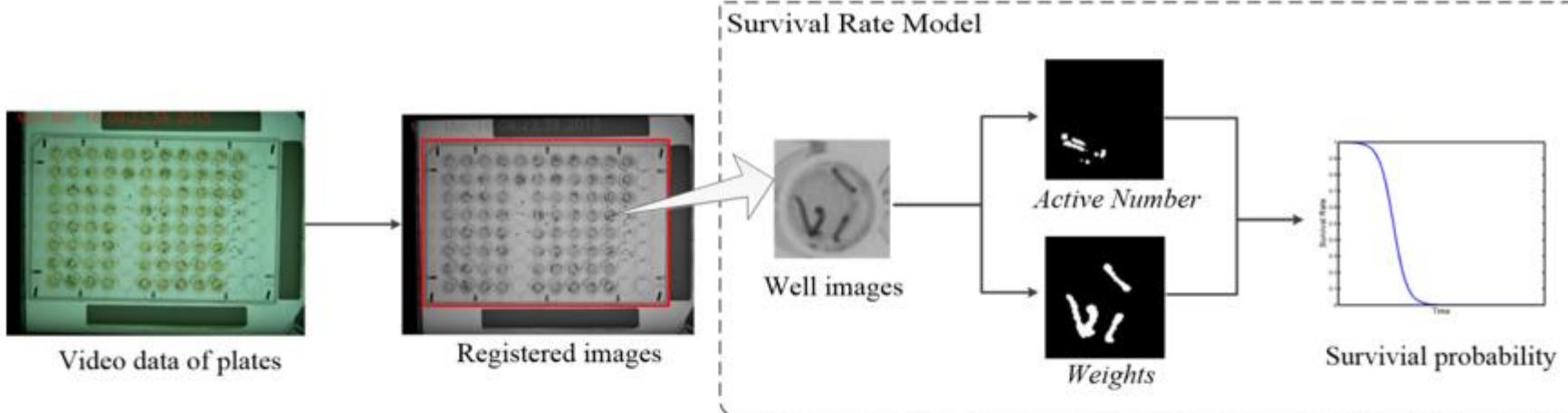
● 非刚体变形

● 运动随机性

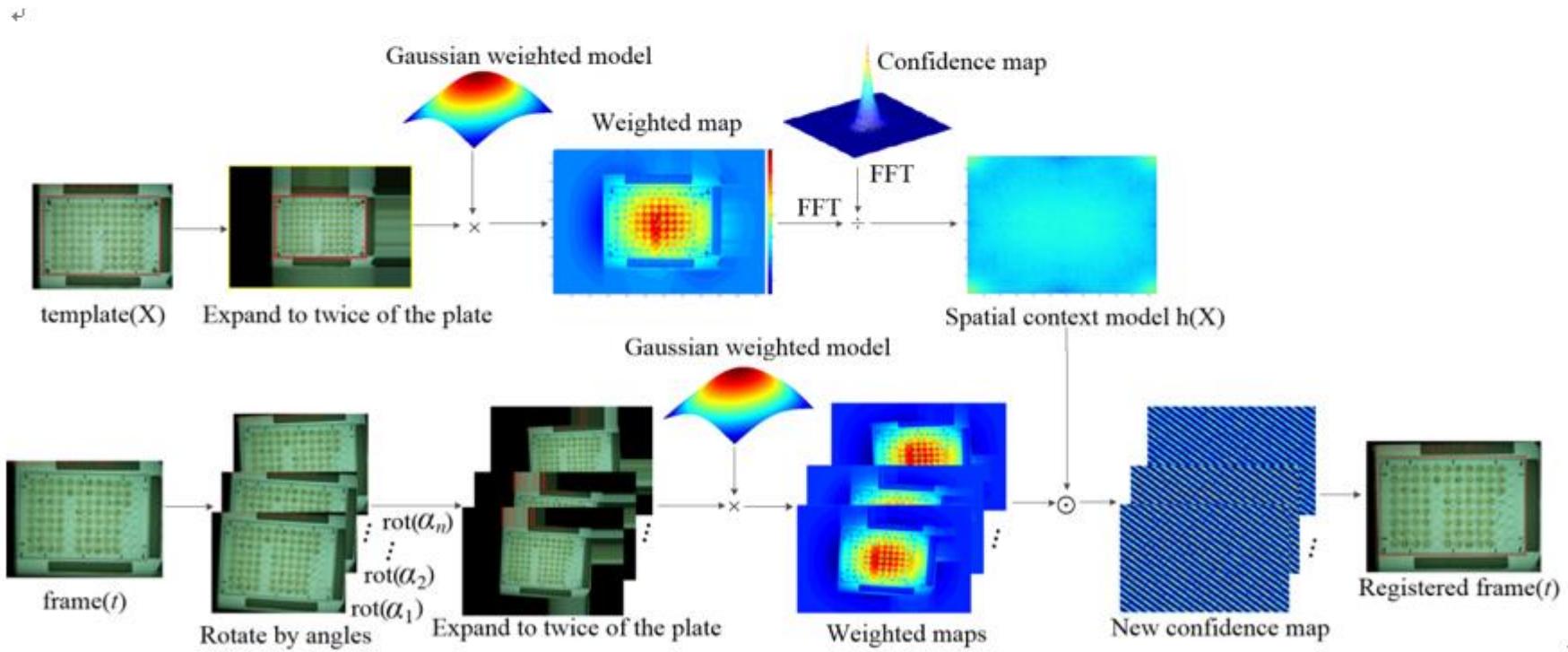


- 难以对遮挡前后目标的身份进行匹配
- 难以跟踪遮挡期间每个目标的状态





面向难区分及可形变微小动物的多目标跟踪算法研究

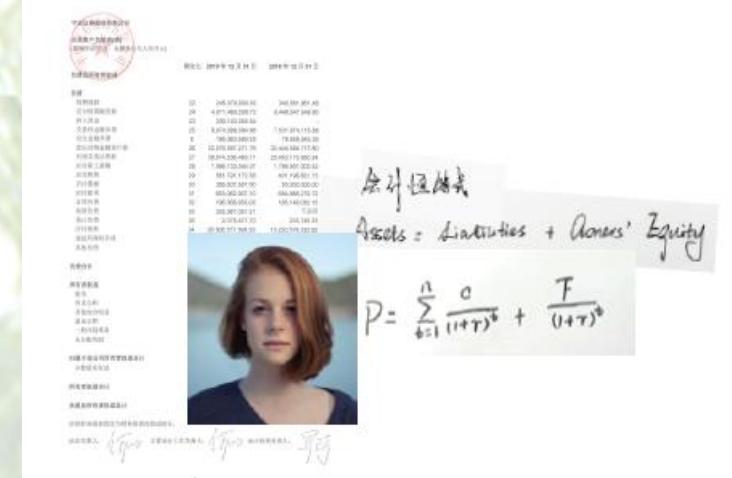


面向应用场景的智能分析处理

金融科技应用研究

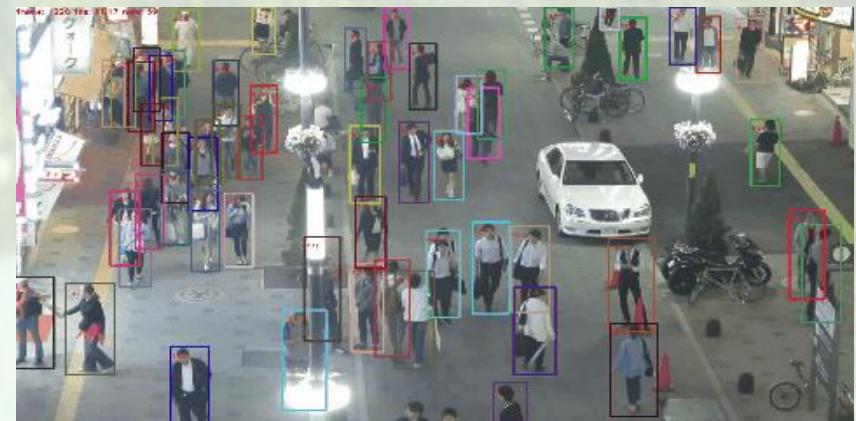
- 手写字和数学公式的智能检测与识别

对图片中的字母、手写字、表格、数学公式等字符进行**智能**检测和识别。



- 多目标进行自动识别及跟踪

用于安防及疫情监控



《2022亚太绿色低碳发展高峰论坛》

面向碳中和的智能信息生态环境：挑战及创新

Intelligent information ecological environment for
carbon neutrality: Challenge and innovation

北京大学 信息工程学院

朱跃生

2022年9月8日
长沙

北京大学

I M A B C D E X S 先进信息技术

不是简单的集成，而是深度融合

These advanced information technologies are not simply integrated, should be deeply fused

- I M A B C D E X S 等先进信息技术本身带来高能耗及大量碳排放问题，不是简单的集成，而是深度融合

These advanced information technologies (I M A B C D E X S) themselves bring high energy consumption and a lot of carbon emissions, so they are not simply integrated, should be deeply fused

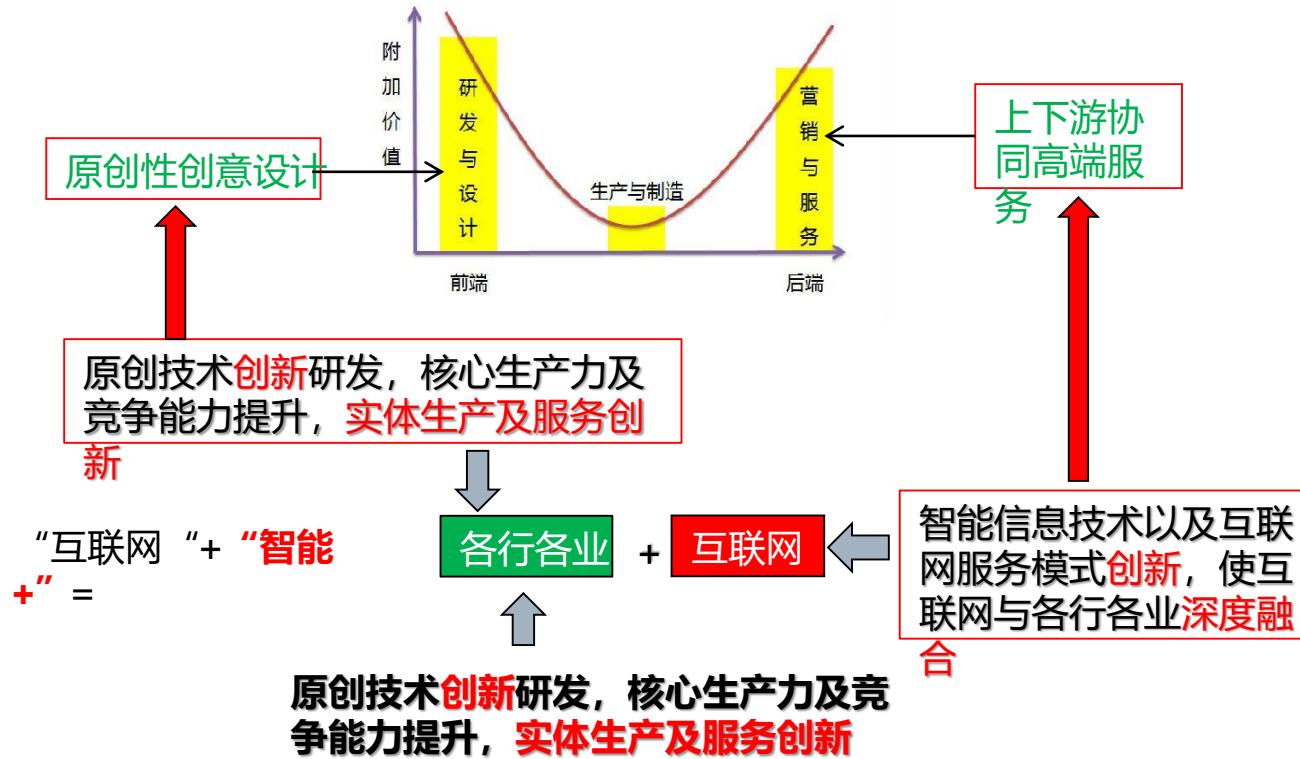
例：AI的算力提升需要服务器/协处理的集群，引入了附加的高能耗及碳排放，因此在选择AI中的机器学习算法做为数据分析模型时，建议根据实际应用场景，做好以下几点：

eg: The AI computing power boost requires server / co-processing clusters, but additional high energy consumption and carbon emissions are introduced, so when selecting the machine learning algorithm in AI as a data analysis model, it is recommended that, according to the actual application scenarios, do the following:

1. 数据特征工程设计
2. 数据集的选择
3. 采集过程设备及数据格式的选择与设计
4. 传输带宽及网络的选择
5. 低复杂度高级机器学习模型的设计与选用
6. 云计算工作模式的选择
7. 硬件设备研发时选用低功耗专用芯片

- Data Feature engineering design
- Selection of datasets
- Selection and design of the acquisition process equipment and data format
- Transmission bandwidth and network selection
- Design and Selection of the Low-complexity Advanced Machine Learning Model
- Selection of cloud computing working mode
- In hardware equipment development, select low-power consumption special chip

“微笑曲线”的变革





联系方式 Email: zhuys@pku.edu.cn

*Thank
You!*



北京大学