## 当前人工智能存在哪些安全风险？如何应对？

1. 在数据爆发的年代，90%的数据是近两年内生成的，据估计2020年，全球平均每秒种产生1.7MB的数据
2. 对抗性机器学习（Adversarial Machine Learning）

随着AI 技术的发展，

1. 模型缺陷与后门（Model Defects and Malicious Models）

近年来，各种结构复杂的二进制代码安全缺陷日益繁多。例如，后门、竞争条件及鉴权绕过等逻辑错误类型的代码安全缺陷。它们不仅存在于二进制单线程程序，而且分布于各种二进制并行程序。而符号执行、污点分析及模糊测试等现有方法难以发现结构复杂的代码安全缺陷，也不能有效地应用于二进制并行程序，使软件系统面临安全性风险

1. 数据污染攻击（Data Processing Vulnerabilities）

内存数据被污染往往是程序漏洞被利用的本质所在，从功能角度把内存数据划分为控制相关和非控制相关，由此引出控制流劫持攻击和非控制数据攻击。两者危害程度相当，前者因利用成本较低而成为主流，但随着控制流劫持防御方法的不断完善，非控制数据攻击逐渐被重视。研究者先后在顶级会议上提出了数据导向攻击得自动化利用框架Data-oriented Exploits （DOE）以及图灵完备性地证明Data-oriented Programming （DOP），使得非控制数据攻击成为热点。

1. 模型数据的推测窃取（Model Inference Attack）
2. 安全隐私问题

在人工智能的保护伞下，诸如机器学习和大数据等问题，都很容易触及到安全及隐私问题。有时基础设施扮演着很重要的角色。与隐私问题有关的安全需求，如将银行帐户和健康信息保密，将会对研究的安全性有更大的要求。2018年，有关安全和隐私的问题将得到解决，这一年，也是人工智能可能出现新的发展的一年。

人工智能的伦理问题也将成为2018年的主要问题，需要解决的伦理和道德问题包括人工智能对人类有哪些好处和坏处。人们也对机器人取代人类的可能性感到担忧，比如护士、治疗师或警察，另一个需要处理的问题是自主武器。

## 人工智能技术在网络安全中的应用场景有哪些？（举例企业的具体产品、技术或实践）

## 如何看待网络安全中人工智能的未来发展趋势？

1. **生成式对抗性网络**

生成式对抗网络GAN（Generative adversarial networks）目前已经成为人工智能学界一个热门的研究方向.GAN的基本思想源自博弈论的二人零和博弈，由一个生成器和一个判别器构成，通过对抗学习的方式来训练.目的是估测数据样本的潜在分布并生成新的数据样本.在图像和视觉计算、语音和语言处理、信息安全、棋类比赛等领域，GAN正在被广泛研究，具有巨大的应用前景。

无论是无监督学习、半监督学习，GAN给我们提供了一个处理问题的崭新思路，就是把博弈论引入到机器学习过程中来。可以预见，GAN本身的算法以及看问题的角度，必将对未来设计算法、以及解决实际问题产生深远的影响。

1. **数据众包**

所有的人工智能公司都追求巨大的数据库，以实现他们对人工智能的雄心壮志。这些公司将开始通过众包方式获取大量数据。企业已经找到了一种方法来评估众包数据的质量和真实性，不仅给企业提供了便利，还能反馈信息给消费者。

目前，谷歌通过众包的方式，获得了大量的图片，并构建了成像算法。该公司还利用众包来帮助改善服务，比如翻译、转录、手写识别和地图应用。而亚马逊还利用众包的技术改善了Alexa的1.5万项现有技能。

1. **所有神经网络的独特格式**

**许多不同的框架在做同样的事情，如今，每一家从事机器学习的大公司都拥有自己的框架和其他开源解决方案。在单独的AI应用中，我们希望使用不同的框架，例如计算机视觉的Cafle2, NLP的PyTorch和一些推荐系统的Tensorkow/Keras。合并它们需要大量的开发时间，它分散了数据科学家和软件开发人员从事更重要任务的注意力。解决方案必须是一种独特的神经网络格式，可以很容易的从任何框架中获得，然后开发人员能够轻松地部署，科学家可以轻松地使用，在这里我们遇到了ONNX标准：**

1. **AutoML更换管道**

**设计一个神经网络框架是一个非常痛苦的任务——虽然有时通过叠加卷积层能获得相当好的结果，但是大多数时候需要非常小心的使用直觉和超参数搜索方法设计宽度、深度和超参数，如随机搜索或者贝叶斯优化。特别是当你不在计算机视觉研究时，这意味着没法在ImageNet上完成一些DenseNet模型的训练，但是可以使用一些3D数据分类或多变量时间序列应用。**

1. **Zoos大爆发**

**深度学习中在计算机视觉任务和自然语言处理任务中将预训练的模型作为新模型的起点是一种常用的方法，通常这些预训练的模型在开发神经网络的时候已经消耗了巨大的时间资源和计算资源，迁移学习可以将已习得的强大技能迁移到相关的的问题上。**

**很多人开始用Cafle Zoo的模型进行迁移学习或特性提取，最近发现它就像大型计算机视觉管道的一部分一样。这意味着实际上没有必要训练自己的网络，例如，对于ImageNet对象的识别或局部识别，这些基本的东西可以下载并插入到您的系统中。使模型能够更快的训练使用到对应的场景中**

1. **加速转向对话式交互**

对于许多人工智能领域研究者来说，语义学习是他们的下一个主要目标。随着技术的进步，图像识别和语音识别都取得了重大突破，而这将有利于计算机更加高效地理解和生成语言，人工智能时代，服务的入口主要是自然语言的语音交互，自然语言处理会是人机交互的主要模式，谁能让机器更懂人类的语言，谁就能有可能取胜。人工智能会全面包围我们生活的方方面面，这意味着，人工智能入口的竞争会更加惨烈，而越早参与，获得越多的用户，胜利的几率就越大。

1. **在智能芯片方面，GPU将进一步得到更广泛的应用**

GPU，也就是我们所说的图形处理器，一直都是AI应用的主导硬件处理器，在图像语音识别、无人驾驶等人工智能领域，GPU正迅速扩大市场占比。

尽管有不少IT巨头和创新企业在尝试定制新的硬件架构，力图在性能、成本和功耗上与GPU竞争，但是由于英伟达公司投入巨资成功建立了产业生态，可以肯定的是，GPU仍然会在相当长的一段时间内得到更广泛的应用。很多人都认为GPU的主导地位会被非GPU方案终结，例如FPGA或ASIC，但是非GPU方案都将面对两个艰巨的挑战：第一，能否实现量产，第二，整个产业生态链是否完整。目前，能够实现大规模商用、取代GPU地位的硬件尚未出现。

1. **智能堆栈**

“AI堆栈”更深层次，在每一个层面都有自己的发展和研究，而不只是由机器学习算法和你最喜欢的框架构成。

阿里云云栖社区认为人工智能开发行业已经足够成熟，它需要有更多不同的专家。在团队中只有一名数据科学家是远远不够的——你需要不同的人来进行硬件优化、神经网络研究、人工智能编译器、解决方案优化、生产实现。以上人员必须是不同的团队领导，软件架构师（必须分别为每个问题设计上面的堆栈）和管理者。我曾经提到过这个概念，它提供了一些愿景，在未来人工智能领域的技术专家能够成长成什么样子(对于那些想成为人工智能或技术领域的软件架构师的人来说，你需要知道该研究什么)。

**CB Insights | 2017年人工智能十大趋势**

**1.人工智能聊天机器人**

**2.应用开发**

**6.人工智能硬件**

**7.人工智能创业**

**8.人工智能劳动力影响**

**预测一：加速转向****对话式交互**

**预测二： 设计将开始发展，以增加我们对AI的信任**

**预测三：我们将开始谈论AI系统之间的沟通方式**

**预测四：人工智能将会遭到固有偏见的冲击**

**预测五：企业开始关注人工智能的投资回报率**

**更好的对话能力**

**认知型机器**

**八个巨头的动作**

**1.Facebook致力于打造世界上最好的AI实验室**

**2.谷歌(微博)掀起并购狂潮**

**3.苹果瞄准数字标牌应用**

**4.Salesforce软件集成AI能力**

**5.Uber收购AI初创企业**

**6.Microsoft Ventures帮助资助AI初创企业**

**7.IBM投资Watson Improvements**

**8.英特尔打造新AI平台**

王煜全对2017年人工智能发展趋势的看法

https://m.igetget.com/share/audio/aid/7bkFVs4psggbPCDWR8rG?from=groupmessage&isappinstalled=1

* 全体IT巨头将重兵布局AI云服务
* 新老人工智能企业将围绕智能入口展开白热化的争夺，服务的入口主要是自然语言的语音交互，自然语言处理会是人机交互的主要模式，谁能让机器更懂人类的语言，谁就能有可能取胜
* 人工智能将占领客厅，语音交互将成为主流电视应用
* 智能玩具将成为AI最早成功的应用领域之一
* 商用机器人将在特定的商业场景中发挥巨大潜力
* 辅助驾驶会成为AI的第一个大规模应用
* 人工智能应用会在各个应用领域迅速普及，有大数据支持的应用创业公司会迎来最好的机遇。
* 在智能芯片方面，GPU将进一步得到更广泛的应用

人工智能网的八大趋势：http://ai.ofweek.com/news/2017-11/ART-201721-8420-30177937.html

**趋势一：科技巨头引领潮流并先行获利**

**趋势二：算法与技术整合**

**趋势三：数据众包**

**趋势四：更多的并购将发生**

**趋势五：开放民主化的工具将获得市场份额**

**趋势六：人机交互将得到改善**

**趋势七：人工智能将渐渐地对所有垂直领域产生影响**

**趋势七：人工智能将渐渐地对所有垂直领域产生影响**

**趋势八：安全、隐私及伦理道德问题**

**机器人时代：https://www.roboticschina.com/news/20160902AI.html**

\_\_1.RT时代的爆发\_\_

\_\_2.新的硬件系统诞生\_\_

\_\_3.新的计算机语言诞生——三进制\_\_

\_\_4.新的算法普及，提升计算能力\_\_

\_\_5.人类认知科技取得突破\_\_

\_\_6.人机交互不再有障碍\_\_

\_\_7.专家系统普及到各种行业\_\_

\_\_8.[机器学习](https://www.roboticschina.com/news/201701250950.html)取得突破\_\_

\_\_9.被取代的行业明晰呈现，新的工作机会强势呈现\_\_

\_\_10.被颠覆的商业\_\_

\_\_11.全息显示设备的出现\_\_

知乎：

https://www.zhihu.com/question/57935491

生成对抗网络（GANs）

所有神经网络的独特格式（Tensorkow/Keras）

Zoos大爆发

AutoML更换管道

形式化的智能堆栈

基于语音的应用

更加聪明的机器人

时间序列分析现状

内嵌函数之外的优化

总结

有几种技术现在可以用于实际产品：时间序列分析，GANs，语音识别，NLP的一些进展。我们不应该再设计用于分类或回归的基本框架，因为AutoML就能做这些。但是可以改进优化，AutoML能够比以前更快。再加上ONNX和Model Zoo，只需两行代码就能为我们的app加入基本的模型。目前制作基于AI的应用程序已经变得非常容易，至少在目前最先进的水平上如此

36Kr

**新的学习模型是关键要素。**

**人工智能会消除人类（认知）偏差，并能让我们变的更像人造的**

**人工智能正在改变物联网（设备）**