

大家好，关于防控中的人工智能很多朋友都还不太明白，今天小编就来为大家分享关于防控中的人工智能是指的知识，希望对各位有所帮助！

本文目录

1. [人工智能的利与弊分别是什么，该如何看待？](#)
2. [什么是人工智能？你听过人工智能吗？我们该如何看待人工智能？](#)
3. [现在的人工智能到底有多智能？](#)
4. [人工智能如何防范黑客攻击？](#)

人工智能的利与弊分别是什么，该如何看待？

人工智能给我们生活带来的好处：人工智能在数据集上有着一定的优势。人工智能有三大商业方向：大数的统计、对用户情绪评估、与用户之间的社交纽带。人工智能通过这三大商业方向，以更好地了解人类。同时也可以创作出更好的软件，以此来给更多的人带来快乐。在未来可以增加客户体验，给客户带来快乐的企业，将会赚取更多的商业价值。当扫地机器人、削面机器人、做饭机器人、工业机器人、消防机器人、战斗机器人等开始运用于我们的生活中时，不得不说给我们的生活带来了极大便利。人工智能在能源发展过程中会间接地提高能源的利用率。这个功能在日常生活中的表现是：有些智能硬件，可以根据你以往的习惯，判断你什么时候到家，这样在你进入房子之前它就可以把室内气温调节到相宜的温度，这样就是一种节约能源的方式。如果这种智能设备能够被成千上万个家庭使用的话，那能源利用率就会极大地提高，能源就会得到极大的节省。其次，人工智能和人类智慧越来越明显的分工会极大地节省人力资源成本，这必然会成为人工智能在未来工业领域的一大趋势：有些效率低的工作由智能机器人做得更好。比如有些重复性的工作，这些工作由智能机器人来做不但节约了人力成本而且提高了工作的效率。如果把人工智能应用在工业中，去调节一些不可控的因素，而不需要消耗大量的人力。比如风车发电，有了人工智能，就不需要浪费大量人力在不确定的风向上，人工智能设备会根据不同的风向对风车做出相应的并且是及时的调整。人工智能在医疗上也起到很大的帮助。很多医生都不能确定的病情，人工智能可以通过它的大数据进行分析和理疗。再好比当下的人工智能无人汽车。在技术保障的前提下，这不仅大大降低了事故发生率，还节省了驾驶人员大量的驾驶时间。

人工智能给我们生活带来的风险：大规模的失业，人工智能的发展，导致很多人失业，机器人不会犯错，不会累，不需要休息，不需要工资，这完全可以代替很多职业；人工智能时代的到来可能是对人类的一次大淘汰。机器人对人类的大淘汰；才争夺战导致垄断、贫富分化加剧，人工智能时代的到来，必将引发空前的人才争夺战。谁拥有的各类一流人才数量多质量高，谁就能赢得最后胜利。随着社会科技的快速发展，人工智能进入了高速发展的轨道。人工智能给我们生活带来了许多便利。

人工智能带给我的利大于弊，机遇与风险并存，如何利用好大数据更为重要!

什么是人工智能？你听过人工智能吗？我们该如何看待人工智能？

人工智能之父John McCarthy说：人工智能就是制造智能的机器，更特指制作人工智能的程序。人工智能模仿人类的思考方式使计算机能智能的思考问题，人工智能通过研究人类大脑的思考、学习和工作方式，然后将研究结果作为开发智能软件和系统的基础。

人工智能的概念很宽，所以人工智能也分很多种，我们按照人工智能的实力将其分成三大类：

1、弱人工智能

弱人工智能Artificial Narrow Intelligence(ANI):弱人工智能是擅长于单个方面的人工智能。比如有能战胜象棋世界冠军的人工智能，但是它只会下象棋，你要问它怎样更好地在硬盘上储存数据，它就不知道怎么回答你了。比如第一个击败人类职业围棋选手、第一个战胜围棋世界冠军的人工智能机器人，AlphaGo其实也是一个弱人工智能。

2、强人工智能

强人工智能又称通用人工智能或完全人工智能，指的是可以胜任人类所有工作的人工智能。一个可以称得上强人工智能的程序，大概需要具备以下几方面的能力：存在不确定因素时进行推理，使用策略，解决问题，制定决策的能力；知识表示的能力，包括常识性知识的表示能力；规划能力；学习能力；使用自然语言进行交流沟通的能力；将上述能力整合起来实现既定目标的能力。

3、超人工智能

假设计算机程序通过不断发展，可以比世界上最聪明、最有天赋的人类还聪明，那么由此产生的人工智能系统就可以被称为超人工智能。超人工智能的定义最为模糊，因为没人知道，超越人类最高水平的智慧到底会表现为何种能力。如果说对于强人工智能，我们还存在从技术角度进行探讨的可能性的话，那么，对于超人工智能，今天的人类大多就只能从哲学或科幻的角度加以解析了。

现在的人工智能到底有多智能？

现在的人工智能总的来说，可以算是有智能没智慧、有智商没情商、会计算不会算

计、有专才而无通才。

我们看待现阶段的人工智能，它的强大，绝不体现在以自主意识为代表的智能上，而主要体现在以大量数据计算的实时性和准确性为代表的智能上，与人的优缺点恰好互补，赋能现有产业，为生产效率带来提升。

现在人工智能的“智能”可以重点关注一下几点。

大量历史经验数据对当前决策的客观指导

当人在面对一个选择时，经常会依赖历史经验来进行决策。古人有言，“早霞不出门，晚霞行千里”，这个时候判断明天天气好坏的依据仅有是否出现早霞和晚霞，这个二维信息进行决策。随着气象科学的发展，我们现在知道，判断第二天天气好坏，需要考虑方方面面的信息，例如：空气湿度、风向风速、地形位置等。

现在我们将目光转向股市，由于全球市场经济的高度耦合，带来了前所未有的复杂性。如果抱着“跌买入，涨买进”这样简单的理财理念，已经完全无法应付股市的复杂情况，银行板块的涨幅，可能受到政策影响、利率影响、粮食价格波动、黄金价格波动等等影响。这个时候对于一个单个的个体而言，想要处理如此繁杂的信息，首先无法很快获取所有信息进行辅助决策，此次人脑也无法客观的将多维的信息进行汇总分析。

而依赖人工智能的机器却更适合处理类似问题，尤其在金融行业，数字化开展较早，因此有大量的数据辅助决策。人只需要将可能影响到这只股票的信息高速训练模型，基于机器学习的算法模型可以按照历史信息进行“学习”，来判断当前状况下，这只股票涨跌的可能性分别是多少，甚至可以预估短时间内可以达到的涨幅。

当前，我需要分析一个股票是否需要买入卖出，算法模型会通过大量多维的历史数据作为“经验数据”，将这些经验通过模型拟合成多维曲线，那么，如果想评估当前情况，我只需要将此时此刻这些影响因素的当前状况为坐标，标记在这个多维曲线中，并映射到一个一维坐标下，即“涨”或“跌”。对于短期进行的估计，人工智能可能会比人类更“靠谱”一些。

需要依赖大量记忆的最佳决策

人类目前即使面对最强大的机器，在自主的创造力上还是保持着“爸爸”等级的存在，人类在创造力上还是属于绝对的领先。即使现在已经广泛应用的机器翻译来说，机器翻译确实已经足够的准确，但是语言的“信达雅”上，机器翻译还是有很长的路要走。

但是，毋庸置疑，人类的大脑构造本身是不适合做存储和计算的。

在审问时，当警察让嫌疑人将所有事件按照时间从近到远再重复一次时，人往往无法对刚刚编出的故事做准确的描述，因此人“记事”往往是用事情的互相关系来进行记忆的，而不只是存储时间本身，并为这些事件标记时间戳。

计算就更不用说了，现在有多少人，即使在计算二位数的加减都要依赖计算器来实现。

而机器却不一样，前几年名声大噪的AlphaGo，打败围棋各路高手，可是AlphaGo的成功是因为它“智能”吗？其实并不是如此。

围棋虽然变化多样，但是规则还是相对简单。在互相对弈的过程中，人类可能会往前演算5-7步，可是这个时候AlphaGo早已经将所有的后续发展可能性演算完成，并按照事先定义好的数据结构进行存储。

换句话说，当人类和AlphaGo在对弈过程中，机器的每步均是在当前情况下，以“最大胜率”为评价分数，将棋子放在了评价分数最高的位置上。当AlphaGo“学习”玩所有的招式后，那么人类与AlphaGo下棋，最佳的结果就是打成平手，因为AlphaGo不会犯错。

总结

总之，目前的人工智能没你想象的那么强大，但是可以比你想象的还要专业。

人工智能如何防范黑客攻击？

简单说说自己的认识吧。

毫无疑问，今天互联网和技术已经成为人类最强大的工具，但对这一巨大力量的有效监管和控制仍有待开发。为超过20亿的在线用户提供高效的安全系统已经成为一个巨大的挑战。

看看近年来的网络安全事件：

2015年年初，希拉里邮件门事件导致曾人气领先的希拉里惜败。

2016年2月，SWIFT黑客事件爆发，孟加拉国等多家银行损失8000多万美元

2016年10月，美国遭史上最大规模DDoS攻击、东海岸网站集体瘫痪

2017年5月，WannaCry勒索病毒事件全球爆发，150个国家、30万名用户中招，数十亿美元损失。

2017年6月，1.98亿美国选民信息泄露

2017年10月，雅虎30亿用户账号信息泄露

(PS：以上事件数据粗略统计，数据来源于网络)

很明显，我们在提供传统的网络安全方面几乎没有取得什么成果，因为没有足够的人力去持续对付那些臭名昭著的网络犯罪分子。据估计，全球需要超过100万名网络安全专家来填补网络安全岗位。

如今，从初创企业到全球大型组织，各种规模的企业都在大力投资人工智能，以改善网络安全。人工智能系统通过在最短的时间内分析大量数据，帮助网络安全专家识别检测到的所有潜在威胁。

以下是人工智能能够真正帮助防止潜在黑客攻击的几种方法:

1.使用机器学习算法

通过整合机器学习算法，智能系统可以不断进化出识别和分析系统安全缺陷的能力。例如，通过不断地仔细检查网络钓鱼信息，人工智能可以发展其检测信息和常用的即使过了信任标签的钓鱼方式的能力。通过应用这种持续的发展的智能，人工智能系统可以很容易地预测系统内部的异常或恶意行为。

2.跟踪网络罪犯

网络匿名已经成为当今黑客的最大福利。虽然网络匿名的利弊仍有争议，但事实是，人工追踪网络罪犯变得越来越困难。在大数据和网络安全分析的帮助下，人工智能不仅可以帮助追踪网络犯罪的源头，还可以帮助预测网络攻击方式以及攻击时间

。

3.分析攻击的后果

不管一个组织或公司有多强的能力来抵御攻击，随着对黑客的持续攻击，没有什么是可以完全预测的。调查攻击的原因和后果是非常重要的，通过使用自动调查算法

，人工智能可以帮助网络专业安全专家理解所需的信息并得出有根据的结论。

4.对攻击立即作出反应

就像网络安全防御技术一样，网络攻击的多样性和复杂性也在不断进化。黑客每天都在寻找新的方法来破坏系统。当系统受到攻击时，时间起着极其重要的作用。在攻击过程中使用旧的病毒检测软件，会损失大量的时间，因为大多数软件只能检测到可识别的恶意病毒。如果是黑客重新设计的新病毒，就很难识别它们。

在这种情况下，人工智能不仅可以帮助检测可识别的病毒，还可以帮助预测和分析病毒的行为。这种快速的预测可以帮助专业人员认识到威胁并尽可能减少损害。

未来。。。

正如任何事物都有两面性一样，在网络安全问题上，人工智能既可用于建设性目的，也可用于破坏性目的。智能系统的快速发展也可以被黑客利用，除非有革命性的技术出现，否则未来依然还是一场猫与老鼠的游戏。

好了，本文到此结束，如果可以帮助到大家，还望关注本站哦！