

2024年 十大数字技术趋势与 其安全挑战



CSA GCR

@2023 云安全联盟大中华区—保留所有权利。你可以在你的电脑上下载、储存、展示、查看及打印，或者访问云安全联盟大中华区官网（<https://www.c-csa.cn>）。须遵守以下：（a）本文只可作个人、信息获取、非商业用途；（b）本文内容不得篡改；（c）本文不得转发；（d）该商标、版权或其他声明不得删除。在遵循《中华人民共和国著作权法》相关条款情况下合理使用本文内容，使用时请注明引用于云安全联盟大中华区。

联盟简介

云安全联盟 (Cloud Security Alliance, CSA) 是中立、权威的全球性非营利产业组织, 于2009年正式成立, 致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识, 推动数字安全产业全面发展。

云安全联盟大中华区 (Cloud Security Alliance Greater China Region, CSA GCR) 作为CSA全球四大区之一, 2016年在香港独立注册, 于2021年在中国登记注册, 是网络安全领域首家在中国境内注册备案的国际NGO, 旨在立足中国, 连接全球, 推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息



加入我们



CSA大中华区官网
(<https://c-csa.cn>)



点击会员



加入联盟



填写相关申请信息



成为CSA会员



JOIN US

致谢

《2024 年十大数字技术与其安全挑战》由云安全联盟大中华区专家撰写，感谢以下专家的贡献：

项目组组长：

张 淼

主要贡献者：

郭春梅 余晓光 闫新成 邢海韬 刘广坤 初 江 高振宇 宗 良

李卓嘉 林艺芳 贺志生 任永攀 王曦光 何伊圣 许冠行

项目评审组：

张 淼 郭鹏程 杨天识 姚 凯

研究协调员：

罗智杰 卜宋博 闭俊林

贡献单位：

华为技术有限公司

中兴通讯股份有限公司

北京沃东天骏信息技术有限公司

北京启明星辰信息安全技术有限公司

上海缔安科技股份有限公司

(以上排名不分先后)

关于研究工作组的更多介绍,请在 CSA 大中华区官网(<https://c-csa.cn/research/>)
上查看。在此感谢以上专家及单位。

如此文有不妥当之处,敬请读者联系 CSA GCR 秘书处给与雅正! 联系邮箱

research@c-csa.cn; [国际云安全联盟 CSA 公众号](#)



序言

随着数字技术的迅猛发展，越来越多的组织和个人在数字化环境中开展业务和活动，享受着数字技术带来的便利和创新。在这个数字化时代，各种技术如量子计算、6G 通讯技术、人工智能、数字孪生等技术带给世界新的生产方式的同时也带来了很大的安全挑战。

本报告旨在针对数字技术，详细梳理数字技术发展产生的安全挑战，并通过与相关的 CSA 研究对应，将这些安全挑战一一列举出来。本文包含十个与数字技术相关的安全挑战，涵盖了组织和个人等方面的安全应对策略。

通过全面分析数字技术发展趋势及随之产生的安全挑战，组织可以预测可能出现的新型攻击方式和漏洞，从而及时采取必要的安全措施。同时可以更好地评估其现有安全措施的有效性，并进行必要的改进，以提高整体的安全性。

相信通过阅读本报告，组织可以深入了解数字技术发展趋势及相关的安全挑战，组织可以更好地应对当前和未来的安全威胁，并采取相应的措施来保护数字资产。我们希望本报告对于提高数字技术安全意识、加强防御措施以及规避潜在威胁带来积极的促进作用。



李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目 录

致谢	4
序言	6
1 数字技术的发展现状	10
1.1 数字技术的概述	10
1.2 数字技术带来的机会和安全挑战	11
1.3 数字技术的迅猛进步和广泛应用深刻影响社会、经济和科技	12
2 2024 年十大数字技术趋势	13
2.1 量子计算	13
2.1.1 量子计算的定义	13
2.1.2 量子计算的应用	14
2.1.3 量子计算的未来预测	15
2.2 6G 通信技术	16
2.2.1 6G 通信的定义	16
2.2.2 6G 通信当前应用	17
2.2.3 6G 通信未来预测	18
2.3 人工智能	18
2.3.1 人工智能的定义	18
2.3.2 人工智能的应用	20
2.3.3 人工智能的未来预测	21
2.4 云原生	22
2.4.1 云原生的定义	22
2.4.2 云原生的应用	24
2.4.3 云原生的未来趋势	25
2.5 数字孪生	26
2.5.1 数字孪生的定义	26
2.5.2 数字孪生的应用	26
2.5.3 数字孪生的趋势	29
2.6 隐私保护	31
2.6.1 隐私保护技术的定义	31
2.6.2 隐私保护技术应用	31
2.6.3 隐私保护未来预测	32

2.7 Web4.0	33
2.7.1 WEB4.0 技术的定义	33
2.7.2 WEB4.0 技术应用	34
2.7.3 WEB4.0 的技术预测	35
2.8 卫星通讯	35
2.8.1 卫星通讯的定义	35
2.8.2 卫星通讯的应用	36
2.8.3 卫星通讯的趋势	37
2.9 算力网络	38
2.9.1 算力网络的定义	38
2.9.2 算力网络当前应用	38
2.9.3 算力网络未来预测	40
2.10 物联网技术	41
2.10.1 物联网技术的定义	41
2.10.2 物联网技术当前应用	43
2.10.3 物联网技术未来预测	43
3 2024 数字技术的安全挑战	45
3.1 量子计算的安全挑战	45
3.2 6G 通信技术的安全挑战	46
3.3 人工智能的安全挑战	47
3.4 云原生的安全挑战	49
3.5 数字孪生的安全挑战	51
3.6 隐私保护的安全挑战	52
3.7 Web4.0 的安全挑战	53
3.8 卫星通讯的安全挑战	55
3.9 算力网络的安全挑战	57
3.10 物联网技术的安全挑战	58
4 应对策略与案例研究	59
4.1 量子计算的安全应对策略及案例	59
4.2 6G 通信技术的安全应对策略及案例	62
4.3 人工智能的安全应对策略及案例	64
4.4 云原生的安全应对策略及案例	66
4.5 数字孪生的安全应对策略及案例	69
4.6 隐私保护的安全应对策略及案例	72
4.7 Web4.0 的安全应对策略及案例	74

4.8 卫星通讯的安全应对策略及案例	75
4.9 算力网络的安全应对策略及案例	78
4.10 物联网技术的安全应对策略及案例	81
5 总结	84

CSA GCR

1 数字技术的发展现状

1.1 数字技术的概述

“数字技术”并不是凭空创造而出，而是随着互联网的迭代与发展，在市场需求中应运而生出来的一门技术。它是指组织在处理或存储数据和完成许多其他功能时所应用的电子工具、设备、系统和资源，目的在于提高组织与员工的生产力和效率。

此外，数字技术包含传统意义上的信息化技术、互联网技术等较为耳熟能详、广为认知的概念与领域，也包含诸如大语言、数字孪生、虚拟仿真、量子计算等新兴或尚处于实验室，甚至理论阶段的技术。

目前，谈到数字技术时候，涉及的重点范畴主要包括但不限于：

- **商业技术：**帮助企业提升运营，如数字营销、数据管理等。
- **IT—信息技术：**涵盖硬件、软件等，使得数据收集、存储和传输更加高效。
- **通信技术：**如 5G、6G、Wi-Fi、蓝牙等，支持数字化通信。
- **IOT—物联网技术：**提升工业网络智能化和效率。
- **自适应人工智能/超级智能：**如聊天机器人、自动驾驶汽车等，基于 AI 的技术应用。
- **教育技术：**基于计算机的教学和在线资源，改变传统教学模式。
- **区块链技术：**安全的网络加密系统，适用于多种业务场景。

在过去的数十年中，企业越来越依赖各种各样的数字技术实现降本增效，更新换代，从激烈的商业竞争中脱颖而出。从使用芯片和 PIN 阅读器的街角小店，到推出 DAP 以辅助超级应用程序的复杂系统的大型企业，数字技术是诸多企业成

功的关键。它帮助企业简化运营，提高生产力，改善客户体验。通过应用各类与企业商业模式、业务逻辑相吻合的数字技术，企业可以在其行业中获得竞争优势，并取得更大的成功。数字技术使公司能够以越来越低的成本提供更好的产品或服务，从而保持领先地位。

1.2 数字技术带来的机会和安全挑战

随着数字技术的迅猛发展，所面临的安全挑战日益增多且变得复杂。个人信息泄露、企业数据安全威胁、网络攻击以及数字诈骗的频发，均是数字化环境中不容忽视的安全风险。数字化进程不仅代表着技术的创新，也意味着安全挑战的不断升级。

国家的数字化战略、企业的数字化转型、个人的数字生活等，已深入渗透至社会的各个方面。伴随而来的安全问题不再仅限于传统网络安全的范畴，而是拓展至数据安全、智能设备安全及与数字身份相关的安全问题。数字化发展的快速与广泛性，直接加剧了安全风险的严重性，使得数字安全成为亟待解决的重要问题。

历史上，技术变革与社会变迁紧密相关。从 Schumpeter 的创新理论到创造性破坏理论，均揭示了技术变革与社会经济、军事、文化和政治的深刻联系。每次工业革命，从蒸汽机、内燃机、信息科技到当今的人工智能、清洁能源等，均引领了社会变迁的潮流。然而，这些变革在创造新机遇的同时，也带来了金融泡沫、经济衰退和社会危机等破坏性后果。

特别是在数字时代，自 2002 年以来，全球数据信息的存储方式从模拟转向数字，信息传输与存储能力呈指数级增长。伴随着这一发展，数字技术带来的安全挑战日益突出，例如 CIH 病毒、震网病毒等重大网络安全事件，以及斯诺登事件暴露的全球监视网络问题，均反映了网络空间安全的重要性。

近年来，受国际政治局势影响，众多国家加强网络安全建设，出台战略规划，推动零信任、量子技术等新兴技术研发，同时完善网络安全机构体系。例如，美

国发布了《首席信息官战略》、《云计划》和《零信任战略》，旨在通过信息技术和资源共享降低研发成本，抢占未来网络空间作战的制高点。

此外，量子通信和量子计算等新兴技术正逐渐成为未来安全通信的关键基础设施。然而，这些技术的发展也对现有的密码体系构成挑战。

面对这些挑战，中国可以借鉴西方国家的发展思路，加强产学研用的协调合作，在网络安全新兴技术领域加速技术升级，利用零信任、量子、5G、云计算等技术提升网络安全防御能力。同时，应合理布局新兴技术，关注技术交叉融合带来的安全机遇，并推行零信任防护理念，实施以数据为中心的网络安全策略。

1.3 数字技术的迅猛进步和广泛应用深刻影响社会、经济和科技

数字技术涵盖计算机硬件、软件开发、互联网和通信技术等领域。在硬件方面，计算机性能飞速提升，从超级计算机到智能设备都在改进。软件开发方面，开源软件、云计算和分布式系统提高了效率。互联网和 5G 技术的普及加速信息传输速度。

数字技术已渗透医疗、金融、制造业、教育、交通、娱乐等领域。医疗领域数字技术使医疗记录电子化、诊断更准确，促进了远程医疗。金融领域数字支付和区块链改变了交易和金融体系。这种迅猛发展不仅仅是技术领域，也深刻影响社会、经济和科技生态系统。在社会层面，改变了社交、媒体消费和信息获取方式；经济上推动创新、提高生产力，催生新商业模式如共享经济和电子商务；科技上推动人工智能、大数据分析、机器学习等技术出现。

2 2024 年十大数字技术趋势

2.1 量子计算

2.1.1 量子计算的定义

传统计算机采用二进制的数字电子方式进行运算，仅能够表示 0 和 1 两种状态。量子计算是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式，它以量子比特为基本单元，利用量子叠加和量子纠缠的特性，能够同时表示多个量子态的叠加。量子计算机的架构与传统计算机完全不同，它主要包含两个部分，一个是量子芯片支持系统，用于提供量子芯片所必需的运行环境；另一个是量子计算机控制系统，用于实现对量子芯片的控制，以完成运算过程并获得运算结果。与此同时量子计算机在计算性能、适用性、信息携带量等方面有巨大突破，可以作为 CPU 的协处理器，对很多重大的数学难题进行指数级加速和破解常见的公钥私钥密码系统。目前所说的量子计算机并非一个可独立完成计算任务的设备，而是一个可以对特定问题有指数级别加速的协处理器，本质上来讲是一种异构运算，即在经典计算机执行计算任务的同时，将需要加速的程序在量子芯片上执行。

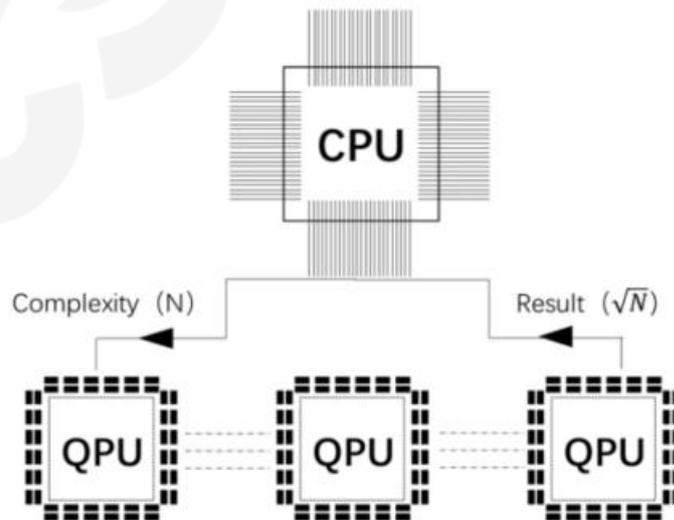


图 1 量子计算流程图

2.1.2 量子计算的应用

量子计算作为一种新兴的计算领域，具有许多强大的潜在应用。未来的主要应用包括以下几个方面：

1. 大规模数据处理：量子计算的快速计算能力将使其能够处理海量的数据，有效解决大数据分析、模拟和优化等领域的问题。例如，在金融领域，量子计算可以用于优化投资组合、风险管理和交易策略的决策。

2. 优化问题求解：量子计算可以在优化问题上提供更快速和高效的解决方案。例如在物流和运输领域，量子计算可以优化路径规划、货物分配和交通流量控制等问题，提高各种系统的运行效率。

3. 高性能模拟：量子计算不仅可以模拟分子和材料的行为，还可以模拟量子系统本身，这对于量子化学、材料科学、生物学和药物研发等领域来说具有重要意义。通过利用量子计算的优势，人们可以更好地理解分子结构、反应机制和材料性质，加速新药的研发和新材料的发现。

4. 密码学与安全通信：量子计算可以应用于密码学领域，例如量子密码学可以提供更高级别的安全性，抵御传统加密算法所面临的威胁。此外，量子通信也可以实现完全安全的通信，确保信息的完整性和隐私性。

5. 人工智能和机器学习：量子计算能够提供更强大的计算能力，为人工智能和机器学习算法提供更快速和高效的开展，加速模型训练和推理过程。这将使得人工智能系统能够更好地处理复杂的问题，提供更准确的预测和决策。

总的来说，量子计算在大规模数据处理、优化问题求解、高性能模拟、密码学与安全通信以及人工智能和机器学习等领域都具备广泛的应用前景。随着量子技术的不断发展和突破，这些应用有望成为未来量子计算的主要领域。

2.1.3 量子计算的未来预测

量子计算领域属于一个新兴高速发展的领域，在最近几十年不论是量子算法的研究还是量子芯片的研发均取得了巨大的进展。量子计算技术通过核磁共振、超导量子线路、半导体量子点、囚禁离子阱和冷原子等平台展示了量子比特的精确操控。但学术界也对量子计算的可行性仍存在很多质疑，特别是对退相干造成的量子信息丢失是否能够有效克服。随后，量子计算发展的重要里程碑是量子纠错理论的建立。

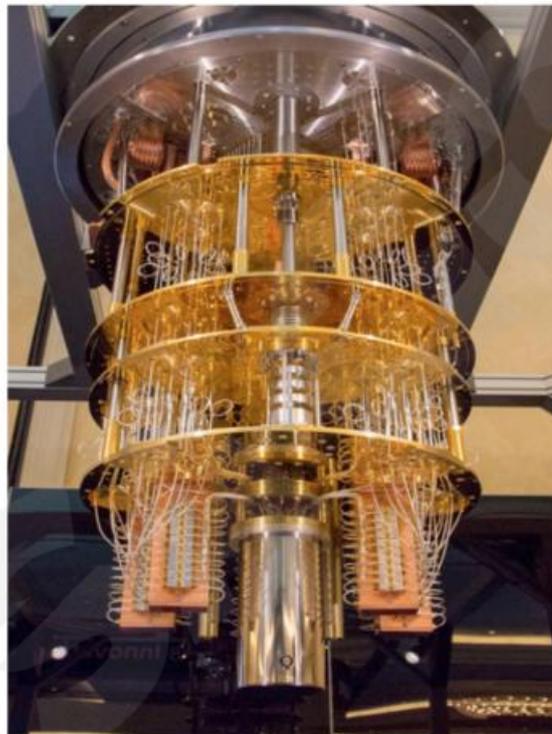


图 2 IBM “50” 量子计算机原型机

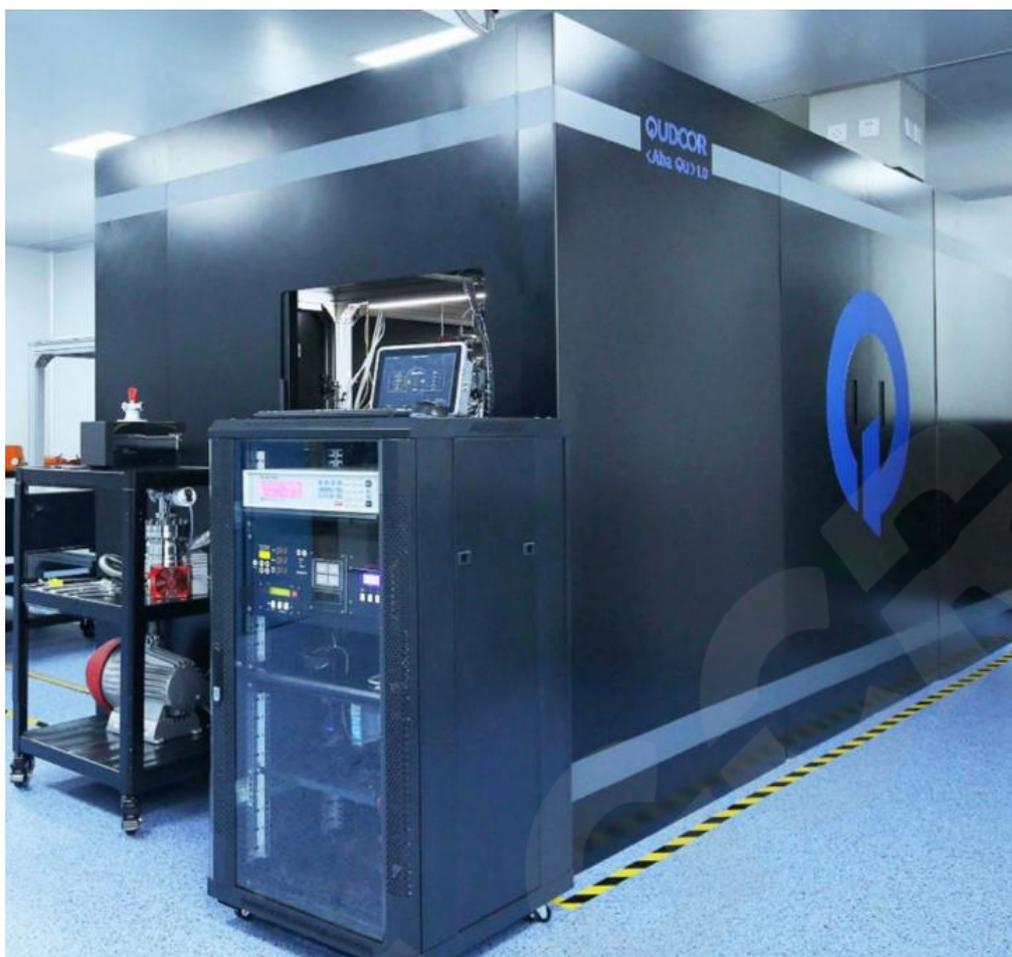


图3 国产离子阱量子计算工程机外观图

目前对量子计算的理解而言，量子体系模拟仍然是主要的应用领域。在量子体系模拟的基础上，可能会衍生出服务于药物开发、新材料、农业等领域的量子计算技术，但需要清楚认识到这些衍生应用是遥远的可能性，而不是已经或即将实现的技术。总的来说，对于量子计算的发展，我们需要有清晰的大局观：前途一定光明，但道路必定曲折。量子计算是一项革命性的技术，能够在非常基础的层面改变。

2.2 6G 通信技术

2.2.1 6G 通信的定义

6G 网络与 5G 相比将会有巨大的革新，中国成立了 IMT-2030（6G）推进组，发布《6G 总体愿景与潜在关键技术》白皮书。美国成立了 Next G Alliance，

聚焦于研发、制造、标准化和商用整个周期。欧盟成立了 Hexa-X 6G 项目，希望引领 6G 网络发展。

6G 的愿景是：数字孪生，智慧泛在。相比于 5G，6G 不仅要求更高的带宽、更低的时延和更高的可靠性，同时 6G 网络会具备更多 5G 所没有的数据形式，如未来 6G 所传输的大量人体数字信息等。6G 还对空天一体化提出了更高的要求，实现更广泛地渗透到工业物联网以及各种垂直行业。

在 6G 时代，由于元宇宙、数字孪生、人工智能等技术的成熟，6G 将实现无所不在的连接和更深刻的体验。在通信网络中所传输的信息会更加敏感和实时，例如车辆位置信息、控制信息，人的生物特征识别信息、家庭电器控制信息等。设备联网的规模、分布将更加广泛，从外太空到深海，人、物都将可以通过 6G 随时随地与互联网相连。在这样的情况下，恶意网络活动可能会导致人们的财产、人身损失。因此，6G 在安全上要一开始就考虑一个完善的架构来应对未来可能出现的挑战。

2.2.2 6G 通信当前应用

6G 是立体的提升，将实现地面与太空、海洋的集成，实现“海陆空”一体化。6G 相对 5G 将有 10-100 倍提升，关键性能指标包括支持 1Gbit/s 的用户体验速率，1Tbit/s 的峰值速率，10~100 μ s 的时延，1Gbit/(s·m²) 的区域通信流量，10⁷ 台/千米² 的连接密度以及至少 1000km/h 的移动性。

6G 网络在频谱、编码、天线等方面需要产生革命性的创新，潜在技术将包括太赫兹 (THz) 通信、可见光通信 (VLC)、新一代信道编码技术、超大规模天线技术、基于人工智能 (AI) 的无线通信技术、空天地海一体化通信等关键技术。

6G 将实现数字孪生、智慧泛在，未来的应用场景包括全息交互、虚拟旅行、沉浸式社交等。典型的 6G 新型应用场景，包括进一步增强的移动宽带 (FeMBB, further enhanced mobile broadband)、超大规模机器类型通信 (umMTC, ultra-massive machine-type communications)、增强型超可靠和低时延的

通信（ERLLC, extremely reliable and low-latency communications）、长距离和高移动性通信（LDHMC, long-distance and high-mobility communications）以及超低功耗通信（ELPC, extremely low-power communications）。

2.2.3 6G 通信未来预测

6G 技术预计在 2030 年左右投入市场，这对整个产业会是一个新的机会和挑战。从应用来看，5G 开启了通信技术融入千行百业的序幕，5.5G 进一步把 5G 的技术发挥到极致，未来几年，5.5G 定义与部署以及 6G 的研究与定义将会同时进行，6G 将实现对 5.5G 超越，深层次的融入到所有人的生产、生活之中。

6G 面临的技术环境将会更加复杂，云计算、大数据、算力网络、AI、区块链、边缘计算、数字孪生、元宇宙等都会带来影响。对 6G 安全来讲，量子通信、内生安全、AI 安全是都将是对 6G 产生直接影响的安全技术。

6G 将实现空天地海的一体化通信架构，在低轨卫星大规模部署的同时，高轨卫星、无人机与高空平台，会成为 6G 的补充。AI 引入网元，并与边缘计算、云计算融合起来构建智慧内生的通信网络体系。算力网络概念深入云网边并统一编排，6G 时代网络与算力融为一体，形成空天地一体的算力网。

6G 时代，物联网设备数量预计达到 800 亿台，大量联网设备带来新的安全挑战。网络通信依赖的重要算法，如椭圆曲线密码系统（ECCs）等密码算法，在未来量子计算技术的性能提升下，将不再安全，而必须用后量子密码技术替代。

2.3 人工智能

2.3.1 人工智能的定义

人工智能（Artificial Intelligence, 简称 AI）是指通过计算机等技术手段模拟、延伸和拓展人类的智能，使计算机具备像人类一样的思维模式、感知、

推理、学习、判断和决策能力。人工智能之父马文·明斯基 (Marvin Minsky) 将其定义为：“人工智能是关于让机器胜任需要人类智慧才能完成的任务的科学。”。人工智能通常分为弱人工智能和强人工智能。AI 的研究经历了以下的历程：

早期探索（1950 年代-1960 年代）：在这个阶段，研究人员开始尝试创建可以模仿人类智能的计算机程序。1956 年，达特茅斯会议被认为是人工智能领域的起点。

知识推理与专家系统（1970 年代-1980 年代）：人们尝试使用可编程规则和知识库来实现人工智能。专家系统是其中的重要成果，它通过存储和应用领域专家的知识，来模拟专家的决策过程，解决特定问题。即“符号主义”的技术路线。

神经网络（1980 年代）：神经网络模拟了人脑神经元之间的连接和传递信息的方式，使得计算机可以通过大量的数据进行训练和学习。基于神经网络的机器学习成为 AI 的重要组成部分。“联结主义”的技术路线开始成为主流。

过度推广与失落（1990 年代）：在 20 世纪 90 年代初，人们对于 AI 的期望过高，并出现了所谓的“AI 寒冬”，许多项目失败或被搁置。

深度学习与多层神经网络（2010 年代至今）：深度学习是一种基于神经网络的机器学习方法，它通过多层次的神经网络结构来模拟人脑的工作原理。深度学习在图像识别、语音识别、自然语言处理等领域取得了重大突破。深度学习成为 AI 研究的主流。

2016 年 3 月，DeepMind 公司的 AlphaGo AI 系统击败了韩国顶级职业围棋棋手李世石。2017 年 5 月 AlphaGo 又战胜了世界围棋冠军柯洁，轰动了世界。AlphaGo 的成功引发了全球范围内的第三次人工智能浪潮。主要国家纷纷将人工智能列为国家发展战略的重要组成部分，包括中国、美国、加拿大、法国、德国、英国、阿联酋、日本、韩国和新加坡等国家。

大模型（2020 年代至今）：随着计算机算力的大幅提高，人们开始思索，

如果将神经网络模型的神经元数量和连接参数增加到人脑的水平,会出现什么样的奇迹? 于是,对 AI 大模型的研究开始加速。

1) LLM(Large Language Model)是指基于语言模型的研究,旨在通过训练大规模的神经网络来学习语言的统计规律和语义表示。其中,BERT、GPT 和 XLNet 等模型大幅提升了自然语言处理任务的性能,并在诸如问答系统、机器翻译和文本生成等方面取得了突破。

2) 2020 年 5 月,美国 OpenAI 公司发布了 GPT-3 模型,一个有 96 层神经元、1750 亿参数的生成式 LLM 模型。GPT(Generative Pre-trained Transformer)使用变压器(Transformer)架构来生成自然语言文本。这是一个强大的人工智能聊天机器人,可以根据用户的提问生成内容。它具备广博的知识,涵盖了 IT、科学、法律、医学、诗歌和绘画等各个领域的知识,而且文笔流畅。甚至可以编写计算机程序。可以生成更长、更准确、更有逻辑性的文本。2023 年 2 月 ChatGPT 引爆全球。

3) 随后发布的 GPT-4 模型有 120 层,每层约 150 亿个参数,总共约 1.8 万亿个参数,是 GPT-3 的 10 倍多。11 月 7 日,OpenAI 发表了 GPT-4 Turbo 模型,功能更强大。成为真正的多模态生成式 AI 模型。可以输入和输出图像、音频、视频、文本。更大规模的 GPT-5 也正在训练中。

ChatGPT 的成功在全球范围里引发了百模大战。大模型的研究也成为当今人工智能发展的主流趋势,如 BERT、Gemini 等多模态 LLM 展现了巨大的潜力,为自然语言处理领域带来了革命性的变革。

2.3.2 人工智能的应用

当前, AI 技术已经渗透到各行各业, AI 正在改变我们的世界。

如:数字经济、在医疗领域、在金融领域、教育领域、自动驾驶的前沿探索、物联网、云计算等领域;还有:科研领域、军事国防领域、司法领域、工业、能源、电力、交通、IT、网络安全等各个领域都在越来越多地拥抱 AI 技术。

总的来说，人工智能技术在各个领域实现了快速和广泛的应用和发展，同时这也需要人们关注其带来的伦理和法律问题，以确保其合法和公正的应用。

2.3.3 人工智能的未来预测

尽管人工智能在多个领域得到了广泛应用，包括以 ChatGPT 为代表的生成式 AI 也取得了巨大的成功，但它们仍旧属于弱 AI，因为只模拟了人的右半脑的思维模式。经常被图灵奖得主和学者们指出的问题和不足包括：①不能处理因果关系、②缺乏可解释性、③常常会产生“幻觉”，一本正经地胡说八道、④“文学博士的语文，小学生的算术”、⑤无法处理动力学系统；⑥不能输出精准结果，只能是概率的等等。

强人工智能成为 AI 发展的下一个里程碑。图灵奖得主、院士、研究者们从计算机科学角度提出强人工智能必须具备的特质：①新的 AI 理论体系、②动力学系统模拟 (Dynamice System)、③因果关系 (Cause-effect relations) 和推理、④可解释性 (Explainable)、⑤人类左右脑 (Left-Right Brain) 思维方式，⑥新机器学习算法 (New Machine Learning Algorithms) 等。

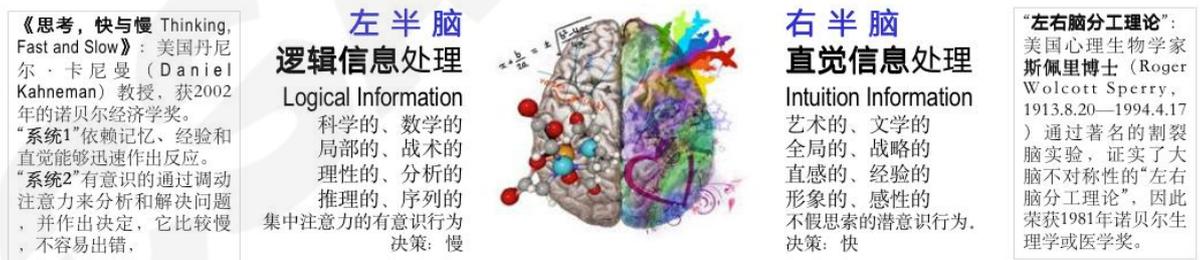


图 4 人脑的思维模式

左右脑 AI 的研究，从理论到实践，已经实现了质的突破。原中科院的 Dr. Gao 在日本早稻田大学博士论文中提出了左右脑型人工智能 (Left-Right Brain AI) 的原型理论，可以让计算机像人脑一样：可以同时使用左半脑和右半脑、同时处理逻辑的和直觉的两类不同性质的信息；并建立了脑胼胝体模型，首次解决了左右脑信息交互的难题。又实现了左右脑 AI 的机器学习算法。这种左右脑 AI 还具

有处理因果关系、动力学系统、可解释性等强人工智能所必需的特质。

这种左右脑 AI 研究已经落地。1998 年曾作为日本政府项目，与日本早稻田大学和丰田汽车公司合作，带领团队为日本丰田汽车公司构建了基于左右脑 AI 的 G-MOS 动态模型，在世界上首次使用“左右脑 AI 模型+实际数据”证明了计算机可以像人脑那样工作：左脑(逻辑信息) +右脑(直感信息) +机器学习-> 意识决定。该左右脑 AI 模型可以高精度预测生产线的故障率，平均提高了汽车自动生产线的信赖性(46%UP)，同时又大幅降低了维修保养成本(31%Down)，提高了工厂生产力。更证明了左右脑 AI 的可用性、实用性和通用性。获日本 99' PM 行业大奖。

与现在的基于神经网络+机器学习、只擅长直觉信息处理的单脑型人工智能（弱人工智能）相比，这种左右脑 AI 更接近人类的思维方式。人类向“强人工智能”的时代又迈出了里程碑式的一步。

2.4 云原生

2.4.1 云原生的定义

在经历了云服务技术兴起、容器和微服务普及、容器编排 kubernetes 诞生之后，在软件工程领域需要一种能描述新的应用架构定义，帮助人们更快更好地构建和管理业务应用。云原生概念应运而生，然后快速发展成熟。从最早模糊的微服务云原生架构、到 CNCF 成立对云原生首次定义：应用容器化、面向微服务架构、应用支持容器编排和调度、再到 CNCF 从理念的角度重定义云原生，迄今为止还在不断发展，理念边界不断覆盖到软件工程、IT 基础设施、云平台等各个领域。

2015 年 Pivotal 公司的 Matt Stine 在《迁移到云原生应用架构》一书中，探讨了云原生应用架构的特征，将这些特征归纳为 12 个方面：代码、依赖、配置、后端服务、编译发布运行、进程、端口绑定、并发、易处置、开发/生产环境一致、日志、管理进程，这些特点较多，而且每个特点的定义都比较复杂，并

没有得到广泛传播，但这可以认为是云原生定义的一个早期探索。

2015 年 Google 主导成立了 CNCF (The Cloud Native Computing Foundation) 云原生基金会。2016 年 CNCF 正式对云原生进行了定义，包含三个方面：应用容器化、面向微服务架构、支持容器的编排和调度。这时的定义主要包含了两大技术容器编排和微服务，但是并不足以描述云原生的本质特征。

2018 年云原生概念不断越来越大，早期的定义已经变成了约束。CNCF 进行了重新定义：云原生技术有利于各组织在公有云、私有云和混合云等新型动态环境中，构建和运行可弹性扩展的应用。新的定义不再局限于特定的技术，而是从底层核心理念出发，对云原生进行思考和定义。此后云原生一直在不断快速发展，已经不局限于某一项或多项技术，更多的是从应用研发、运行、维护效率的角度出发，通过各种方法对应用全生命周期进行提升。



图 5 云原生技术

云原生代表技术除了 CNCF 的定义：容器、服务网格、微服务、不可变基础设施和声明式 API 外。从普遍认知来看，还包括 DevOps、kubernetes 容器编排、云基础设施。这些技术都是在软件工程领域经过长期积累形成的，为云原生应用

独特的敏捷性、可扩展性优势。能够极大地提高研发和运维效率、运行资源利用率、业务交付速度和质量。

2.4.2 云原生的应用

云原生能够帮助企业在开发和上线效率提升、业务敏捷性、降低 IT 基础设施成本、基础设施标准化和可移植性等方面带来显著的价值。这些优势能够极大地增强企业在数字技术时代的竞争力。

云原生技术的最典型应用就是通过容器构建应用，kubernetes 进行编排。通过容器构建应用能够极大地提高应用的部署效率，实现一次编译，处处运行。单一容器难以构建一个完整的应用，kubernetes 容器编排技术实现了多容器自动化编排，只要完成编排描述文件，就能够在任意 kubernetes 集群自动化部署，从此业务应用才真正实现了可移植。容器技术的另一个优势就是资源隔离，能够大幅提高计算资源的利用率，降低 IT 基础设施成本。



图6 云原生 DevOps 全流程

DevOps 理念出现在云原生技术之前，但一直难以完全实现，更多关注在设计、编码、测试、编译方面，直到云原生出现，弥补了发布、部署、运维、监控自动化流程，DevOps 才真正实现了全流程自动化，整个流程才真正运行起来。研发人员从代码提交开始，就能自动化构建业务进程，打包成容器，通过 kubernetes 进行编排部署，全流程都无须干预，真正实现了开发上线一键执行，

能够极大提高研发敏捷性。

微服务和服务网格为企业在业务灵活性、扩展性上提供了极大帮助。通过抽象服务公共逻辑，形成微服务网关和服务网格，能够让企业研发人员更多地关注自身业务本身，无须关注微服务之间的调用、隔离、部署等。而且微服务和服务网格具有更好的可观测性，业务运行状态都能够直观展示。

2.4.3 云原生的未来趋势

经历了爆炸增长期，云原生核心技术功能逐渐稳定，已经逐渐形成事实标准。向下屏蔽 IT 基础设施差异，向上抽象业务公共逻辑，标准化云原生能够有效地提高业务的可移植性，解除厂商技术绑定，激活 IT 资源流通性，快速在不同的 IT 基础设施之间选择最适合的业务运行环境。因此云原生的未来趋势的核心方向就是通过改变应用构建、部署、运行方式，解耦应用运行环境绑定，从而在整个应用生命周期提高生产效率，降低资源消耗。具体有如下几点：

- **多云和混合多云普及：**在云原生之前，业务应用和底层计算、存储、网络都有很强的绑定关系，虽然企业基于容灾、可靠性、隐私性需求会在多个地域进行应用规划部署，但是往往由于迁移困难，并不能很好地利用云的灵活性。未来企业应用会越来越多地真正在多云部署、动态调整、灵活扩容。
- **微服务和服务网格兴起：**随着云原生发展，微服务和服务网格越来越标准化，运维成本越来越低，随时都能快速部署、调用各种功能完善的微服务，整个数字技术世界正在不断向着一体化演进。
- **持续交付部署效率进一步提升：**云原生 kubernetes 打通了部署和运维自动化流程，自动化 CI/CD 正变得越来越流行，更快的应用交付速度、更高的软件质量，不断形成正反馈，加速企业数字技术的发展。
- **无服务计算应用广泛：**为了进一步提高应用交付速度，研发人员只需要研发代码，其他都能够自动运行管理的无服务计算越来越受欢迎。这种模式

可以进一步提高研发效率和资源利用率，而且随着技术发展启动速度、首次响应速度也得到了大幅优化，在越来越多的场景得到应用。

总的来说，云原生应用正在改变我们创建、部署和运行应用程序的方式。我们可以预期云原生将持续推动数字技术的创新和进步。

2.5 数字孪生

2.5.1 数字孪生的定义

关于数字孪生，很多组织都给出了自己的定义。Gartner 对数字孪生的解释为：数字孪生是现实世界实体或系统的数字表示形式。数字孪生的实现是一个封装的软件对象或模型，它反映了独特的物理对象、流程、组织、人员或其他抽象。来自多个数字孪生的数据可以聚合为跨多个现实世界实体（如：发电厂或城市）及其相关流程的复合视图；麦肯锡对数字孪生的解释为：数字孪生是物理对象、人或过程的数字表示形式，在其环境的数字版本中进行了上下文文化。数字孪生可以帮助组织模拟真实情况及其结果，最终使其做出更好的决策；IBM 认为：“数字孪生是一种旨在精确反映物理对象的虚拟模型”。

在此，我们将数字孪生定义为：数字孪生是对现实世界进行抽象并完成数字表示与交互，它能够精确、真实的反映现实世界的变化过程与结果。

2.5.2 数字孪生的应用

普遍被接受的数字孪生概念起源于美国宇航局阿波罗计划，在阿波罗计划中美国宇航局构建了多个相同的航天器，其中一个发射到太空，其余的则留在地球上用于反映太空中航天器的工作状态和操作试验。2011 年，NASA 首次使用了 Digital Twin（数字孪生）一词，并将其描述成一种反映现实世界状态的综合载体。2016 年，Gartner 将数字孪生放进当年的十大战略科技发展趋势，这一技术开始受到全球范围的广泛关注。



图 7 数字孪生生态系统

数字孪生技术给研究对象（例如：航天器）装配与期望受控功能相关的传感器，生成与现实世界各个方面状态相关的数据（例如：输出功率、飞行姿态、环境温度等等），并将这些数据转发至处理系统并应用于数字副本，虚拟模型基于相关数据进行模拟执行，研究与功能和性能相关的问题并生成可能的改进方案。数字孪生围采用双向信息流设计，即传感器可以向处理系统提供相关数据，处理系统也可以将其得出的研究成果与源对象进行共享，例如下表 1：

	计划	构建	运行	维护
文档管理	PLM	PLM	运行手册	服务记录
模型	物理属性预测		优化	诊断
模拟	设计模拟	虚拟调试		
3D 表示	设计图	生产手册		服务手册

数据模型	工程数据	产品数据	运行数据	服务数据
可视化			显示运行状态	显示健康状态
模型同步			实时行动	模型反演
连接分析			运行 KPIs	资产健康 KPIs

表 1 数字孪生示例

数字孪生包括组件孪生、资产孪生、系统孪生和流程孪生 4 种主要类型：

- **组件孪生：**组件孪生是数字孪生的基本单元，是系统或产品单个组成部分（例如：齿轮）的数字表示。
- **资产孪生：**两个或多个组件一起组成资产，资产孪生用于研究组件之间的协同。
- **系统孪生：**也称为单元孪生，系统孪生则将单独的产品建模为更大系统，研究不同资产汇聚在一起工作时的交互。通过系统孪生，可以研究资产相互交互的关系，从而提高生产力和效率。
- **流程孪生：**流程孪生是协同工作的系统的数字表示形式（例如：系统孪生对生产线进行建模，流程孪生则对整个工厂进行建模，包括工厂车间操作机器的员工）。流程孪生可帮助确定最终影响整体效率的精确时间控制方案。

利用数字孪生能够更高效地研究和设计产品，真实反映和监控生产系统，在整个生产和运营流程中获得和保持高效率，以及对产品进行生命周期管理。数字孪生具有的种种优点，获得了众多企业和组织的关注。然而，并不是所有对象都能达到足够的复杂程度，需要数字孪生技术中所必需的密集、频繁的传感器数据流。考虑到投资回报（ROI），当前应用数字孪生的背景往往基于实体规模较大，或者涉及生命或人身安全的项目（例如：航天工业、核工业、汽车制造、飞机制

造、建筑工程、发电厂等行业)。

2.5.3 数字孪生的趋势

数字孪生市场正在经历迅猛发展期，根据统计，2021 和 2022 年的北美数字孪生市场分别达到了 22.5 亿美元和 29.4 亿美元，一些行业分析师推测，至少在 2026 年之前，这一数字还会继续大幅攀升，预计将会达到 482 亿美元。这些数据验证了数字孪生技术已经在诸多行业中得到应用，并且其需求将在未来的一段时间内持续增加。

关注生命安全、人身安全，以及 ESG（环境、社会和治理）驱动的现代运营环境正在发生根本性变化，数字化是现代运营模式转变的技术驱动力，正在影响资产管理、生产力效率以及流程等关键要素，而数字孪生则是数字化转型的重要组成部分。因此，化学工业、智慧城市、0 碳园区、应急指挥、自动驾驶医疗服务等行业将会更广泛的采用数字孪生技术，以实现降本增效和社会责任的双重目标。

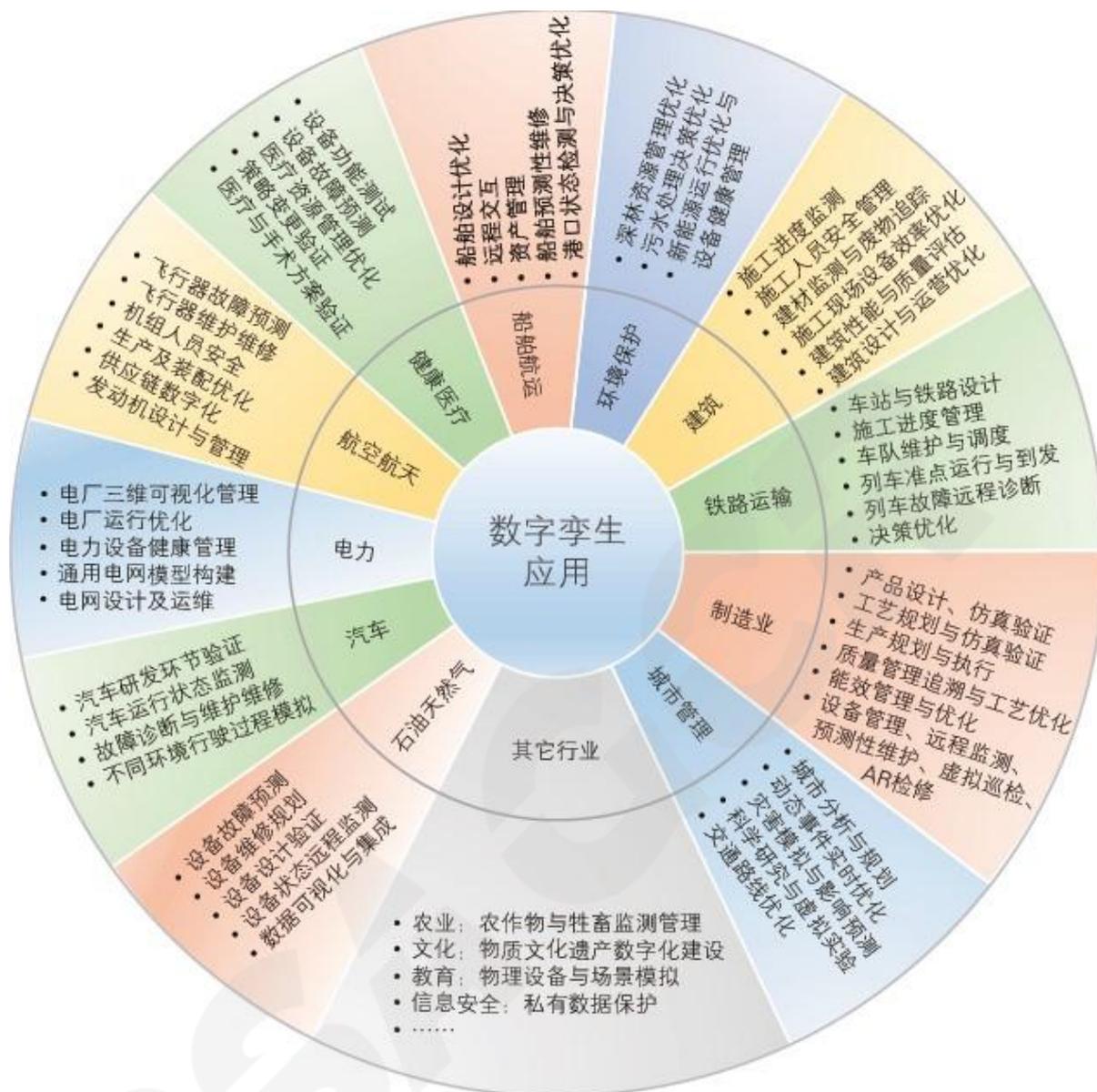


图 8 数字孪生行业应用

以人工智能为代表的新技术越来越多的不断投入到数字孪生系统中，使得数字孪生技术的未来应用几乎具有无限可能性，这些技术的运用还包括：

- 云计算为数字孪生提供了基础设施所需的环境，例如：弹性的高性能计算；
- 虚拟现实与增强现实为数字孪生的可视化和互操作提供了坚实的基础；
- 数据互操作给数字孪生带来了更加良好的生态环境；
- 5G&6G 技术为数字孪生的数据通信要求低延迟、高速率提供了可能性；

- 机器学习与人工智能为处理系统提供了建模基础，等等。

2.6 隐私保护

2.6.1 隐私保护技术的定义

隐私是指个人或组织在数字化环境中保护个人信息和个人生活不受不必要干扰和侵犯的权利。隐私保护是保护个人信息和个人生活的机制和措施。在我国，隐私的定义主要由《中华人民共和国个人信息保护法》（个人信息保护法）进行规定。该法于 2021 年 11 月 1 日正式生效，明确了个人信息的定义和隐私权的保护范围，规定了个人信息的收集、使用、存储和传输等环节的义务和责任。个人信息保护法中对个人信息的定义如下：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

隐私保护技术是降低隐私风险，保证业务合法合规的重要手段，针对不同的隐私风险，可以采用不同去标识化技术对隐私风险进行消减。参考 GB/T 37964-2019 去标识化指南，去标识化是通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。去标识化技术是降低数据集中信息和个人信息主体管理程度的技术。常见的去标识化技术包括掩码、枚举、差分隐私、隐私计算、同态加密、多方计算等。

2.6.2 隐私保护技术应用

由于多行业均存在数据安全合规协作的需求，隐私保护技术的落地场景也分散于各行各业。政务、金融、能源、运营商、互联网、医疗、安防等都有具体需求和落地方向。以金融为例：

1) 普惠金融

小微企业的信用数据来源的分散化、碎片化使银行获取数据的成本高、难度大，加上整个社会信用信息体系尚未完全打通，信息获取的渠道不通畅，彼此之

间仍然存在着组织壁垒、数据孤岛的问题。基于隐私保护技术与政务数据融合，横向打通的数据包括税务、交通出行数据、水电燃气数据、公安数据、征信数据等，赋能普惠小微金融。

2) 智能风控

一直以来，征信与风控是金融业管理风险的重要手段。然而，传统信贷风控的模式和手段正面临越来越多的难题，比如数据采集范围局限、接入门槛高、客户或关联方上传数据积极性低、更新不及时等等，已经成为金融发展的障碍。借助隐私保护技术可以在保护用户信息不泄露的前提下将来自更多维度数据纳入联合风控模型中，从而构建更精准大数据风控模型。

3) 智能反诈

近年来，在互联网、大数据及人工智能等新兴技术的驱动下，商业银行积极开拓创新产品及服务，业务活动日趋复杂。与此同时，不法分子依托新兴技术手段，通过银行渠道进行诈骗活动，尤其是信用卡欺诈行为逐渐呈现出组织化、移动化、隐蔽化、场景化等特征，并形成灰黑产业链，对居民资金安全以及银行业务安全造成严重威胁。基于隐私保护技术，提供反诈风险名单共享方案，进一步提高金融机构反风险能力，保障机构及客户资产安全。

2.6.3 隐私保护未来预测

1) 控密双态计算

近年来数据的流动与使用也滋生出各种乱象，数据窃取、数据买卖、数据滥用等情况频发，数据安全与隐私泄露成为社会各界关注的话题。与此同时各国《隐私保护法》《网络安全法》等法律条例陆续颁布与实施。控密双态计算（Control & Crypto Computing）是 CSA 提出的一种解决方案。它实现“动静用转”和“云网边端”全面覆盖。确保环境、模型、算法、算力和用户身份的安全可信，进而保障数据在使用和流转中的安全可信。具体定义如下：

控态路径：存控、传控、用控、转控，保障数据的完整性、可用性和可信 IAT，不仅安全，而且可信、可控。目前控态类技术路径，早期已有大规模应用的架构模型和产品原型，如：NIST 的零信任参考架构、NIST 大数据参考架构、IDSA（国际数据空间协会）的数据安全空间。

密态路径：密存、密传、密用、密转，保障数据的私密性。目前密态类技术路径，大多数是基于隐私计算的，目前主要的密态技术：多方安全技术计算、同态加密、差分隐私。

2) 数据本地化

出于国家主权、数据安全、隐私保护等多种因素的考虑，越来越多的国家和地区采取数据本地化措施，限制数据跨境流动。截至 2023 年，100 多个国家实施了数据本地化措施，其中一半以上是在过去 5 年中出现的。更为重要的是，这些措施的限制性越来越强，三分之二的措施涉及禁止数据流动的存储要求。安全和风险管理领导者面对着尺度不一的监管环境，在不同地区需要采取不同的本地化策略，这使得企业机构为应对跨国业务战略风险而采取一种适合所有服务模式的新型服务化设计和获取方法。由此，数据本地化规划将成为科技企业设计和获取方面的首要任务。

3) 以用户为中心的隐私

消费者对主体权利的需求增加，以及对透明度的期望提高，将推动对集中式隐私用户体验的需求。有远见的组织了解将隐私以用户为中心的所有方面（通知、cookie、同意管理和数据主体权利请求）整合到一个自助门户的好处。

2.7 Web4.0

2.7.1 WEB4.0 技术的定义

Web（World Wide Web）是全球广域网，也称为万维网，它是一种基于超文本和 HTTP 的、全球性的、动态交互的、跨平台的、分布式图形信息网络。Web4.0

是第四代万维网。利用先进的人工智能、环境智能、物联网、可信区块链交易、虚拟现实、和增强现实等功能,虚拟和真实的物体和环境将完全集成并相互通信,从而实现真正直观、身临其境的体验,无缝融合物理和现实数字世界。

纵观整个 Web 的发展,可以发现,一切都是为了交互和易用而做出的改变。Web1.0 的概念在 1991 年被创建。它是一个可以使用超链接的在线文档系统,这使得用户可以更快速、轻松地共享信息,同时用户也可以创建网站、提供自己的内容。在 20 世纪末与 21 世纪初,网站与内容的数量急剧增加,并持续了将近 20 年。Web 早期专注于提供静态内容。该内容通常采用文本与图像的形式。

Web2.0 的概念在 2004 年被提出,这个术语用于描述从静态 html 页面到更加动态的 web 的转变,同时用户可以在其中与 web 应用程序以及其他用户进行交互。Web2.0 的主要功能之一就是它允许用户在线创建和共享内容。包括博客、社交媒体等。同时用户的终端也从 pc 逐渐转移到移动设备。Web2.0 使互联网成为一个更具互动性和协作性的场所,并催生了在线开展业务和营销的新方式。可以发现 Web2.0 提供了更丰富的用户交互手段,并降低了用户使用互联网的门槛。

2.7.2 WEB4.0 技术应用

当所有人将自主生产的数据、内容和记录存放在网络中后,各大互联网公司逐渐积累了大量的个人信息和财富,这种集中化的情况造成了用户与平台之间权利的不平衡,同时也使企业与个人面临网络安全、欺诈与数据分享。此时,web3.0 的概念诞生,它的出现改变了原有的基础架构,将网络的主权转给用户。通过引入区块链、云计算等技术,在密码学的保护下,让用户能够安全地拥有自己的数字身份与数字资产。

Web4.0 的应用程序被设计得更加用户友好,并允许用户轻松共享信息与想法。Web4.0 代表了从传统 Web 开发模型向更具协作性和以用户为中心的方法的转变。

2.7.3 WEB4.0 的技术预测

Web4.0 建立在之前的 3 个 Web 的版本的基础上，引入了新的技术，目的是让互联网更加的用户友好、高效与安全。Web4.0 可能引入的新技术有脑机接口、元宇宙、人工智能、物联网等。其中脑机接口允许人类使用他们的思想与计算机进行交互并广泛应用于通信与娱乐。人工智能是计算机科学的一个分支，致力于创造能够独立思考与工作的智能机器。物联网是一个由物理设备、车辆、家用电器和其他物品组成的网络、这些物品嵌入了电子设备、软件、传感器和链接工具，使这些对象能够链接和交换数据。通过这些新的技术，可以让网络更容易被用户使用与活动，简化网页，使其更容易被导航和理解，并添加允许用户相互交互以及与页面内容交互的功能并使用户能够以更有效的方式相互联系并共享信息。

当下正处于重大技术转型的开端，虚拟世界是 Web4.0 的重要推动者，可以显著改变人们的日常生活，并为许多商业和工业生态系统带来广泛的机会，应确保企业、公共机构和个人抓住机遇，做好准备，同时应对随之到来的挑战。

2.8 卫星通讯

2.8.1 卫星通讯的定义

卫星通讯是指利用人造卫星作为中继器，将信息从一个地方传输到另一个地方的通信方式。利用信息与无线电波信号互转技术，借助发射和接收设备提供空中卫星与地面接收设备之间的信号传递，最终可实现远距离的信息传送。卫星通讯可以覆盖广阔的地理范围，包括陆地、海洋和空中，因此在军事、航空航天、电信、广播、气象等领域都有广泛的应用。

卫星通讯具有以下特点：

序号	特点	内容
1	广覆盖	卫星通讯可以实现全球范围的通信连接，覆盖陆地、海洋和

		空中，通信不受地理位置限制。
2	高速率	卫星通讯可以具有高速信息传输特性，从而满足大容量数据传输的业务需求。
3	稳定性	卫星通讯系统可以提供稳定的通信连接，不受地面基础设施的限制和天气条件的影响。
4	灵活性	卫星通讯可以根据需求进行灵活的配置和调整，满足不同应用场景的需求。

表 2 卫星通讯特点

2.8.2 卫星通讯的应用

近年来，卫星网络与移动通信网络及传统互联网融合技术逐渐成熟，数量庞大的低轨卫星组成具有全球覆盖、大容量宽带接入、低通信时延的互联网基础设施，为全球用户提供无缝的高速互联网接入。

卫星通讯网络包含以下典型应用场景：

- 全地形覆盖：地面基站无法覆盖到的区域，如海洋、湖泊、岛屿、山区等；移动平台，如飞机、远洋船舶、高铁。
- 应急通讯：地震、海啸等灾害。
- 广播业务：低速的广播服务，如公共安全、应急响应等消息等；广播，点播多媒体业务。
- IOT 服务：远洋物资跟踪、偏远设备监控、大面积物联网设备信息采集。
- 信令分流：通过卫星网络传递控制面的信息。

2.8.3 卫星通讯的趋势

卫星通讯的未来趋势包括以下几个方面：

- 全球覆盖能力

未来的卫星通讯系统将更加注重全球覆盖能力，广泛应用于各个领域，包括航空航天、物联网、农业、交通等，满足全球范围内的多样化的通信需求和应用场景，为不同行业提供定制化的通信解决方案。

- 高速宽带通信

随着卫星技术的不断发展，未来卫星通讯将提供更高速的宽带通信服务，满足用户对高速互联网的需求。

- 异构卫星协同通信

未来的卫星通讯系统将采用多卫星协同通信的方式，通过卫星之间的协同工作，提供更稳定和可靠的通信服务。

- 低轨卫星通讯网络

低轨卫星通讯网络（LEO）将成为未来的发展趋势。LEO 卫星通讯网络具有较低的延迟和更高的带宽，可以提供更快速的通信服务。

- 高度自动化和智能化

未来的卫星通讯系统将更加自动化和智能化，通过人工智能和自动化技术，实现卫星的自主运行和管理，提高通信系统的效率和可靠性。

总体来说，未来的卫星通讯将更加高速、全球化、智能化和多样化，为人们提供更便捷和可靠的通信服务。

2.9 算力网络

2.9.1 算力网络的定义

算力，就是设备的计算能力，一般分为通用算力、超算算力和智算算力三种类型。随着边缘计算业务的蓬勃发展，需要分布式多元化的算力资源，虽然这些资源可能归属于不同的所有方，但可以通过网络有效地将各方资源关联起来，形成一个整体提供给用户。算力网络就是一种根据业务需求，在云、边、端之间按需分配和灵活调度计算资源、存储资源以及网络资源的新型信息基础设施。在算力网络中，用户无需关心网络中的计算资源的位置和部署状态，而只需关注自身获得的服务即可，并通过网络 and 计算协同调度保证用户的一致体验。

算力网络的核心思想是通过新型网络技术将地理分布的算力中心节点连接起来，动态实时感知算力资源状态，进而统筹分配和调度计算任务，传输数据，构成全局范围内感知、分配、调度算力的网络，在此基础上汇聚和共享算力、数据、应用资源。

2.9.2 算力网络当前应用

算力网络的应用场景非常广泛，其中通用算力一般应用于消费互联网、产业互联网以及政府互联网等领域的常规计算场景，超算算力一般应用于科学计算领域和工程计算领域，而智算算力主要用于人工智能计算的相关领域，以下介绍一些主要的应用场景：

零：国家级战略工程“东数西算”

“东数西算”是国家于 2021 年推出一项重要的国家级战略，通过加快构建算力、算法、数据、应用资源协同的全国一体化大数据中心体系形成全范围的新型算力网络体系。在京津冀、长三角、粤港澳大湾区、成渝地区双城经济圈、贵州、内蒙古、甘肃、宁夏等地区布局全国一体化算力网络国家枢纽节点，建设数据中心集群，结合应用、产业等发展需求优化数据中心建设布局。将东部的算力

需求有序引导至西部地区，优化国家数据中心建设布局，促进东西部间的协同联动，使西部的优势算力资源更好的得以利用，支撑东部地区的一些场景需求，如东数西训（AI 训练）、东数西存（冷数据和温数据）、东数西渲（视频、VR/AR）等。

一、个人生活场景

虚拟场景：VR 虚拟场景观看点播或全景直播，通过算力网络提供差异化服务保障，何时何地都能享受社交、娱乐沉浸式服务体验，算力网络降低云游戏运营门槛，提升用户体验，算力网络促进应用在云端和边端部署，降低终端计算、存储等资源压力，让应用体验突破终端性能的限制，实现高质量服务升级。

二、智能交通场景

交通数据分析：摄像头、雷达等传感设备，获取交通多维数据，并对海量数据分析学习，推理调度决策，调节交通信号指导车辆自动行驶，

车路感知信息：全场景车路信息感知处理，需协同车内、车间、车路等多维度信息，基于算网协同调度能力，将不同时延、算力需求等应用分发到云、边、端算力节点，形成精准实时的驾驶策略。

三、智慧医疗场景

全息医疗影像：传统核磁共振等二维医学影像存在病灶模糊、病灶与健康组织重叠，及周围器官结构情况不能等问题，三维可视化技术将三维立体病理影响与 VR 技术结合，配置触觉交互等技术，医护人员可构建空间感的全息医疗。通过算力网络可实时构建渲染的全息影像，网络质量全程保障，满足医疗场景术前、术中和术后以及医疗教学多场景的影响分析需求。

四、高性能计算场景

尖端科研项目：如引力波验证、粒子加速器、蛋白质内部结构研究等尖端科研，需要大量 CPU、GPU、内存和网络资源。

高校科研：现有高校科研机构在科学数据处理时大多选择公有云算力或自建计算集群，成本高，算力网络的经济模式可将算力消耗的任务分布调度到社会存量算力上运行，降低科研单位算力成本。

2.9.3 算力网络未来预测

近年来随着全球范围内芯片、服务器、超级计算机等行业的发展，全球算力网络市场快速增长，2021 年我国算力产业市场规模约 535.18 亿元，同比增长 55.28%，2022 年市场规模约为 628.11 亿元。随着人工智能的快速发展，算力需求将大幅增长，预计 2023 年市场规模将进一步增长至 753.85 亿元。

算力网络技术发展趋势，预测如下：

算力呈现出内核多样化、分布泛在化的趋势。算力内核从通用走向多用，并通过定制化激发性能极致体验；算力不仅从单点向集群演进，更形成泛在化的分布式能力，并进一步向广域协同发展；算力基础设施从云向算泛在演进，其位置的分布从中心向边缘和端侧泛在延伸，具备云算力超集中、边端算力超分布的特征；算力服务形态从算力资源向算力任务转变，从简单的云边协同向云网边一体化转变。

算力与网络进一步深度结合的趋势。通过网络连接泛在算力，突破单点算力的性能极限；通过对算网资源的全局智能调度和优化，有效促进算力的流动，满足业务对算力按需使用的需求。同时，伴随着行业应用对网络端到端质量方面的极致要求，网络从尽力而为向端到端确定性保障演进。

算力网络中多要素融合、互相促进。算网大脑通过算网数据感知获取全域实时动态数据，结合算网智能化、多要素融合编排实现要素能力的一体供给和智能匹配，横向全面融合网、云、数、智、安、边、端、链多种能力要素，纵向深度贯穿应用、平台到底层资源，进而为新型信息基础设施对外提供一体化服务提供能力支撑。

2.10 物联网技术

2.10.1 物联网技术的定义

物联网(IoT)设备通过互联网或其他通信网络与其他设备和系统连接并交换数据,无需人工输入即可通过网络收集和传输数据,以实现设备的智能化识别、定位、跟踪、监控和管理。它是信息联网、移动联网基础上的一种新型连接模式,是一个多维度的生态化、智能化的网络体系。物联网技术基于计算机互联网和传输控制协议的基础,利用 RFID、无线数据通信、传感器等技术,构造一个覆盖世界上万事万物的“万物相连的互联网(IoT)”。物联网技术不是对现有技术的颠覆性革命,而是融合现有技术实现的综合运用。物联网核心技术包括传感器技术、射频识别技术、网络和通信技术、云计算、数据处理与挖掘等。

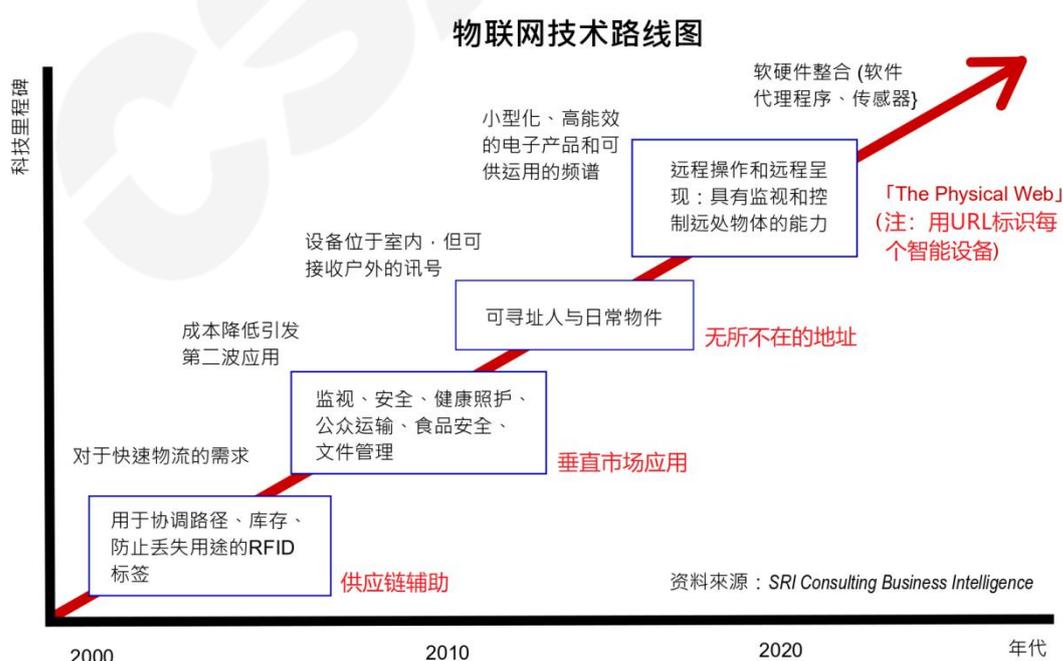
物联网技术架构分为三层:感知层、网络层、应用层。其中,感知层由各种传感器组成,将物体的数据,通过传感器收集后,由网络层传输发送;网络层包含互联网、云端、运营商网络、各种短距离局域网(如蓝牙网状网络、Wi-Fi、ZigBee 等);应用层是物联网与用户的交互接口,通过 UI 界面的形式展现。每层的关键技术为:

- 感知层:感知层的关键技术主要为传感器技术和短距离传输网络技术。其主要完成信息的采集、转换和收集等。
- 网络层:网络层的关键技术既包含了现有的通信技术(如:移动通信技术、有线宽带技术、Wi-Fi 通信技术等),也包含了终端技术,为行业终端提供通信能力的通信模块(如:蓝牙, ZigBee 等)。其主要完成信息传递和处理等。
- 应用层:应用层的关键技术主要是基于软件的各种数据处理技术(如:数据存储、并行计算、数据挖掘、平台服务、信息呈现等)。其主要完成数据的管理和处理,并将此数据与各行业应用的融合,实现应用创新。

随着计算技术、人工智能、大数据等的不断发展、完善与融合，进一步促进了物联网技术的创新技术发展。以下技术可用于物联网系统：

- **边缘计算**：边缘计算是指让智能设备向 IoT 平台发送或从中接收数据以及执行其他操作的技术。它提高了 IoT 网络边缘的计算能力，减少了通信延迟并缩短了响应时间。
- **云计算**：云技术用于远程数据存储和 IoT 设备管理，可以让网络中的多个设备访问数据。
- **机器学习**：机器学习用于处理数据并根据相关数据做出实时决策的软件和算法。机器学习算法可以部署在云中或边缘。
- **人工智能**：人工智能驱动了物联网的创新，创造了智能机器，可以在很少或没有人为干预的情况下实现智能行为和决策。

目前，已有组织为物联网技术的发展描绘出一条路线，其依据时间轴可分为四个阶段：供应链辅助、垂直市场应用、无所不在的寻址（Ubiquitous positioning）以及让每个智能设备都以 URL 来标示（The Physical Web），如下图所示：



2.10.2 物联网技术当前应用

随着物联网技术的快速发展，其广泛应用于智能家居、公共服务、农业、物流、服务、工业、医疗等领域，带动了物联网行业整体呈现爆发式增长态势。

工业应用：物联网在工业的应用称为工业物联网。以物联网、大数据、人工智能、云计算等信息技术为支持，让工业运作各个环节实现系统感知、分析和处理等功能，提高制造效率，改善产品质量，降低产品成本和资源消耗等。工业物联网涵盖了整个工业应用，包括了机器人、医疗设备和软件定义生产流程等，物联网技术是工业 4.0 中不可或缺的重要部分。目前主要应用包括智能制造、智能运输、智能物流等。

消费者应用：基于物联网技术的消费者应用主要体现在家庭物联网（例如：智能家电、家庭监控、智能手机等）以及移动物联网（例如：可穿戴设备、家庭自动化、联网的健康监控设备、远程监控设备等）。

农业应用：通过物联网技术，赋予农业以数字化、智能化改造。通过融合物联网、人工智能、大数据等现代信息技术，分析与运用从温度、降水、湿度、风速、病虫害和土壤成分等收集的数据，利用决策支持系统，实现了对农业生产全过程的精确管理与智能控制，可以实现农业可视化诊断、远程监控和灾害预警等功能。

除了上述介绍的应用领域外，物联网技术广泛应用于智慧城市、智能驾驶、医疗和保健、智能交通、零售业物联网等领域，科技与人类生活的完美融合，帮助人们更好地实现数字化、智能化、可持续化的生活和工作。

2.10.3 物联网技术未来预测

物联网 (IoT) 结合新一代通信技术、云计算、大数据、人工智能、边缘计算等新兴技术，可以提高运营效率、降低成本、改进决策并增强用户体验，成为各

个行业数字化转型的关键推动因素。对物联网技术的未来发展趋势，预测如下：

1、人工智能和物联网技术(AIoT)

人工智能广泛应用于机器学习、深度学习、自然语言处理和计算机视觉等领域，将对 AI、物联网、大数据技术、chatGPT 等创新技术的进一步融合，将为物联网带来新的创新活力。AIoT 结合了人工智能和物联网的技术和效率，使其适合解决分布式智能系统的特定问题。AIoT 解决方案将进一步促进从制造业到零售业、医疗保健、银行业等行业的产业升级。

2、更丰富的连接技术

随着 5G、6G、WiFi 6、LPWAN 和卫星等连接技术的发展与改进，物联网连接技术的各个方面也会随之改进，包括传感器、边缘计算、可穿戴设备、车联网等。进一步推动匹配物联网连接技术类型的基础设施的建设，更有效地支持物联网网络所需的连接技术和数据传输。

3、隐私和安全

鉴于物联网的规模和复杂性呈爆炸性成长，物联网设备很容易受到网络攻击、数据泄露、隐私泄露、非法入侵等。业界对此非常重视，目前已有多种解决方案为消费者提供更好的安全保障。未来，将有更多的端到端安全解决方案的使用。加快对物联网认证、边缘计算、终端安全、数据传输等防护技术、零信任等新技术的研究和探索，并将其应用于物联网安全防护中，满足物联网技术未来发展的隐私与安全保护需求。

4、低延迟和更安全的边缘计算

边缘节点主要负责现场/终端数据的采集，按照规则或模型对数据进行初步处理与分析，最终将结果予以上报，极大降低上行链路的带宽要求。云平台提供海量数据的存储、分析与价值挖掘。边缘计算将计算资源分配到边缘，而其他资源则集中在云端。边缘计算技术实现了云边资源的有效结合，这种特殊的计算布

局可以减少数据传输的成本和延迟，同时也提高了数据的安全性和隐私保护。随着物联网的发展，边缘计算将会进一步普及和应用，涉及更多的行业和领域，并为人们带来更多的便利和效益。

除了上述介绍的发展趋势外，物联网认证技术、云计算、可穿戴技术、数据的挖掘与整合、区块链等技术将进一步促进物联网技术的可持续发展。

3 2024 数字技术的安全挑战

3.1 量子计算的安全挑战

在现代密码学体系的支持下，全球建立了相对完善的密码保护体系。然而，密码破解技术一直在不断挑战和促进密码学的发展。尤其是以量子计算为代表的计算能力的快速发展，对基于大数分解和离散对数等数学难题的公钥密码系统提出了前所未有的挑战。与此同时，基于量子物理的量子密码技术（如基于量子通信的量子密钥分发）和基于新型数学难题的抗量子计算公钥密码算法正在承担抵御量子计算挑战的重任，部分企业（如 IBM）和研究机构（如中科院）已经开发出量子计算机的原型机，国家、机构甚至个人的核心数据保密需求将会面临目前已经被截获和储存等待未来破解的安全风险。因此，实践量子安全保护已经具备现实意义。

在现代密码技术中，量子密码的应用相对较少，主要集中在量子密钥分发和量子比特承诺等领域。其中，量子密钥分发是最受关注的应用之一，可以实现安全的信息传输。现在，我们将简要介绍传统密码系统，重点是安全的信息传输。

传统密码系统由密钥和密码算法两部分组成。密码算法通常是公开的，密码系统的安全性主要取决于密钥的保密性。在传统的加密过程中，加密者 Alice 拥有加密密钥 k_1 ，解密者 Bob 拥有解密密钥 k_2 ，攻击者 Eve 则是在传输信道上的存在。当 Alice 想要将数据 m 发送给 Bob 时，她使用加密密钥 k_1 对数据 m 进行加密，得到密文 c ，并将其发送给 Bob。Bob 使用解密密钥 k_2 对密文 c 进行解密，从而获得原始数据 m 。

根据密钥的使用方式，加密系统可分为对称加密系统和公钥加密系统。在对称加密系统中，加密和解密使用相同的密钥，即 $k_1=k_2$ ，这个密钥是保密的。对称加密系统包括流密码和分组密码，其中分组密码是最常见的。我们所熟知的 DES、AES 和我国的 SM1、SM4 都属于分组密码算法。这些算法通常是基于密码学家的设计原则和分析方法，而不是基于数学和计算复杂性理论中困难问题的。

量子计算机的快速发展有可能对现代公钥密码学形成挑战。由于量子计算机能指数或多项式量级地加快某些复杂计算问题的求解速度，因此现代公钥密码学很有可能被量子计算技术彻底颠覆。以 Shor 量子算法为例，其可以在多项式时间内解决大整数分解和离散对数求解等复杂数学问题，因此可以快速破解广泛使用的 RSA、ECC、ElGamal 等公钥密码。例如，分解一个 400 位的大整数，经典计算机需要约 5×10^{22} 次操作，而量子计算机仅需要约 6×10^7 次操作，后者所需操作数仅为前者的八十万亿分之一。

3.2 6G 通信技术的安全挑战

未来的 6G 通信网络架构将实现重大转变，由集中规划式向分自治式转变，存在海量的动态联结；由叠加复杂式向一体智简式转变，智能化简化，协议一体化简化；由外挂式设计向内生式设计转变，初始设计即考虑智慧内生安全内生，数字孪生；由多域异构向统一融合转变，一套架构多种场景，一套协议多种组网。在这种情况下，6G 通信技术的安全挑战将变得更加复杂，主要的挑战包括：

- 空天地海跨域安全挑战

6G 对于卫星通信、人工智能、大数据等技术的创新融合，以及不同应用场景下软件定义切片的灵活泛在应用，将会在 5G 基础上进一步实现信息的随时随地可取，并推动整个社会各个行业走向数字化，这同时使得传统的安全边界变得更加模糊，整个网络面临更多的挑战。随着网络架构革新与区块链、AI、数字孪生、量子计算等新技术的应用，6G 网络将展现更高性能的通信指标，也将衍生出全新的通信安全挑战。因此，6G 网络的接入异构一体化、设备接入小型化以及不同应用场景的切片化、通信服务边缘化，都将对 6G 通信安全问题变得更加

有挑战。

● 内生安全挑战

6G 时代，安全从“补丁式 Add-on”的传统安全模式转变为网络主动免疫、安全弹性自制的内生安全模式。内生安全应具备“自适应”、“自主”、“自成长”的特点，在网络的不同场景业务下，能够根据业务特性，立足于自己的安全需求，针对不同的攻击类型，建立自主的防御架构，构筑持续成长的安全能力。这就要求网络要与 AI 结合，在遭受攻击时动态调整安全策略、业务运行态势、暴露面，减少攻击伤害、保障业务顺畅运行、定位和解决安全问题。

● 物理层安全挑战

可见光通信 VLC 作为 6G 通信系统中光无线通信的主要部分，将会在未来有大范围的应用。VLC 本身具有一些固定的安全性能，如可见光的物理性质决定了它的传播范围局限在一个没有遮挡物的区域内，这样在室内通过可见光进行的数据传输在理论上无法被室外或者遮挡物之后的人拦截和窃听。然而，与通信双方在同一空间下的实体，就很容易发现并窃取到信息，因此，VLC 技术需要足够可靠的物理层安全技术来对其通信的机密性进行保障。

3.3 人工智能的安全挑战

随着 AI、大数据、云计算等技术的快速发展和应用，AI 安全作为一种新生事物正在悄然滋生着，正在成为当前许多领域愈发关注的重要问题。这些挑战可以总结为以下几个方面：

1、AI 带给社会的冲击和负面影响。

1) 数据隐私和泄露以及知识产权纠纷：生成式 AI 系统依赖大量数据进行训练和学习，主要来源是从互联网上获取，其中可能包含用户的敏感信息。此外，还存在知识产权的纠纷，如文章、图片的知识产权归属问题。

2) 偏见和不公平性：AI 系统的训练数据可能存在偏见，导致系统在做出决

策或提供服务时对某些群体不公平。例如，招聘算法可能会对某些特定人群进行歧视性筛选，造成不公平的结果。

3) 敲诈勒索事件会上升：生成式 AI 容易生成虚假图片、虚假视频、虚假电话；真假难辨。导致今后社会上敲诈勒索事件将会多发。学术不端的事件也会上升。

2、对生成式 AI 的网络攻击

1) 作为提供互联网服务的生成式 AI 网站，其互联网基础设施的安全问题不容忽视。AI 网站可能遭到 DDoS 攻击、勒索攻击、APT 攻击、SQL 注入等。

2) 提示注入攻击：黑客可以通过发送恶意提示信息，引诱生成式 AI 输出敏感信息和非法信息。如：奶奶攻击。

3) 对 AI 数据的投毒攻击：主要是在训练数据中加入精心构造的异常数据，破坏原有的训练数据的概率分布，导致模型在某些条件会产生分类或聚类错误。

3、AI 使能的网络攻击技术

AI 使能的攻击技术已经快速发展。在网络钓鱼方面，利用 AI 制作网络钓鱼电子邮件，已经向用户展现出其强大的能力。恶意攻击者可以利用它来生成令人信服的网络钓鱼和鱼叉式网络钓鱼电子邮件，并且这些恶意电子邮件可以轻易地通过电子邮件提供商的垃圾邮件过滤器。

在 AI 自动生成攻击代码方面，黑客专用的大模型网站 FraudGPT 可自动生成多种网络攻击代码，低门槛无编程快速。已被证明能够自动生成针对攻击目标的网络端点和 IT 环境量身定制的恶意脚本和代码，逃避端点检测和响应系统。并开发可以绕过静态签名检测的恶意软件变体。FraudGPT 上线一周里竟有逾 3000 买家下单！

FraudGPT 的“成功”，标志着生成式 AI 武器化和黑客攻击技术大众化的危

险时代已经到来。意味着初级黑客个人就可以借助生成式 AI 每日生成多个高级网络攻击武器，包括 AI+勒索、AI+APT 攻击等。互联网上黑客机器人开始泛滥。AI 网络攻击武器已经列装多国网军。

以生成式人工智能为代表的 AI 技术的进步使得网络空间防御变得异常困难。几乎所有的基于攻击特征值的传统安全产品将会被千变万化的 AI 赋能的网络攻击技术轻松地、低成本地击穿。攻击者会使用 AI 技术去识别和发现防守方的 IT 系统、OT 系统、云平台的各种漏洞（已知漏洞、未知漏洞、秘密漏洞），并实施精准攻击。

为解决人工智能发展带来的新的安全挑战，需要在技术、政策和法律等多个方面采取措施，才能确保人工智能技术的安全和可持续发展。

3.4 云原生的安全挑战

随着云原生的快速发展，核心能力逐渐稳定，安全问题日趋紧急。在云原生安全领域不但有新技术带来的新风险，传统 IT 基础设施下的安全威胁也依然存在。早期的云原生安全 1. x 方案已经无法满足复杂多样的安全防护需求。

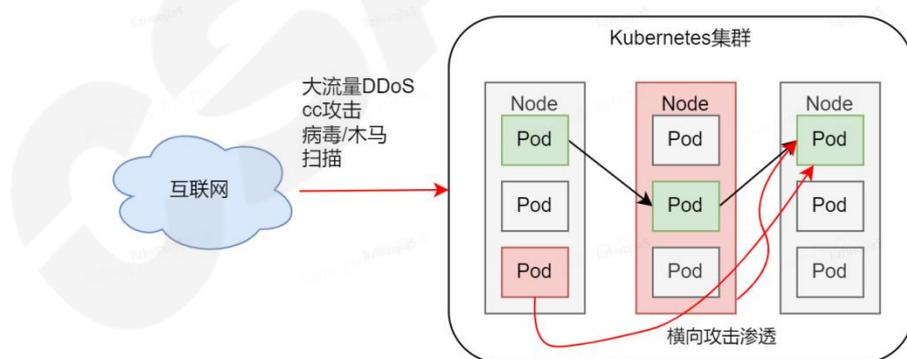


图 10 云原生威胁

● 云原生技术带来的新安全风险

云原生技术发展的同时带来了一系列全新的安全挑战与冲击。据 Red Hat

的发布的 Kubernetes 安全状况报告记录的安全事件中, 53%是由于配置错误造成的, 38%是由于利用漏洞造成的。主要不安全的配置有: K8S 组件的问题主要是指各组件的不安全配置、API Server 未授权访问、etcd 未授权访问、kubelet 未授权访问、kube-proxy 不安全配置。统计数据显示高达 47%生产环境容器镜像会来源于公用仓库。Docker Hub 上的公开可用镜像进行的一项研究: 51% 的镜像存在严重漏洞, 400 万个最新镜像中约有 6,500 个可能被视为恶意。由于无意中的不良编码行为, secrets 可能会嵌入 image 中, 通过将 SSH 密钥或 API 密钥嵌入到容器中, 攻击者可以在部署容器后获得访问权限。镜像没有使用特定用户进行配置来运行, 导致权限失控。

容器运行过程 IP 快速变化, 通过传统基于 IP 的边界防护难以实施。容器之间网络互相连通, 入侵到某一个容器后, 很容易进行横向渗透攻击。

微服务导致内部调用快速增长, 服务之前认证鉴权复杂, 请求难以跟踪, 很容易就造成权限失控、数据泄露。

- 传统 IT 基础设施的威胁依然存在

云原生不能脱离底层 IT 基础设施: 计算、存储、网络而存在, 因此这些 IT 基础设施面临的问题在云原生场景下依然存在。DDoS 攻击防护、cc 攻击防护、Web 攻击、漏洞、木马、病毒、数据泄露等等安全风险, 并没有因为云原生的发展而降低。

同时, 云原生安全 1. x 无法满足快速发展的业务需求。在云原生安全早期, 人们的惯性思维就是利用传统的安全防护手段去进行云原生安全防护。经过这么多年的攻防对抗, 传统产品在各自的领域都已经身经百战, 解决对应的安全问题也都不在话下, 这些安全产品通过简单地改造, 就可以与云原生架构配合运行。这个阶段云原生安全尚未构建一个完整的架构, 各安全产品就像搭积木一样跟云原生架构进行配合。随着产品构建, 工程师们很快就发现, 安全并没有因为云原生的到来发生什么改变, 这种搭积木式的云原生安全方案, 从远处看各方面的安全都能有, 但是从近处看就能看到安全产品之间基本没有联系, 使用起来并没有

什么改变，安全和云原生是两个独立的领域，这样的架构无法支撑云原生的快速发展，也没有办法满足云原生安全的自动化、智能化发展趋势。

3.5 数字孪生的安全挑战

数字孪生是现实世界的数字映像，其价值使它可能成为网络攻击的对象。为了实现数字孪生应用，在不同场景下集成了不同的数字技术，包括：数字标识、网络连接、高性能计算、智能控制、3D 建模、仿真、虚拟现实与增强现实、人工智能等技术，以及不断涌现的新技术，诸多技术的运用给数字孪生带来了网络安全复杂性的挑战。

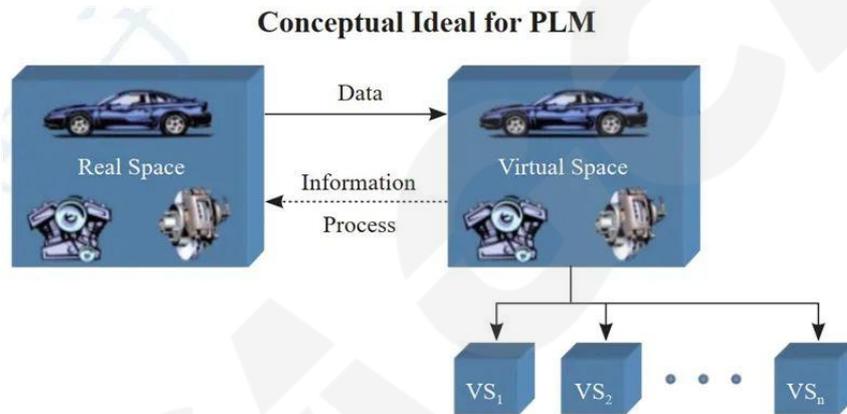


图 11 Grieves 全生命周期管理课程

上图来自美国密歇根大学 Grieves 教授的产品全生命周期管理课程，虽然当时“Digital Twin”一词还没有被正式提出，Grieves 将这一设想称为“Conceptual Ideal for PLM (Product Lifecycle Management)”，但在该模型中虚拟空间构建的数字模型与物理实体交互映射，忠实地描述物理实体全生命周期的运行轨迹。该图明确的显示了数字孪生具备 IoT、传统网络安全的特质，同时数据 (Data、Information Process) 是数字孪生技术的核心承载，因此其数据自身和生命周期安全需要特别的重视。

传统网络安全：数字孪生处理系统建立在传统网络与基础设施之上，因此需要应用网络安全与信息安全的对数字孪生可能发生的安全问题进行防范、检测和

响应，包括基于资产、漏洞与威胁对网络安全风险建模等方法；

IoT 属性相关安全：数字孪生的现实世界（物理）对应物是物联网（Internet of things），典型的物联网安全在数字孪生的世界里同样适用，例如：PLC 安全；

数据生命周期管理：数字孪生的基础是基于现实世界对应物所采集的数据，因此数字孪生天然就是数据安全，因此数据全生命周期安全管理和数据治理也是数字孪生所必须完成的工作；

数据污染防范：数字孪生处理系统往往基于机器学习与人工智能的技术应用，而机器学习和人工智能的应用需要优质的数据集，包括训练数据集、验证数据集，因此，防范数据污染工作是数字孪生需要解决的重要安全问题之一。

3.6 隐私保护的安全挑战

个人信息安全是当今数字时代面临的重要挑战之一。随着大数据和云计算的兴起，个人和机构的数据正在以前所未有的规模被收集、存储和分析。然而，随之而来的是日益增长的个人信息安全风险。

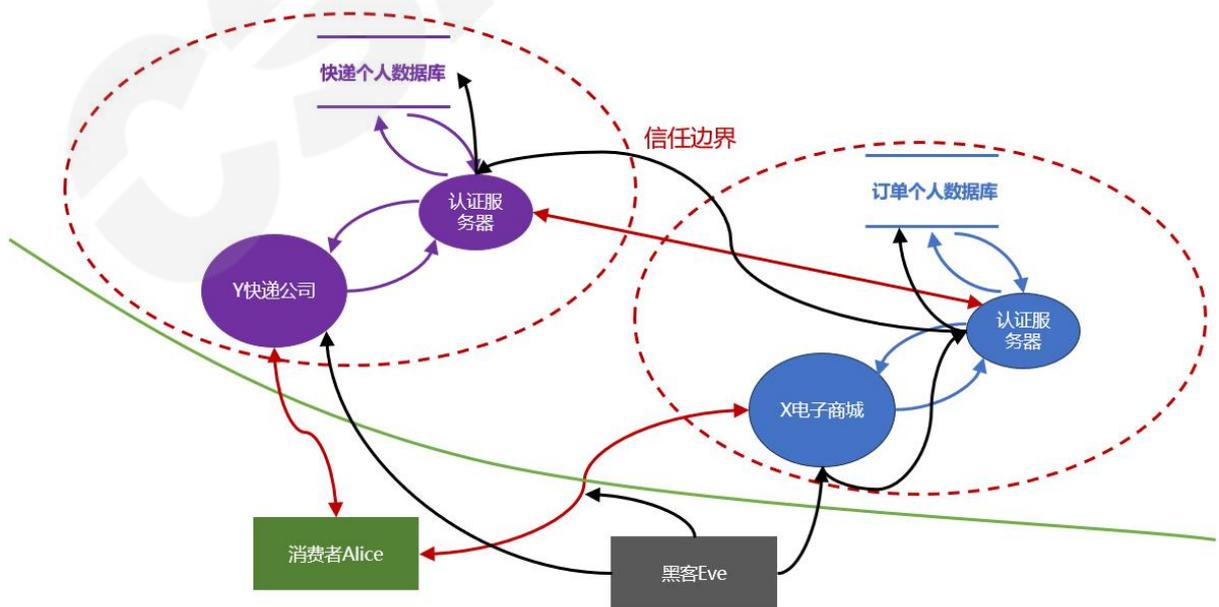


图 12 消费者进行网上购物面临的威胁建模示意图

- 大数据带来的数据融合，增加精准个人识别、数据滥用、隐私泄露的风险。在多数情况下，个人信息泄漏事件被公众知晓是滞后的。以消费者网上购物为例，电子商城或快递公司的个人数据被黑客攻击获取到后，就可以开始地下交易。个人信息对于攻击者而言就是金矿。个人信息富含个人信息、购物信息、社会关系、访问凭据、健康和资产等信息，既可以在地下交易，也可以为下一次攻击提供丰富的情报。在很多勒索攻击事件中，受害者数据并没有被加密，攻击者通过所窃取的数据进行精准个人识别并勒索。
- 员工依然是安全防护的薄弱点。除了员工恶意地实施数据泄漏之外，还有相当比例的数据泄漏与员工的疏忽和安全意识不足有关。一方面，人为错误直接暴露信息，另一方面，无法准确地辨识威胁使得社会工程和各种钓鱼攻击能够得逞。泄漏的信息又增强了下一次攻击的欺骗性，这是一个恶性循环。
- 个人数据安全合规。在数字化时代，个人数据已经成为组织的宝贵资产，但同时也带来了许多隐私和安全问题。为了确保个人数据的安全和保护，政府和监管机构制定了许多隐私法规（如欧盟 GDPR、中国的个保法）和标准（如 ISO 27701）。这些法规和标准要求组织遵守一系列数据处理和安全保护措施，以确保个人数据的合规性和安全性。如果组织未能遵守适用的法规和标准，可能会面临巨额罚款和声誉损失。不合规的数据处理实践也可能导致个人数据的泄露、滥用和不当使用，对受影响的个人的权利和利益产生负面影响。此外，由于各国法律标准和监管机构的不一致，跨国数据流动带来的合规问题成了一个复杂的挑战。

3.7 Web4.0 的安全挑战

Web4.0 比以往的技术迭代更具有革命性，与其他所有的新技术一样，必然存在一些需要克服的安全风险。随着越来越多的个人数据被存储在线上，身份盗窃和其他网络犯罪的风险也越来越大。保护用户的个人信息和隐私权，防止数据

泄露和滥用，将是一个持续的挑战。在 Web2.0 时代，大量数据被集中存放在平台的远程服务器中，数据泄露将造成严重的后果。在 Web3.0 中，身份认证依赖与密码学技术，对私钥的保密要求很高，同时部分的数据存储在公链上，这些数据虽然经过加密，但随着硬件算力的提升与密码学的发展，这些数据的安全性会遭到严重威胁。而 web4.0 中引入的物联网和脑机接口技术，如果发生数据泄漏，将对实体资产和身体健康造成破坏。

- 随着人工智能在 Web4.0 中的广泛应用，恶意用户可能会利用 AI 进行自动化的攻击，例如自动生成钓鱼网站或冒充身份。在软件及硬件层面，包括应用、模型、平台和芯片。编码都可能存在漏洞或后门来实施高级攻击。在模型层面上，攻击者同样可能在模型中植入后门并执行攻击。在数据层面，攻击者同样能够在训练阶段掺入恶意数据，影响模型的推理能力，也可以在判断阶段对要进行判断的样本加入少量人类难以察觉的噪声，来可以改变检测结果。
- 物联网设备的爆炸式增长为网络安全带来了新的挑战。许多 IoT 设备存在弱点，攻击者可以利用这些弱点入侵网络，从而威胁到用户的隐私与安全。物联网设备同时存在着物理安全与生命周期安全，IoT 设备可能被物理攻击，包括设备被窃取、拆解等。同时在设备寿命结束之后，数据可能被泄漏。
- 从 Web2.0 时代开始，云计算就变得越发主流，到了 Web4.0，云计算的安全变得更加重要。去中心化的结点基本都运行在云服务器上，云服务器上存储着账本和身份认证等重要信息，如果不对这些敏感信息进行适当的加密与访问控制，会导致严重的安全威胁。
- Web4 中新普及的 AR 和 VR 技术可能会导致新的安全风险，包括用户在虚拟环境中受到追踪或被侵犯隐私。AR 和 VR 在提供沉浸式和增强现实体验时会收集大量用户的隐私信息，如位置数据、生物特征等，在未经过充分保证的情况下，这些信息可能会被滥用或泄露，造成隐私问题。虚拟环境

的交互与信息提供有别于之前的 Web 服务，恶意用户可能会在虚拟环境中进行欺诈、骚扰或虚假信息的传播。

总而言之，web4.0 相较于之前 web 服务，融合了更多的新技术，每个新技术在带来更友好的交互方式的同时也带来了新的风险，多种新技术的组合也可能产生难以预料的新问题，只有清楚每种新技术的缺陷，才能应对新出现的挑战。

3.8 卫星通讯的安全挑战

卫星通讯在提供便利性和广覆盖的同时，由于其架构复杂、拓扑时变、网络开放等特性，面临的安全挑战将会更加严峻。早在 2016 年，欧洲航天局的一颗卫星被黑客攻击，黑客通过入侵卫星控制系统，篡改了卫星的指令，导致卫星无法正常运行。这个事件引起了对卫星通讯安全的广泛关注，并促使相关机构加强了卫星通讯系统的安全性。大量案例表明卫星通讯系统面临着来自黑客和间谍等恶意攻击者的各种安全威胁和攻击，对其承载通信业务和个人信息造成严重危害。

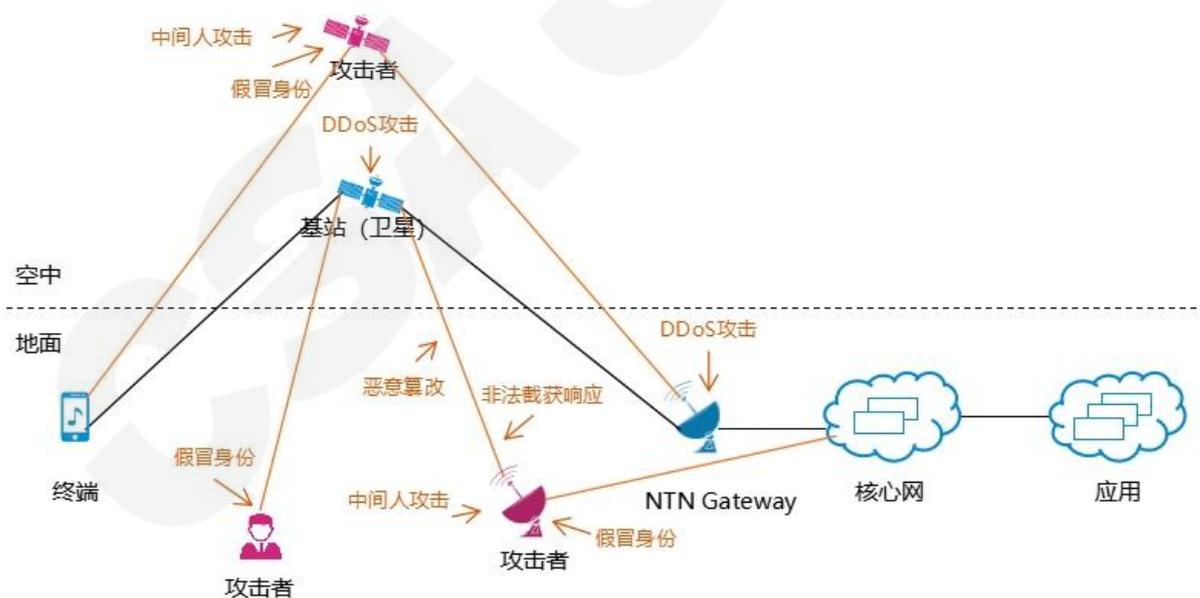


图 13 卫星通讯面临的安全威胁示意图

具体地，卫星通讯存在以下安全挑战：

- 身份可信。卫星通讯中的身份验证是一个重要的安全问题。如果未能正确验证通信的发送者和接收者身份，可能会导致未经授权的访问和信息泄露。对于终端，由于空天地通信覆盖的终端类型更加丰富，海量的终端全球随时随地接入，终端的真实性问题不可小觑。对于卫星设备，由于卫星节点不断加入，卫星设备的可信性理应更加重视。卫星节点部署位置呈现周期性变化，使得卫星通讯网络的拓扑始终高度动态变化，任何潜在的脆弱性、漏洞、错误配置等安全问题都可能帮助攻击者假冒、劫持合法网络节点，窃取、篡改、伪造数据，对网络内部或者接入终端造成威胁。
- 数据安全。基于移动通信的卫星通讯网络需要移动通信网络和卫星网络的异构互联互通。业务数据需进行远距离跨域传输，数据传输过程中黑客可以通过截获卫星信号或攻击地面站点来获取敏感信息。数据传输的安全防护难度加大，增加了数据窃取、劫持、篡改或破坏等攻击威胁的可能性。需要重点考虑对网络进行分段保护或是端到端保护。
- 网络通信安全可靠。现有移动网络的攻击，在基于移动通信的卫星通讯网络中仍然存在，再加上卫星网络环境的开放性、较低的处理能力等，基于移动通信的卫星通讯网络可能更易遭受中间人攻击、DDoS 攻击等安全威胁，增加了数据窃听、篡改等安全威胁的可能性，给业务的可用性、可靠性带来了严峻的挑战。
- 网络隔离。无线网络切片为不同行业应用在共享的网络基础设施上，提供差异化的网络服务，推动了应用服务的发展，而现有的网络中并未考虑切片机制，卫星网络融合无线网络后，也需考虑切片的安全机制，尤其是切片隔离机制。
- 物理安全。卫星通讯设备和基础设施需要保护免受破坏或盗窃等物理攻击，包括保护地面站点、卫星发射设备和卫星本身。

3.9 算力网络的安全挑战

算力网络通常将算力资源彻底融入通信网络，以一个更整体的形式提供给满足用户需求的资源服务。由于算力的泛在化引入了更多的安全风险点，更加开放的网络架构和更大范围的数据流动导致不确定性安全威胁增加，相较于传统网络，算网安全风险的变化主要体现在以下几个方面：

- 算力终端的多维度攻击挑战。算网终端的泛在接入导致的网络攻击暴露面增加，巨量的泛在终端存在被恶意软件感染的风险。算力网络将边缘计算、云资源池、个人终端、物联网终端等不同类型的计算资源整合后提供算力服务。这些算力节点分布式存在于算网中，其中可能存在一些不可信节点，它们可能故意提供错误的计算结果，从而破坏整个网络计算的准确性。算网网络中的重要计算资源，可能成为黑客发动的大规模服务拒绝攻击（DDoS）的目标。一旦网络服务被拒绝，将导致计算任务无法正常进行，从而引起算网局部乃至整体能力的瘫痪。
- 算网网络架构变化引入的风险。算力网络架构上分为多层，一般包括资源层、编排控制层以及运营层。在各层之间存在大量的调用接口以及每层引入的新网元实体或能力均会带来大量的风险因素，如新增算网大脑单元风险、承载感知、决策和控制能力的网络功能单元、SRv6 技术及其承载单元的安全风险等。
- 算力使用及交易流程引入的风险。数据泄露风险，算力网络存储大量数据，既有个人信息，也包括商业秘密数据等。如果未能采取有效的安全措施，黑客可能利用漏洞获取这些数据，并进行非法利用。因算力交易新商业引入的端到端数据安全风险和管理复杂度双提升，如数据暴露面增加、存证溯源复杂度和要求提升等带来的算力交易风险。

3.10 物联网技术的安全挑战

随着物联网技术的不断发展，其将不断赋能各行各业，成为产业升级、应用场景创新发展、产业链持续完善的重要动力。物联网技术涉及通信网络、云计算、人工智能、移动 APP、WEB 等技术，不仅沿袭了传统互联网的安全风险，而且还包括传感器安全风险、感知终端安全风险、云端安全风险等。通过对安全风险进行分析，物联网的安全风险建模如下图 14 所示：

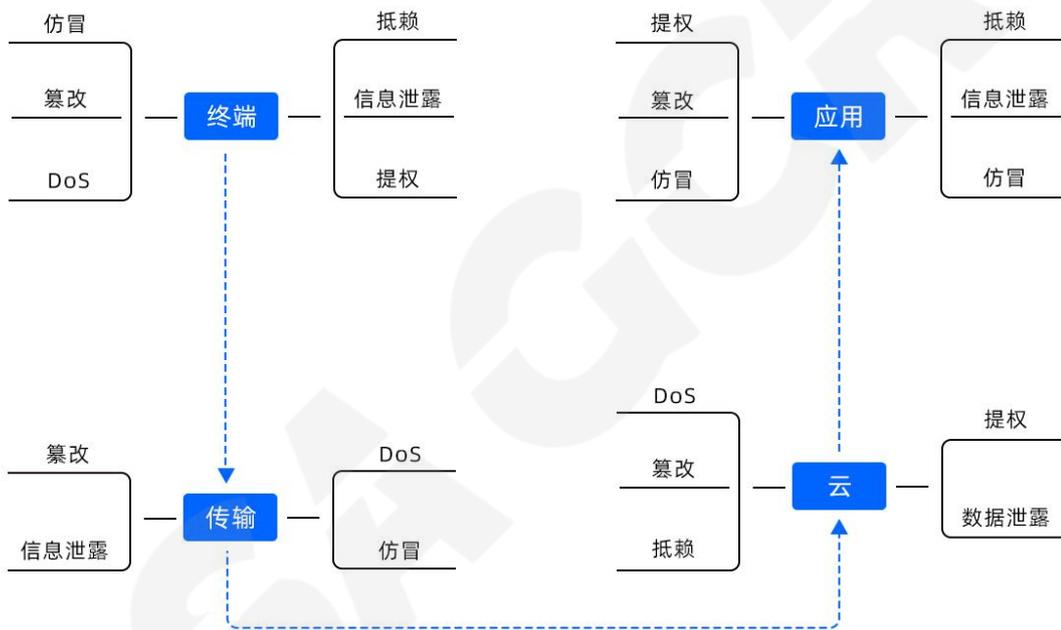


图 14 物联网的安全风险建模示意图

随着新技术、法规、用例和威胁的出现，物联网技术仍面临着一系列的安全挑战，主要体现在以下几个方面：

- AIoT 技术的安全挑战。AIoT 系统的安全问题包括内外部安全问题。内部安全问题主要是 AI 资产的安全。AI 需要实时检测、评估和响应各种输入，因此 AI 内部存储设备和接口不适合加密，否则同样的操作需要耗费更多的资源 and 时间。通常将其存储在外部非易失性存储器中，这将使其面临着日益增加的攻击风险，因此内部存储设备和接口设计都需要采取适当的安

全防护措施。AIoT 安全的外部挑战也日益增加，各国政府都被勒索软件和其他恶意事件攻击日益频繁。此外，AIoT 系统需要多种类型的计算，主要包括智能终端、网络设备、云服务、业务服务等部分。其中智能终端是最基础也是最关键的一环，而智能终端所依赖的 AI 芯片、操作系统、AI 算法等仍依赖国外技术，甚至使用国外密码算法。AIoT 核心部件“卡脖子”的核心技术掌握在别人手里，供应链未能实现自主可控，无法满足我国现有安全合规要求。

- **数据安全传输。**在信息技术背景下考虑数据传输的安全性并不是新问题，但物联网实现的诸多属性提出了新的独特安全性挑战。由于物联网的网络异构特性，攻击者能够在数据传输过程中找到合适攻击点的概率大大增加。在数据传输过程中可能发生的安全挑战主要包括：仿冒、篡改、信息泄露、拒绝服务等。
- **应用安全。**随着物联网技术的快速发展，现已广泛应用于不同的领域，部署的云端服务、应用程序、应用系统和相关软件的漏洞都可能导致系统受攻击和破坏。不安全的应用程序风险如缺乏数据访问权限设置及授权、身份认证、系统或用户的密码缺乏复杂程度或使用弱加密算法、缺乏输入和输出认证等。不同的应用会有不同的用户使用权限，因此需要采用身份验证技术和访问控制方法以防止非法用户的访问和保障企业数据安全。软件漏洞和配置错误是物联网技术的常见威胁，这些威胁通常易被攻击者使用的攻击工具入侵。软件开发人员采用非标准代码来编写软件，这可能会导致缓冲区溢出漏洞等问题。使用不安全的接口、不安全的默认配置、过时的组件、弱密码等技术，也会使安全漏洞频发。

4 应对策略与案例研究

4.1 量子计算的安全应对策略及案例

量子算法的出现对传统密码系统产生了一定的冲击。相对于经典算法，量子

算法在某些问题上具有显著的加速性，即可以在多项式时间内解决传统计算机需要指数时间解决的问题，比如大整数分解。然而，并非所有数学问题对量子算法都具有优势，对于某些问题，如 NP 完全问题、基于格、基于编码和基于多变元方程的数学问题，量子算法并没有明显的优势。

尽管如此，量子计算的发展催生了后量子密码学的研究，旨在设计对抗量子计算机的经典密码算法。其中一个基本问题是 Learning Parity with Noise (LPN) 问题，要求在已知系数和结果的情况下解决未知数。该问题被证明是 NP 完全问题，迄今为止，无法找到解决该问题的有效算法。在该领域，我国学者在后量子对称密码算法和密码分析上取得了领先成果。

LPN 问题的推广是 Learning with Errors (LWE) 问题，其要求解决在更大的素数域上的方程组。虽然 LWE 在效率上有所降低，但它具有更广泛的密码应用，如公钥加密、抗碰撞哈希函数和全同态加密等。

保密类型	技术基础	专用设备	出发点	关注点	安全性	现存问题
经典密码	数学原理	无需专用设备	解析数学难题	密钥的保密性	不能抵御量子计算机攻击	不能抵御量子计算机攻击
QKD	物理原理	需专用设备	一次一密加密体制	解决密钥分配问题	量子环境下，理论绝对安全	成本高、有硬件要求、应用场景有限
PQC	数学原理	无需专用设备	解析数学难题	非对称密码系统	量子环境下，理论绝对安全	未经过充分验证

图 15 PQC: Post-Quantum Cryptography, QKD:量子密钥分发

量子算法对于传统密码系统的冲击是双重的，一方面它可以高效地解决某些问题，另一方面它也催生了后量子密码学研究，以应对量子计算机的威胁。美国国家标准技术研究所 (NIST)、欧洲电信标准化协会 (ETSI)、美国电气和电子

工程师协会（IEEE）以及大型科技企业（如谷歌、微软）等对后量子密码的技术应用和标准制定投入了大量的工作。

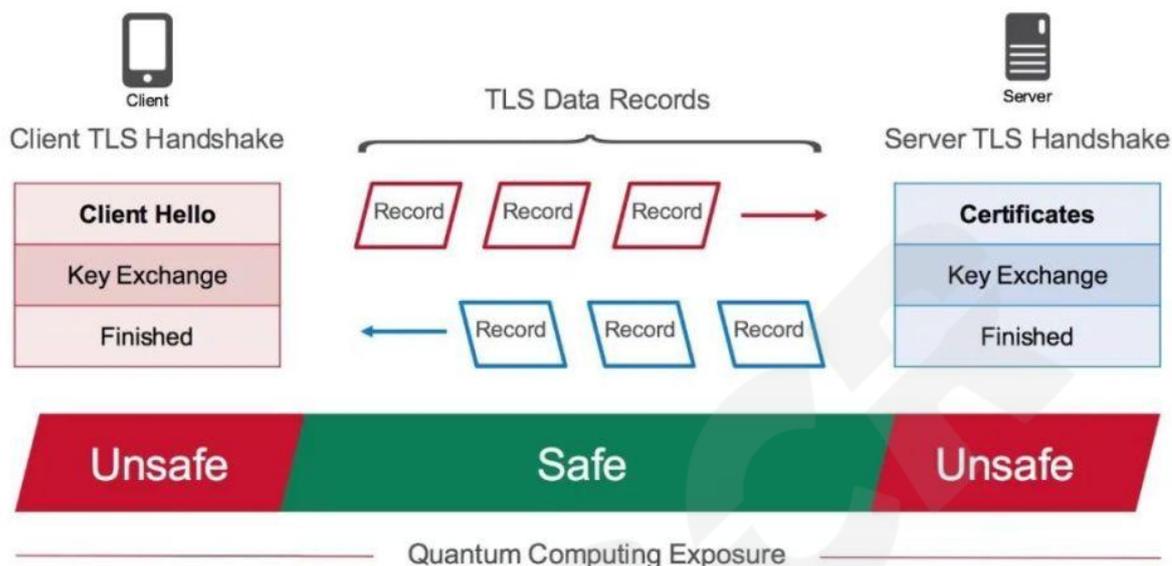


图 16 Quantum computing exposure, TLS Protocol

从 Chrome116 版本开始，谷歌 Chrome 浏览器将支持混合后量子密钥协议 X25519Kyber768。这种混合机制将 X25519 椭圆曲线算法与 Kyber-768 抗量子密钥封装方法结合起来，用于会话密钥的创建。X25519 在 TLS 中广泛用于密钥协商，而 Kyber-768 是美国国家标准技术研究院（NIST）公布的首批后量子密码标准算法之一。O'Brien 指出，谷歌团队正在努力准备网络迁移到抗量子密码学，并更新技术标准，测试和部署新的抗量子算法，与生态系统合作，以确保成功应对这一重大转变。

谷歌浏览器使用的 TLS（传输层安全协议）是一种加密协议，可为通过 Internet 在应用程序之间发送的数据提供端到端的安全性，它通过加密称为记录的应用程序数据块来实现这一点。

这些记录使用所谓的对称密码进行加密，通常是像高级加密标准（AES）或像 AES-GCM 这样的流密码，它生成一个数据流，可以简单地与明文进行 XOR 操作以创建密文。记录的最后部分是一个哈希消息认证码（HMAC），这是校验和。接

收者可以使用 HMAC 来确定记录没有被篡改。但是，在客户端和服务器开始在传输过程中来回发送这些记录之前，它们需要就用于加密所有记录的快速加密密钥达成一致。应用最广泛的公钥密码系统是基于椭圆曲线离散对数分解的 ECC 和基于大数的质因数分解的 RSA 加密。然而，ECC 和 RSA 都容易受到量子计算机的攻击。一旦密钥被破解，传输的数据就会被盗取，这意味着在 Chrome 中，越早更新 TLS 以使用抗量子会话密钥，就能越早保护用户网络流量免受未来量子密码分析的影响。

谷歌 Chrome 的使用混合椭圆曲线算法和抗量子密钥封装方法这一策略标志着整个网络安全领域对于量子计算潜在威胁的认知升级。在量子计算日益成熟的今天，传统的加密方法可能会面临前所未有的挑战。而谷歌此次的决策，实际上是对未来可能的量子攻击的一种预防性策略。

4.2 6G 通信技术的安全应对策略及案例

6G 安全应对策略可以分为三类：一是技术赋能 6G 安全，包括区块链、软件定义安全和人工智能安全等技术；二是可信内生安全技术，包括无线物理层安全、拟态防御拟态构造等技术；三是传统安全技术增强，包括量子安全、隐私保护等技术。从保障目标来看，三类技术将围绕安全、弹性和可信的目标，支撑整体 6G 安全体系设计。重点介绍其中几种应对策略和案例。

● 无线物理层安全技术

无线物理层安全技术利用无线信道的各点异性、随机时变性和第三方测不准特性等天然的内生安全属性，面向电磁传播机理的内源性缺陷设计安全功能，提供可融合但不依赖于传统密码的安全方案，在物理层实现对抗无线广义不确定扰动的无线通信广义鲁棒控制。

(1) 轻量级接入认证

物理层认证技术，是利用无线网络物理层的私有信道特征提供低复杂度、高安全性的安全方案，分为基于设备指纹的认证和基于信道指纹的认证两种。前者

利用硬件设备的电特性差异提取设备独有的特征，将这种唯一标识作为设备的认证指纹；后者不需要额外的信号提取设备，从无线信道特征入手，利用不同位置设备的信道特征之间存在的不相干性进行认证。

（2）轻量级加解密

物理层密钥生成技术，通过利用信道的互易性、时变性、唯一性等特征，基站与用户对信道进行探测，得到共同随机性以生成对称密钥，进行轻量级的加解密处理。物理层密钥生成可以做到一次一密，实现信息论安全的密码安全保护。

（3）6G 案例应用

6G 网络为多种网络环境下的海量设备提供了统一的接入服务，包括移动通信网、卫星互联网、车联网、智慧城市、物联网等。这些异构设备的接入认证需求各不相同，例如车联网传感设备需要低时延和轻量级的认证，而卫星互联网终端则需要随时接入和频繁切换的认证。未来，6G 网络可能会采用可见光通信技术、超大规模天线技术、AI 无线通信技术等技术，这些新技术对 6G 无线安全技术提出了更高的要求。

● 核心网拟态防御构造技术

拟态防御以动态异构冗余（Dynamic Heterogeneous Redundancy, DHR）构造为核心，基于“结构决定安全”的方法论，具有安全性可量化设计/可验证度量的实践规范，能够用一体化架构解决 6G 网络安全与功能安全交织难题等，有效防御“挖漏洞、设后门、植病毒、藏木马”等基于软硬件内部漏洞后门的经典网络攻击，有力抑制或管控确定或不确定风险、已知或未知的安全威胁，是实现网络弹性的理想解决方案。

（1）内生安全原生云平台

内生安全云原生平台架构上可分为基础设施层、云平台层和应用层，通过对微服务拟态化共性需求进行提炼，形成内生安全微服务框架。内生安全微服务框

架能自动化地为微服务应用提供拟态基础能力，包括拟态架构编排、异构执行体的选择、定时执行体轮换机制、受攻击执行体轮换机制等。

（2）拟态构造微服务

核心网内生安全技术利用 6G 网络池化资源的动态性、异构性、冗余性等天然内生安全属性，针对微服务通信故障或微服务功能设计实现上的漏洞后门带来的未知安全威胁，遵循隘口设防/要地防护的防御原则，对网络关口和关键微服务等进行内生安全 DHR 构造，利用不可信、低可靠的构件来构造安全、可靠的系统，同时应对不确定安全威胁和不确定随机故障，一体化解决安全可信性、功能可靠性、服务可用性。

（3）6G 案例应用

面向人机物三元融合的世界，还需特别重视 6G 网络的广义功能安全（Safety & Security），以便能有效应对“高强度网络战”对数字基础设施的“致瘫致乱”攻击。另一方面，在云化网络部署中，为了保证业务的高可靠性，网元微服务将会进行冗余部署，这些特点为微服务拟态化构造提供了极大便利，因此不会带来过多的成本代价。

4.3 人工智能的安全应对策略及案例

要应对人工智能带来的安全挑战，需要综合多种措施。已得到各国政府的高度重视：中国已经发布了《人工智能安全白皮书》（2018 年）、《新一代人工智能伦理规范》（2021 年）、《生成式人工智能服务管理暂行办法》（2023 年）、《全球人工智能治理倡议》（2023 年 10 月 18 日）等相关指导规范；美国、欧盟和世界卫生组织等也发布了《人工智能应用监管指南》（2020 年）、《世界卫生组织卫生健康领域人工智能伦理与治理指南》（2021 年）等，以规范 AI 的开发利用行为。

这里重点讨论 AI 网络攻击的防御策略。因为 AI 网络攻击将严重威胁国家安全、公共安全和经济繁荣，并污染互联网环境。

当今的网络安全行业严重依赖传统方法（主要是人工驱动+基于攻击特征值的防火墙、WAF、IDS/IPS、UTM 等传统安全产品的方法）。随着基于大语言模型的生成式 AI 变革浪潮袭来，首当其冲的是网络安全行业正面临一次技术和方法的颠覆性革命。人工智能攻击的防御是急需研究的课题。这是全新的挑战。

1) 使用水印技术识别 AI 生成的结果

人工智能生成的虚假信息可以非常熟练地模仿我们的脸、我们的声音、我们的手势，但完全是虚假的。可以要求 AI 生成的图像都带有水印或标签，以便计算机能够检测这个系统是否是由生成式 AI 系统生成的。可以以可见或不可见的方式使用隐写术加水印技术，这可以通过图像、视频和音频的生成过程来实现。

2) 使用人工智能识别 AI 攻击

利用基于神经网络 AI 的方法去识别、防御 AI 攻击。这是很容易想到的技术路线。目前的研究情况是：在威胁检测方面，人们尝试基于机器学习的恶意代码检测，到后来尝试过用深度学习解决安全问题，到今天尝试用 AI 的大模型、用多模态这些技术来做检测。但在实战中都没有取得理想的结果。因为存在两大问题：

① 高质量的训练数据集是关键。遗憾的是：我们无法实时得到千变万化的 AI 攻击的特征值，我们只能使用过去的特征值。从原理上 AI 不可能从过去的已知攻击的旧数据里学习出明天后天出现的新未知攻击（包括 AI 攻击）的特征值。

② 机器学习的滞后性问题：训练大模型时需要事先准备大量的标记数据，然后学习本身也要大量的时间和成本。这种学习速度很难应对今天互联网上每天产生的 38 万到 72 万“前所未有的恶意软件”，以及爆发的千变万化的 AI 攻击。

如果这两个问题得不到突破的话，这条技术路线目前还看不到希望。距离到实战还有很长的路要走。目前，AI 检测机器人只对旧的已知攻击的检出有一定帮助。

3) 生物自防御技术的应用

从防御方的角度看，千变万化的 AI 网络攻击呈现出不可识别、不可拦截、不可预测、不可模拟的特性，与其它的未知攻击一样。不可能事先得到攻击特征值。更何况 AI 网络攻击已经进化到攻击特征值是动态可变的：每 24 小时自动生成新攻击代码。因此对 AI 网络攻击的防御必须摆脱对攻击特征值的依赖，必须另辟蹊径。互联网未知攻击的防御是迫切需要解决的世界性难题。是数字经济发展的拦路虎。

研究表明：“隔离+生物自防御”机制是未知攻击的克星。在自然空间里这一机制曾帮助我国在没有特效药的情况下战胜了前所未有的 SARS、新冠病毒的未知攻击。人体里有一套“生物自防御”机制或系统，至少包括：数字皮肤、免疫、自我痊愈、神经监测和排毒五道主防线。但是在网络空间的计算机里、网络里、云平台里因为缺乏这种“生物自防御”机制，所以病毒和攻击者一侵入就出事了或者丧命了。就像白血病患者一样脆弱不堪.....

生物自防御技术是研究如何把这套“隔离+生物自防御”机制复制到计算机和计算机系统里，增加抗未知攻击的能力的前沿交叉学科。

4.4 云原生的安全应对策略及案例

随着在云原生安全方向上的深入研究，人们发现安全+云原生并不是简单组合就能变成云原生安全。要想做好云原生安全，就必须按照云原生的理念去思考安全问题怎么解决，云原生安全应该是一个整体，而不是各个割裂的安全产品。



图 17 云原生和安全不是简单的组合

云原生的一个底层核心理念就是拆解、组合和标准化，这其实也是软件开发领域一个软件工程师长期追求的目标，即将业务逻辑和通用逻辑不断拆分，通用

逻辑逐渐独立标准化，开发人员只需要关注自身业务逻辑。kubernetes 从业务应用的角度将通用逻辑拆解，解决部署和运维自动化的问题。不可变基础设施作为云原生技术要素，是最容易被忽略的，但是这个理念却是云原生能够持续发展的核心，极大地降低了云原生的复杂度，将标准化发挥到极致。基于这个理念，不再需要关注业务运行过程的复杂变化，业务灵活性、可移植性都有大幅提升。基于这些云原生理念和面临的安全问题，云原生安全的发展方向应该朝着安全原生化、安全一体化发展。

● 安全原生化

安全原生化就是要从云原生的角度思考和实施安全，让安全融入云原生应用生命周期的每一个阶段：代码、测试、构建、运行、维护，每个阶段都能够有合适的安全防护措施，这些措施与云原生能够紧密结合，用户在接受这些安全防护措施保护的时候，能够无感。代码阶段能够自动进行白盒扫码、编排文件扫描、敏感信息扫描，测试阶段能够自动进行安全测试、模糊测试，构建阶段能够自动进行编排文件扫描、镜像扫描、提供安全基础镜像，运行阶段安全隔离、安全防护能够自动与应用进行结合，维护阶段安全事件能够自动化处置和响应。这样云原生应用就能够实现上线即安全，运行即安全。

● 安全一体化

安全一体化包含了两部分：安全能力原子化和安全方案一体化。传统安全产品经历了多年发展，每个产品都包含了众多安全能力，在云原生架构下，这些安全能力需要重新进行思考，在合适的位置使用。安全能力不应受到惯性的影响，需要将安全产品切分到原子化的安全能力，再寻找到合适的位置，重组成新的云原生安全。例如安全领域最基础的安全隔离，传统的边界隔离不能满足云原生应用的灵活性需求，就要将安全隔离能力分解，既要有传统大边界安全隔离也要有能动态调整的安全微隔离，通过两种方式来实现完整的云原生安全隔离。安全方案一体化就是在安全能力原子化的基础上，将各安全原子能力按照云原生架构进行组合，形成统一的安全产品方案，不再是一堆安全产品堆砌和组合。

以上云原生安全应对策略和方向，还可以细化为更加具体的执行策略和评估方式。

● 自动化安全

传统安全受限于应用架构的影响，很多场景都无法做到完全自动化，虽然近年来也提出了 SOAR 自动编排响应，但具体完全实现自动化还有很长的路要走。云原生得益于架构优势，整个生命周期都能够实现完全自动化，这也让自动化安全成为可能，因此自动化可以做云原生安全方案是否良好的一个评估标准。

● 安全能力全面覆盖

云原生贯穿整个应用生命周期，因此云原生安全应覆盖应用的整个生命周期。另一方面应用的运行路径也会被云原生架构管理，天然具备架构感知识别能力，因此安全也要覆盖到应用运行路径的整个链路，确保每个角落都能具备合适的安全能力。

● 安全智能对人友好

传统安全基于策略和告警模式，告警繁多，需要专职的人员进行告警处理，大量无效告警不仅浪费人员精力，还容易造成心理懈怠。云原生场景下，这些告警应能够进行智能化地分析，基于资源关联和告警路径，实现告警自动化处理，减少人员重复工作，自动进行响应和处理，及时有效地阻断攻击。

● 零信任思想

零信任的一个核心要素是身份，传统架构下身份无法实现自动化，要管理身份就需要人为介入，赋予对象合适的身份，或者对接各种 CMDB，在现实场景会遇到诸多问题，就导致在传统架构下零信任实施困难。在云原生架构下，所有的资源都能够通过自动化管理，因此天然就具备身份。以 kubernetes 网络安全策略为例，就能够在不关注具体 IP 地址的情况下，自动基于命名空间、名称、标签等多种手段实现网络隔离，这就为零信任的实施带来了极大便利。

构建云原生安全体系时，需要注重包括安全左移在内的全生命周期原生安全。这流程意味着在软件开发和部署过程中将安全性考虑纳入早期阶段，并嵌入全生命周期流程，保障镜像构建、存储、分发以及运行时的安全。

总之，云原生安全应从各个维度进行防护，不仅包括传统的南北向 DDoS 防护、WAF、IPS 能力，还应包括东西向的零信任微隔离，防御攻击横向渗透。

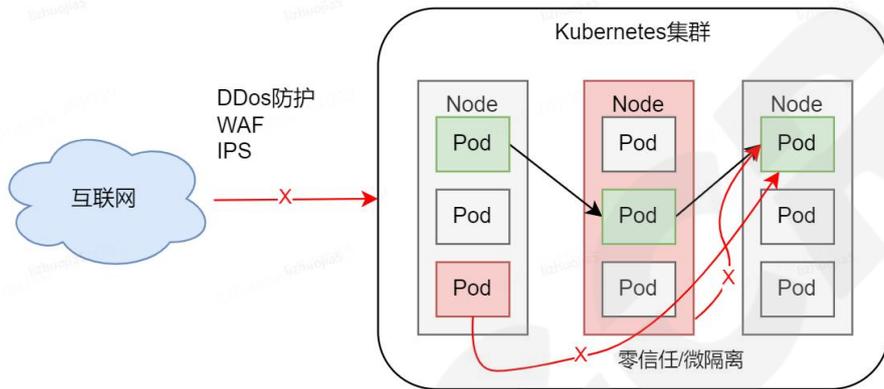


图 18 云原生安全防护方案

云原生安全发展到现在，越来越多的企业也在推出自己的云原生安全解决方案，在这个市场上，不仅有传统安全厂商、云厂商，还有众多创业型的云原生安全公司。可以看到不管是市场规模，还是未来发展都有很大提升空间。传统安全厂商有安全能力积累的优势、云厂商有基础设施和安全能力组合的架构优势，新兴创业型云原生安全公司没有历史包袱，相信这些企业能够为云原生行业带来新的安全范式。

4.5 数字孪生的安全应对策略及案例

针对数字孪生的各种威胁和脆弱性，需要采取适当的策略控制数字孪生受到攻击时的损害。除了应对传统网络攻击和新兴技术攻击所需要制定的应对策略外，还应当考虑到数字孪生的特性，例如：数字孪生允许现实世界到处理系统的循环状态更新，因此数字孪生的精确表示，即保真度，对于数字孪生安全至关重要。然而，数字孪生模型越能够准确地反映其现实世界对应目标物，攻击者就越容易

理解系统行为。针对数字孪生系统的攻击视图如下表：

攻击者工件	目标
产品生命周期	<ul style="list-style-type: none"> ● 操纵数字孪生的良性行为，将 CPS 引导到不安全的状态 ● 利用数字线索，因为它在整个产品生命周期中被用于链接数据
复制模式	<ul style="list-style-type: none"> ● 通过将数字孪生的虚拟行为复制到物理设备的相应程序状态来运行直接循环状态更新
仿真模式	<ul style="list-style-type: none"> ● 通过重新运行测试仿真来学习系统行为 ● 在安全测试期间操作仿真参数或系统规格数据
设计阶段	<ul style="list-style-type: none"> ● 利用数字孪生的基于规范或基于机器学习的流程知识
停用阶段	<ul style="list-style-type: none"> ● 由于数字孪生处置不当而导致的系统知识重用 ● 使用数据安全漏洞（如未经授权的访问）来访问存档的数字孪生数据
横向移动	<ul style="list-style-type: none"> ● 获得对高价值资产（如设计工件）的控制 ● 以随机间隔操作传感器读数或模拟参数，同时确保新值不会与实际过程值明显偏差

表 3 数字孪生系统的攻击者透视表

因此，针对数字孪生安全，我们还需要特别关注：

首先，需要制定数字孪生的安全策略，决定熟悉孪生系统在遭受攻击时是完全断开服务网络，还是降级服务进入安全状态。这需要组织制定应急计划，通过快速补救措施和小规模修复，减少事件发生的可能性及其恢复时间。

其次，数字孪生的生命周期跨越不同的阶段，在不同生命周期阶段执行各种任务涉及多个利益相关者。因此，需要制定相关的数字孪生系统访问权限的企业策略和规则，并对数据全生命周期执行加密。

第三，基于技术、拓扑和控制件生成虚拟环境中的参数可以帮助模拟现实世界对应目标的正确行为。为了避免 GIGO（垃圾输入垃圾输出）问题，确保生成数据的来源的可信度，可以使用基于底层系统网络/逻辑层设计规范的工程知识，即工程知识可以作为隐式安全规则的基础（例如：根据设备良性行为定义安全状态、根据阈值交叉验证设备数据、检测未知设备或未识别的连接）。

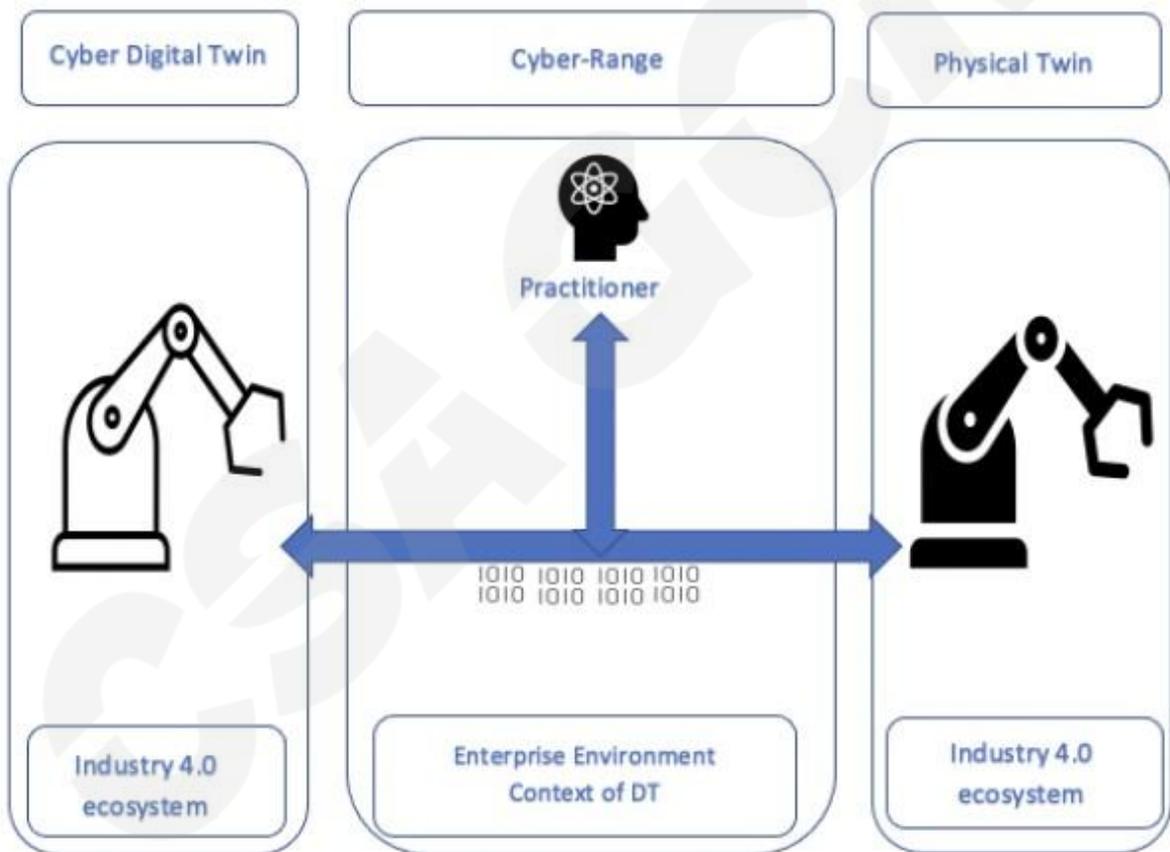


图 19 数字孪生语义建模与网络靶场

第四，采用威胁情报驱动的解决方案收集有关攻击者行为的信息。威胁狩猎可以使用此类情报（例如：IoC，即失陷指标）来识别攻击事实。在恢复的过程中，关闭受影响的设备或服务可以限制网络攻击造成的进一步损害。

最后，实施基于可信数据流解决方案对数字孪生进行审计活动，跟踪设置参数和状态数据，以及访问这些数据的实体，以检测和定位系统中的故障节点。

● 案例研究

IEEE 在第 46 届计算机、软件和应用年会发布了名为《利用数字孪生安全模拟系统网络威胁情报》的报告。这一报告把数字孪生和网络威胁情报进行了深度融合，利用数字孪生对工业控制系统 (ICS) 的攻击场景进行仿真，获得有价值的威胁信息，它的意义在于尝试把上述数字孪生的安全策略与数字孪生本身有机的结合到了一起。报告概述了从数字孪生安全模拟开始的结构化威胁情报报告的系统步骤：首先展示了行动过程并定义了框架部署的正式需求；然后，使用一个原型数字孪生应用程序进行攻击模拟，以评估所定义的框架；使用 STIX2.1 标准，通过实用工具来指导流程步骤帮助生成 CTI（网络威胁情报）。实验结果表明，该数字孪生系统可以系统地构建 STIX2.1 CTI 报告，并有可能根据现存的用例进行定制；将数字孪生安全模拟添加到 CTI 源列表中可帮助组织改善其安全状况。

4.6 隐私保护的安全应对策略及案例

当今大数据时代，个人信息的泄露已成为一种十分普遍的现象，尤其是在信息技术日新月异的今天，黑客攻击、网络钓鱼等安全威胁层出不穷。因此，如何进行个人信息保护，保障存储个人信息的系统安全已成为一个紧迫的问题。安全方法论也正逐步从“针对威胁的安全防御”向“面向业务的安全治理”等演进。企业安全能力框架 (IPDRR) 是美国国家标准与技术研究所的网络安全框架（简称 NISTCSF）。它包括风险识别 (Identify)、安全防御 (Protect)、安全检测 (Detect)、安全响应 (Response) 和安全恢复 (Recovery) 五大能力，从以防护为核心的模型，转向以检测和业务连续性管理的模型，变被动为主动，最终达成自适应的安全能力。



图 20 网络安全框架 CSF

具体来说 IPDRR 主要包含了五个部分：

识别（Identify）识别网络资产及风险，是指对系统、资产、数据和网络所面临的安全风险的认识及确认

保护（Protect）保护网络，是指制定和实施合适的安全措施，确保能够提供关键基础设施服务。

检测（Detect）发现攻击。在攻击产生时即时监测，同时监控业务和保护措施是否正常运行，制定和实施恰当的行动以发现网络安全事件

响应（Respond）：响应和处理事件，指对已经发现的网络安全事件采取合适的行动。具体程序依据事件的影响程度来进行抉择，主要包括：事件调查、评估损害、收集证据、报告事件和恢复系统

恢复（Recover）：恢复系统和修复漏洞。将系统恢复至正常状态，同时找到事件的根本原因，并进行预防和修复。

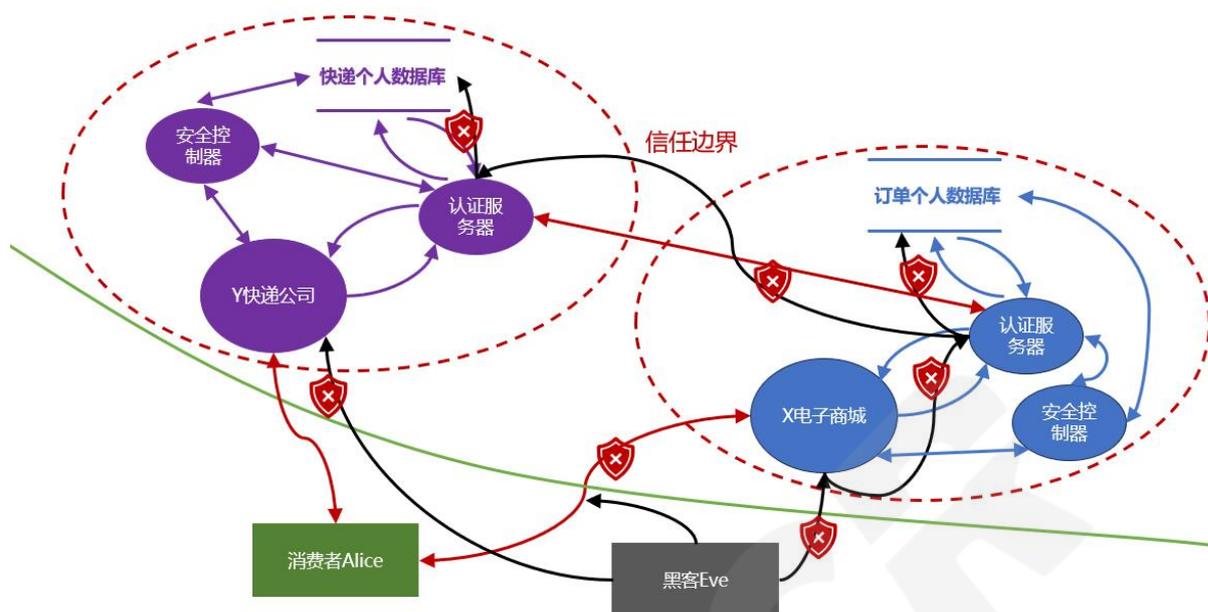


图 21 IPDRR 示例

以电子商城 X 企业为例，X 企业可以通过在内部落地 IPDRR。首先要识别企业的网络安全资产如重要信息系统、服务器等，确保漏洞，基线配置满足合规要求。然后需要做好基本的安全防护，比如在域间设置防火墙、主机装 EDR、开启基于零信任的认证访问控制器、部署入侵检测设备等。其次，还要部署安全控制器将这些基础防护设备的告警接入做到安全告警的检测分析做到运营态安全。比如发现漏洞要进行补洞加固等、发现攻击封堵 IP 等。最后是恢复，对已经造成的攻击破坏进行恢复至正常运行状态，安全控制器对于被失陷的主机进行隔离杀毒或重装系统等。

4.7 Web4.0 的安全应对策略及案例

使用虚拟现实或增强现实技术是提升交互感的最直接的方式。使用虚拟现实技术用于模拟场景可以进行相关行业的培训。在医疗方面，在传统的外科手术培训中，由于解剖的材料稀缺，通常由多个人甚至几十人共用一个解剖材料进行训练练习，导致教学质量大受影响。而在虚拟世界中，可以提供仿真的 3D 模型，其便携性、易用性以及随时可操作练习为传统的外科手术培训提供了新的可能。

同时，使用物联网与高速网络可以让外科医生能够远程操控医疗器械进行手术。而在轻度的精神疾病中，对于传统的治疗方案，都是医生与病人进行言语交流，引导患者疏导心理压力。但多数的精神疾病患者都是独处且抗拒与他人接触，通过虚拟现实技术可以帮助患者在虚拟世界的互动改善心理状况，可以塑造各种情景，让患者更快地进入情境，医生更快地掌握病情，更好更快地对症治疗。

在以上所讲的三种在医疗的使用场景中，最重要的便是对生物特征与个人信息的保护。市面现有的可穿戴设备大多为安卓系统，还有还未上市的使用苹果自有系统的可穿戴设备，攻击者可以通过攻击操作系统的方式窃取相关信息，或传递虚假内容。为了反制这种攻击，可以重新研发专为该种设备运行的操作系统，并进行严格安全测试。

4.8 卫星通讯的安全应对策略及案例

由于卫星链路的开放性、移动性和低功耗等特征，与移动网络的攻防态势存在着较大的差异，但也存在着诸多相通的技术，可以使用和借鉴。对基于移动通信的卫星通讯网络安全性进行分层考虑，重点对认证、可用性、数据通信安全、切片隔离几个安全属性进行分析和考量，以防范身份假冒、中间人攻击、DDoS攻击、数据泄露等安全威胁。

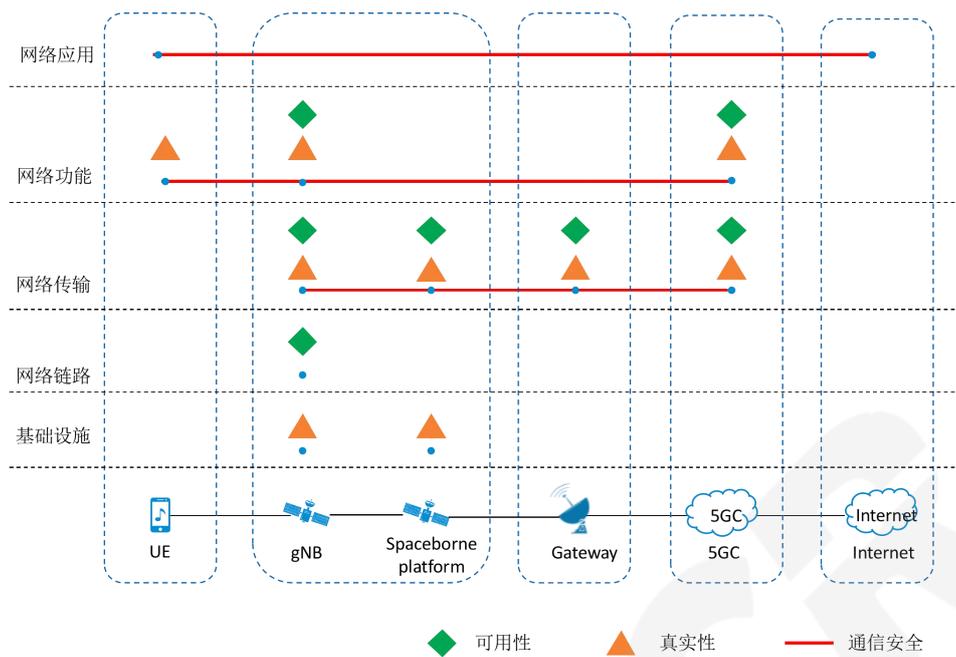


图 22 卫星通讯安全机制

(1) 设备间认证

设备间认证提供了终端接入认证、网络节点间认证和卫星节点可信启动等多层次、全方位的身份可信保障机制。基于统一认证架构对终端和服务网络实现双向认证，保护用户和网络之间的相互可信。同时采用二次认证或切片认证机制，防止未授权用户访问业务或者切片。借助 IKE 协议，在通信对端节点之间进行身份信息交互，验证对端节点身份的合法性，实现网络功能节点间的互信认证。此外，为保障卫星节点的可信可靠，可结合可信计算技术，每个卫星节点从系统启动开始防护，对可信启动链条中的每个实体逐级进行完整性验证，与其他可信节点共同形成一个可信的网络。同时利用可信根保存验证结果，避免外部软件对验证数据的恶意篡改。

(2) 数据通信安全

考虑到卫星通讯网络的复杂性，可以对网络进行分段防护，包括空口安全、星间链路安全、回传网络安全和应用层安全，保障控制面和数据面完整性和机密性。为保证空口通信安全，用户终端与基站之间的 RRC 和 NAS 信令需要进行完整

性保护，信令机密性、数据机密性和完整性根据网络需要选择性开启，可有效阻止伪基站引发的数据劫持攻击。对于承载网络，星间链路的机密性和完整性保护可参考现有安全机制，如 SCPS-SP、IPSec 等安全协议。卫星网络与无线核心网之间的回传网可以考虑 LAN-to-LAN IPSec 技术。此外，还需考虑应用层通信安全。终端与服务方之间往往采用 TLS 和 IPSec 协议，以便从端到端保护应用层数据的机密性和完整性。

（3）可用性与可靠性

考虑采用轻量级的攻击检测技术（如 SOM 自组织图、SVM-SOM 等），或者结合 LSTM 深度学习模型、SVM 等在空间网络中进行 DDoS 检测。通过加强终端接入认证与验证、基于终端的业务身份向终端授权业务访问、由卫星节点对数据业务提供会话轻量化验证等机制，及时识别异常流量，实现近源端的业务合法性主动防御。控制面的 DDoS 攻击可以采用禁止 ICMP 报文、禁止广播报文、增加 ACL 过滤、增加黑白名单、单包授权等机制实施防护。

移动网络 NR 竞争接入通常采用限速方式，避免竞争接入产生的信令风暴。同时还可以对用户接入的响应消息进行加扰，使得攻击者无法正确解码，避免用户终端随机接入攻击的发生。

在频段压制方面，对无线信道进行动态信道分配、增加频段保护带、提高滤波精度、移频等技术，可以一定程度上应对频段压制。

（4）切片隔离

网络切片端到端安全隔离机制包括 RAN 切片安全隔离、承载切片安全隔离以及核心网切片的安全隔离。根据不同应用场景需求，利用资源池预留和分配实现卫星接入网子切片的定制化，实现无线资源的隔离。承载网隔离机制通过将一个物理端口划分为多个逻辑端口实现切片，支持任意子速率分片和隔离，业务约束在某切片中承载。对于核心网，可以采用物理隔离的方案，为安全性要求较高的切片分配相对独立的物理资源，也可以采用逻辑隔离方案，借助成熟的虚拟化技

术，在网络层通过划分 VLAN/VXLAN 子网进行隔离，在管理层通过分权分域实现切片管理和编排的隔离。

4.9 算力网络的安全应对策略及案例

与传统网络安全一样，为保护算力网络端到端的安全，需要采用以下增强安全机制：

- **数据加密和身份验证：**算力网络中的数据加密是保护敏感信息的重要措施。通过使用加密算法，可以将数据转化为无法被解读的密文，以防止黑客窃取。同时，要对访问算力网络的用户进行身份验证，确保只有授权用户才能访问和处理数据。
- **安全漏洞和漏洞修复：**算力网络中存在的安全漏洞可能会被黑客利用来进行攻击。因此，及时发现和修复这些漏洞是非常重要的。网络管理员应定期进行系统和应用程序的安全扫描，并及时更新补丁，以保持网络的安全性。
- **强化访问控制和权限管理：**为了防止未经授权的访问和潜在的数据泄露，算力网络应实施严格的访问控制和权限管理机制。只有经过授权的用户才能访问特定的数据和功能，并且需要严格的身份验证和授权流程。
- **实施网络监测和入侵检测系统：**算力网络应配备网络监测和入侵检测系统，可以实时监控网络流量和检测潜在的入侵行为。这些系统可以及时发现异常活动，并采取措施阻止入侵，保护网络的安全性。
- **建立灾备和恢复机制：**算力网络的安全性还需要考虑到灾备和恢复机制。在发生安全事件或故障时，需要有备份数据和灾备计划，以确保数据的可靠性和业务的连续性。

在算力网络体系中，通过将网络、算力、安全能力融合协同，以安全内生和弹性资源供给的方式构建安全体系，对算网中的威胁进行实时定位、智能研判、协同联动，打造全程可信的确定性安全算力网络。

一方面，基于算力网络安全需求识别，将终端、服务、网元身份和位置进行数字化统一表达，充分考虑算力业务特点及其安全防护需求，在算网设计顶层进行具有内生安全特性的 NISC

(Network with Intrinsic Security Communication) 可信通信技术体系构建。面向算网系统的 NISC 可信通信技术应考虑身份可信接入和服务合法访问的应对策略，为未来算力网络提供实时、高效、可信的攻击主动防御能力。

● 身份可信接入

传统 IP 网络缺乏基本的安全性设计，仿冒源地址引发的算力攻击层出不穷，而现有的可信通信技术验证开销大、保护机制考虑不够周全，难以满足拥有多样化应用、海量终端的泛在网络安全需求，因而需要考虑如何系统性构建高效的真实源验证安全机制。通过可信身份的纵向信任传递框架、关键信息的轻量化验证方案的设计，算力业务源 IP 的真实性控制机制提供基于用户可信身份的认证增强、用户资源的可信分配授权、面向用户身份的接入网验证技术，避免地址假冒引发的网络攻击、信息非法获取等异常操作，实现用户接入算力网络时的轻量化实时验证、精细化管控和网络安全可信传输。

● 服务合法访问

充分保证访问算力业务的源地址可信的同时，目标业务可合法访问也应得以关注。端到端通信业务如何确保业务获取目的端访问授权、如何高效识别数据报文的合法与否均值得深入研究。面向算力业务的网络层防御通过全方位构建目标域鉴权授权和业务随路精细化控制机制，及时阻止无合法访问权限的真实地址用户非法访问业务行为。利用验证信息的统一化生成、一致性表达、动态更新管理以及轻量化抗重放机制，为算力业务访问提供高效的合法性验证依据，增强网络主动抵御攻击的能力。在网络层面实现近源、中间传输节点以及近目的的多点攻

击防范，完善整套面向未来算网系统的攻击主动防范和溯源灵活阻断技术方案，达成流量实时高效检测控制的安全防护系统。

另一方面，也需要构建端、边、云、网整体安全体系，围绕数据全生命周期进行安全保障，确保算力资源安全接入、调度与交易，各类组件正确配置，组件之间的接口正确安全调用。



图 23 算力网络安全防护框架

为了更好的支撑算力网络中的各类应用场景，如智慧城市、智慧制造、车联网、工业互联网等方向的整体防护需求，算力网络安全防护框架在设计上建议分为三层架构，安全组件层、安全平台层、安全运营层。

安全组件层为整体防护体系提供必要的安全组件能力支撑，覆盖云、网、边、端、属、用和密码共计七类主要能力，是整个体系的基石。安全平台层通过对安全数据湖收集到的海量数据进行综合智能分析评判，与基础安全知识库一起形成各行业的专有模型库，在这层的分析引起可以包括 AI 引擎、UEBA 引擎、分布式关联分析引擎知识图谱引擎、统计分析引擎等。安全运营层通过综合运营流程、工具平台及人力专家快速实现自动化的安全运营服务，包括但不限于以下一些能力：安全态势、溯源分析、自动化响应、威胁情报、攻击面管理、资产测绘以及异常应急处置等。

4.10 物联网技术的安全应对策略及案例

随着物联网技术的快速发展，其在各个领域的应用越来越广泛，但同时也带来了更多的安全挑战。智能家居中的摄像头、智能门锁等设备很容易被黑客攻击，导致隐私泄露等问题。因此，在智能家居中需要加强设备的安全认证和授权管理，确保只有经过授权的设备才能访问和使用网络资源。同时，还需要加强数据的安全保护，对数据进行加密和完整性保护，确保数据传输的保密性和完整性，及时发现和处置安全事件。智能家居的物联网安全是一个非常重要的问题，因为它涉及家庭数据和个人隐私的保护。另外智能交通是物联网技术保障交通系统正常运行和防止黑客入侵的重要领域。例如，智能交通中的交通信号灯、车辆监控等设备很容易被黑客攻击，导致交通混乱等问题。

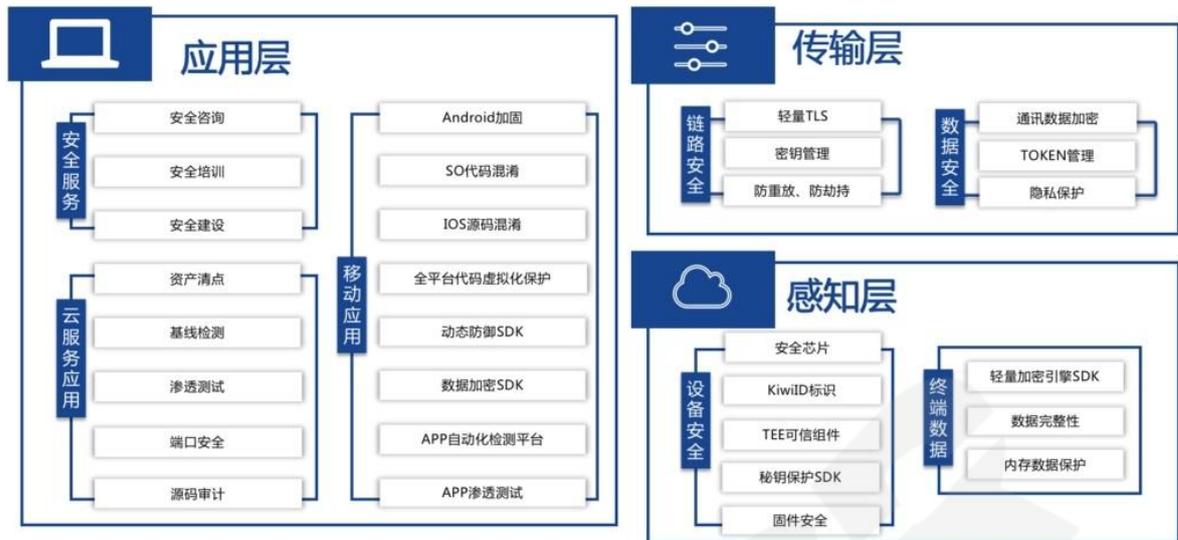


图 24 三大层面

1. 建立健全物联网安全体系

作为保障物联网技术应用安全的重要举措。这个体系应该包括物理层、数据链路层、网络层和应用层等多个层次，以确保各层之间的安全性和协调性。其中，物理层的安全性需要关注设备的硬件和软件配置，确保设备不被非法访问和攻击；数据链路层的安全性需要关注数据的加密和完整性保护，以确保数据传输的保密性和完整性，网络层的安全性需要关注网络协议的安全性，以确保网络通信的安全；应用层的安全性需要关注应用系统的安全性，以确保应用程序不被非法入侵和攻击。

例如在智能车辆的防盗方面，就需要一个健全的安全管理系统，包括但不限于使用远程定位及追踪技术，通过全球卫星导航系统（如 GPS）将车辆位置信息传输到用户手机或指挥中心，帮助寻找被盗车辆，车辆身份认证技术可以防止非法复制车钥匙启动车辆。另外像在智能停车场方面可以利用物联网感应设备、视频监控系统等技术，实时监测停车场内车辆数量和停放状态。同时，加密车牌识别技术可以确保与用户账号或支付信息的匹配，减少非法访问风险。此外，建立安全的停车场网络结构，采用防火墙和入侵检测系统等技术来预防黑客攻击。

2. 加强物联网设备的认证和授权管理

这是保障物联网技术应用安全的必要手段。这个过程需要建立一套认证机制，对设备进行身份验证和授权管理，以确保只有经过授权的设备才能访问和使用网络资源。同时，还需要建立一套授权机制，对设备进行权限管理，以确保只有经过授权的设备才能访问和使用网络资源。

例如在智能音箱的安全方面，语音助手就可能让黑客远程控制智能音箱，因此建议禁用语音助手。确保智能音箱使用强密码，并要求用户进行身份验证，例如使用双因素身份验证，以避免未经授权的访问。使用安全的通信协议，如 TLS（传输层安全性）来加密与其他设备和云服务器之间的通信。敏感数据也应在存储和传输过程中进行加密。

3. 加强物联网数据的安全保护

对数据进行加密和完整性保护，以确保数据传输的保密性和完整性。同时，还需要建立一套数据备份机制，对数据进行备份和恢复，以确保数据不会丢失或损坏。

例如智能路由器安全，需要使用最新的固件更新，确保路由器是最新版本。另外，不要轻易将路由器密码分享给其他人，避免使用简单的密码，例如“123456”或“password”。可以考虑使用 WPA2、WPA3 或更加安全的加密协议来保护网络连接和数据传输过程中的安全。同时也很有必要向设备用户和开发人员提供相关的安全教育，提高他们对物联网安全问题的认识和理解，包括如何保护物联网设备、如何防止黑客攻击等。

4. 加强物联网的安全监控和管理

对网络进行实时监控和分析，及时发现和处置安全事件。同时，还需要建立一套安全管理机制，对安全事件进行分类和处理，以确保网络安全不受威胁。

例如交通信号灯控制系统可以采用加密技术，加强对终端的监控和管理，确保信号灯指令的安全传输，防止黑客篡改信号灯状态。智能交通监控系统使用视频分析算法，检测异常交通行为和事件，例如交通拥堵和事故。这些技术可以及

时提供数据和信息给相关部门，以支持交通管理和决策。还有在智能票务系统方面可采用加密技术，确保支付信息的安全，以防止黑客攻击目标乘客的个人数据。同时，在实现智能公共交通服务时，需要建立健全的用户身份验证机制和数据保护措施，以防止个人隐私泄露和非法使用。

5. 安全固件更新和漏洞修复

关注设备供应商或安全研究机构发布的安全漏洞公告，了解固件中存在的漏洞以及相应的修复方案。及时发布并推动设备厂商提供安全补丁和固件升级，以修复已知的漏洞，并持续关注新的安全威胁。

例如摄像头安全，确保摄像头具有最新的固件更新，并且使用有效的加密协议（如 AES）来保护视频流。此外，可以考虑采取额外的安全措施，如将摄像头设置在云端存储，而不是将视频流直接传输到互联网，访问视频流需要账号密码的身份验证。还有智能门锁的安全，需要使用最新的智能门锁固件更新，并确保门锁使用了有效的加密协议来保护数据传输。此外，可以考虑采取额外的安全措施，如双重认证或生物识别技术（如指纹或面部识别）来增加门锁的安全性。

物联网安全需要用户和制造商共同努力来提高安全性。用户应该保持警惕，及时更新设备固件和应用程序，并使用最新的安全补丁和加密协议来保护自己的网络连接。制造商也应该加强产品的安全性，并为用户提供更强大的安全功能和更好的保护措施。还需要相关部门和企业加强协作，定期进行系统漏洞评估和更新，提高整体的安全性，并制定相应的法规和标准来规范物联网安全的建设和运营。

5 总结

随着科技的快速发展，数字化已经成为现代社会的标志，各行各业都在逐步实现数字化转型。行业数字化不仅改变了人们的生活方式，也深刻影响了企业的运营模式和行业的发展趋势。《2024 年十大数字技术趋势与其安全挑战》报告

深入研究了 2024 年引领变革的数字技术发展趋势，其中包括量子计算、6G 通信技术、人工智能、云原生、数字孪生、隐私保护、Web4.0、卫星通讯、算力网络和物联网技术。

报告详细分析了这十大数字技术的未来应用和 2024 年预测，同时识别了与之相关的安全挑战，并提供了策略性的安全应对建议。本报告旨在帮助企业管理者深入了解数字技术的发展趋势，以便制定具有前瞻性的战略规划 and 政策。研究结果将为决策者提供有关数字技术发展安全风险的关键信息，保障技术创新的安全性，引导投资和资源配置，并帮助企业更好地应对数字时代的挑战。此外，项目还将为企业提供有关数字技术发展的深入见解，帮助他们了解最新的技术趋势和发展动向，以优化企业运营和提高竞争力。总之，本项报告将为决策者提供宝贵的数字技术安全洞察和指导，帮助制定有效的数字发展战略，推动企业数字技术的健康和可持续发展。同时确保技术与安全并行，这对于探索全球数字经济繁荣的安全保障具有重要意义。

Cloud Security Alliance Greater China Region



扫码获取更多报告