人工智能安全技术不包括什么

人工智能安全技术涉及多个领域，包括但不限于：

1.AI模型安全：涉及模型窃取或者模型污染等安全问题。

2.AI数据安全：包括数据丢失或者变形、噪声数据干扰人工智能研判结果等问题。

3.AI系统安全：涉及系统稳定性、隐私保护、反制技术等问题。

4.AI算法安全：包括算法的正确性难以保证、对抗样本等问题。

以上内容只是部分人工智能安全技术，还有很多其他技术也同样重要，需要根据不同的应用场景和需求进行研究和应用。

人工智能安全是指什么

ETSI发布了有关AI安全的报告。ETSISAI主席AlexLeadbeater在记者采访中指出，该报告描述了基于机器学习的基于AI的系统和解决方案的安全保护问题，以及在AI生命周期的每个阶段与机密性，完整性和可用性相关的挑战。人工智能面临许多挑战，包括偏见，道德规范和在规则内部署的能力，许多应用对于自动化网络的安全性而言已变得至关重要。

人工智能

人工智能（AI）在社会的数字化转型中起着关键作用。很难想象，没有一个在各种商品和服务上都没有人工智能的世界，在工作，金融，医疗保健，安全和农业领域已经发生了许多变化。人工智能对于欧洲的绿色交易和疫情后的经济复苏至关重要。

作为一门科学学科，人工智能包括多种方法和技术，例如机器学习，机器推理和机器人技术。因此，涵盖人工智能，机器人技术和相关技术的道德方面的法规是关键目标。

欧洲议会也对此发出了声音，欧洲议会已经宣布，在2021年的头几个月中，将以规制的形式对算法进行规范。它成立了一个特别的临时议会委员会（AIDA），以分析AI对欧盟经济的影响。

ETSI文件

ETSI将人工智能定义为系统处理显式和隐式表示的能力，以及执行由人类执行的被认为是智能的任务的程序。在机器学习和深度学习技术的发展以及数据分析技术的广泛应用的推动下，一系列技术正在继续朝着完全适用性的方向发展。

“AI显而易见的一件事是，大多数历史安全模型都不太适合。因此，AI本质上是高度并行，高度分布式的。它既是威胁自身，也威胁其他AI。” Leadbeater说。

人工智能可以促进新一代产品和服务的开发，包括在欧洲公司已经占据优势地位的行业中，例如循环经济，农业，医疗保健，时尚和旅游业。实际上，它可以提供更平滑，更优化的销售路径，改善机械维护，提高产量和质量，改善客户服务并节省能源。

人工智能已成为社会变革的最强大动力之一：它正在改变经济，影响政治并重塑公民的生活和互动。与人工智能相关的许多具体的道德和法律问题已经出现在各个领域，例如责任，保险，数据保护，安全，合同和犯罪。数据保护在AI与法律之间的关系中起着重要作用，因为许多AI应用程序涉及对个人数据的大量处理，包括基于该数据对人进行针对性和个性化处理。

基于人工智能的系统正在以多种形式淡化人类和社会世界：工厂中的工业机器人，家庭和医疗设施中的服务机器人，交通中的自动驾驶汽车和无人飞机，电子商务和金融中的自动电子代理，将军事和智能通信设备集成到每个环境中。

当然，并非所有算法都涉及AI，但是每个AI系统（如每个计算机系统）都包含算法，其中一些算法处理直接影响AI功能的任务。尽管AI系统包含许多算法，但也可以将其视为单个复杂算法，将执行其各种功能的算法与通过触发相关的较低级算法来协调系统功能的高级算法结合起来。

人工智能，区块链和大数据技术在全球数据处理基础架构中的相互作用可以带来许多好处：改善信息访问；全球知识的产生和传播；节省成本，提高生产率和创造价值；以及新的高薪创意工作。

人工智能的安全特点

大家好，今天跟大家分享一下人工智能的安全风险有哪些特征。

人工智能可以看作人类智慧的延伸，它是一种以人类内在需求为导向的科学技术。

人脸识别、刷脸支付、语音助手、自动驾驶等人工智能应用给我们的生活带来了更多的便利，人们的生活方式、思维方式、发展理念乃至社会制度都有着不同程度的

变化。

因此，这种共生形式会从技术本身以及技术对于社会上层建筑的影响两个方面形成安全风险。

人工智能在建筑安全管理的应用

人工智能建筑应用:通过生成设计改进设计，建筑信息建模是一个基于3D模型的过程，为建筑、工程和建筑专业人员提供有效的规划、设计、建造和管理建筑和基础设施的洞察力。

为了规划和设计建筑，3D模型需要考虑建筑、工程、机械、电气和管道(MEP)计划和每个团队的活动顺序。挑战在于确保子团队的不同模型不会相互冲突。

人工智能安全的解决方案

建立安全活动基线以检测异常情况

物联网的顶级安全人工智能解决方案之一是异常检测，它不仅仅基于规则和威胁签名。即使事先不了解此类威胁，人工智能也可以通过研究行为来检测潜在威胁。使用人工智能的高级安全解决方案，可以扫描网络活动和设备行为，以建立常规或安全活动的基线。有了这个安全活动和行为的基准，就可以更容易地发现恶意活动并做出相应的响应。

人工智能收集有关设备行为、环境条件、网络流量以及其他可被视为威胁或攻击的相关方面的数据。然后，通过异常检测算法处理数据，以查找恶意行为或攻击迹象，例如异常数据移动、对更多权限的请求增加或升级的特权，以及尝试访问功能不需要的数据。

一两个异常行为实例可能不是真正的威胁，因此检测模式或特征非常重要。如果这些良性实例被视为威胁，结果可能是过多的误报，这可能会对事件响应产生负面影响。由于涉及的设备数量众多，在监督物联网安全时，对误报或不准确的安全警报的警惕尤为重要。

手动设置安全活动基线是不切实际的，在某些情况下实际上是不可能的。人类安全分析师不太可能充分涵盖企业网络中的所有活动，特别是当涉及的物联网设备数量不断增加时。创建区分安全活动与有害或恶意活动的相应规则或参数将极其困难。人工智能辅助异常检测可以说是唯一可行的选择。