LAB 10: ARTIFICIAL INTELLIGENCE AND CRACKING CAPTCHAS

Satvik Anand

404823011

TOPICS

Explain what AI is and how it works

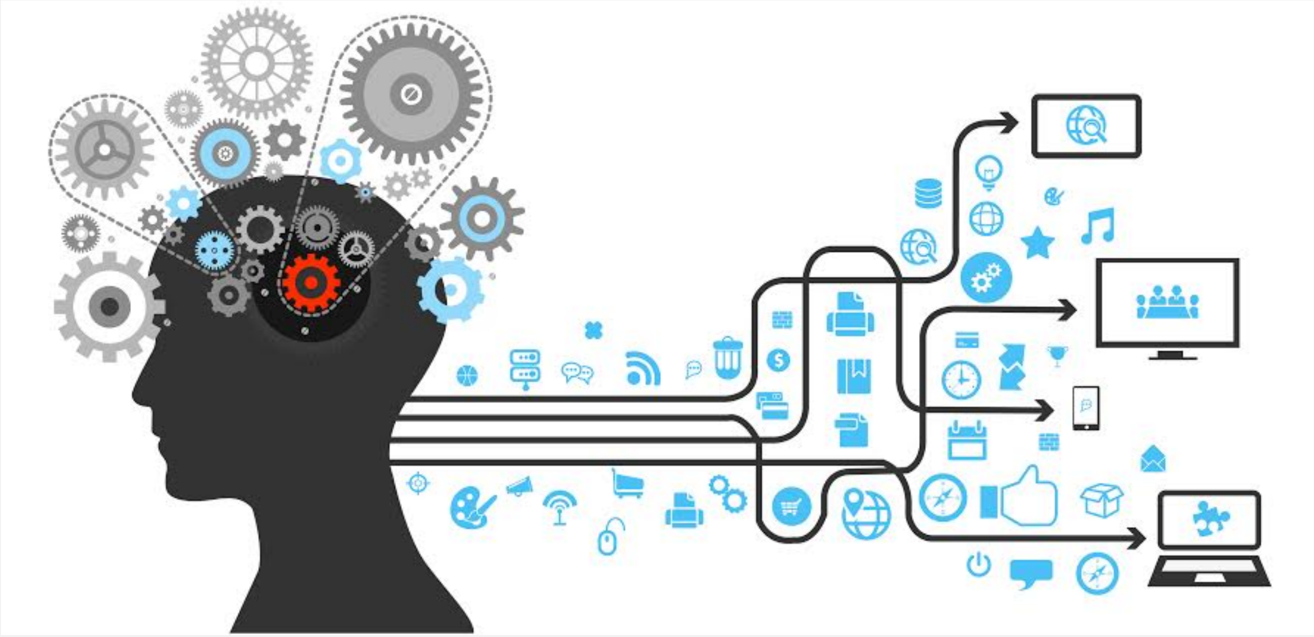
What are CAPTCHAs

How AI cracking CAPTCHAs is a measure of how good the AI is

How does the AI crack CAPTCHAs

Next steps

ARTIFICIAL INTELLIGENCE



MACHINE LEARNING

Machine learning deals with making computers learn without being explicitly programmed

You basically create programs that are trained to recognize new patterns and evolve on the basis of these patterns.

Once you have created these patterns, you’re able to eliminate the eventual need to write code because your basic programs are doing everything for you

CAPTCHA

- CAPTCHA stands for Completely Automated Public Turing Test To Tell Computers and Humans Apart
- What it actually is the squiggly lines/characters that you've seen on tons of websites.
- Turing Test is a test that is used to decide whether a machine is capable of acting in an intelligent manner

THINGS TAKEN IN ACCOUNT IN CREATED CAPTCHAS

Metadata accessible to robots.

Predetermined CAPTCHAs with predetermined answers

Random strings of letters to prevent brute force attacks

Distorting

Puzzles and extrapolation

BREAKING CAPTCHAS

Lots of attempts

Ticketmaster sued a tech company which was able to buy tickets in bulk

These attempts were only exploiting a weakness in the CAPTCHA which could be fixed

BREAKING CAPTCHAS

New methods involve deep learning

Deep learning is a technique where you have layers of neurons and you train those neurons to respond in a way that you decide.

There are downfalls to deep learning as well.

RECURSIVE CORTICAL NETWORK

AI sees things and builds its own model of what it sees.

Understands contours and shapes

Tries to correlate new images with the models that it has in its memory

NEXT STEPS

Long term goal through these kinds of experiments is to build machines that are fully able to think like humans

So AI which requires less training is better than that which requires more training

It's not clear how much impact this will have on information security