谷歌镜像：

<https://scholar.xiayige.org/>

arXiv镜像：

<http://xxx.itp.ac.cn/>

arXiv收录未被期刊或会议发表的文章，换句话说，是提前抢占学术高地。谷歌上AI相关文章基本都被arXiv提前收录。

利用镜像下载论文，只需将论文识别号（例如，1911.13019）加在链接上

<http://xxx.itp.ac.cn/pdf/1911.13019.pdf>

CCF推荐期刊会议：

<https://www.ccf.org.cn/Academic_Evaluation/NIS/>

CCF中安全四大会：CCS、S&P、USENIX SECURITY、NDSS

CCF中人工智能顶会：ICML、NeurIPS、CVPR、AAAI、IJCAI （这些会包含很多AI安全文章）

除此之外，未被CCF收录的最高水平的AI顶会 ICLR，论文收录链接：

<https://openreview.net/group?id=ICLR.cc/2020/Conference> （历年收录均有，只需链接修改年份）

选择要看的论文：  
1）近年顶会文章，相关方向文章。

2）引用顶会文章的最新文章，一般提前发表在arXiv。首先要判断文章中作者水平，查看前几位作者是否发过顶会。

3）访问顶会文章作者的谷歌主页或是个人主页，查看是否有最新文章。

人工智能中安全与隐私基本包括：

安全：Poisoning attack, Adversarial attack, Backdoor attack

隐私：Membership inference attack, Model extraction attack, Property inference attack, Model inversion attack, Watermarking