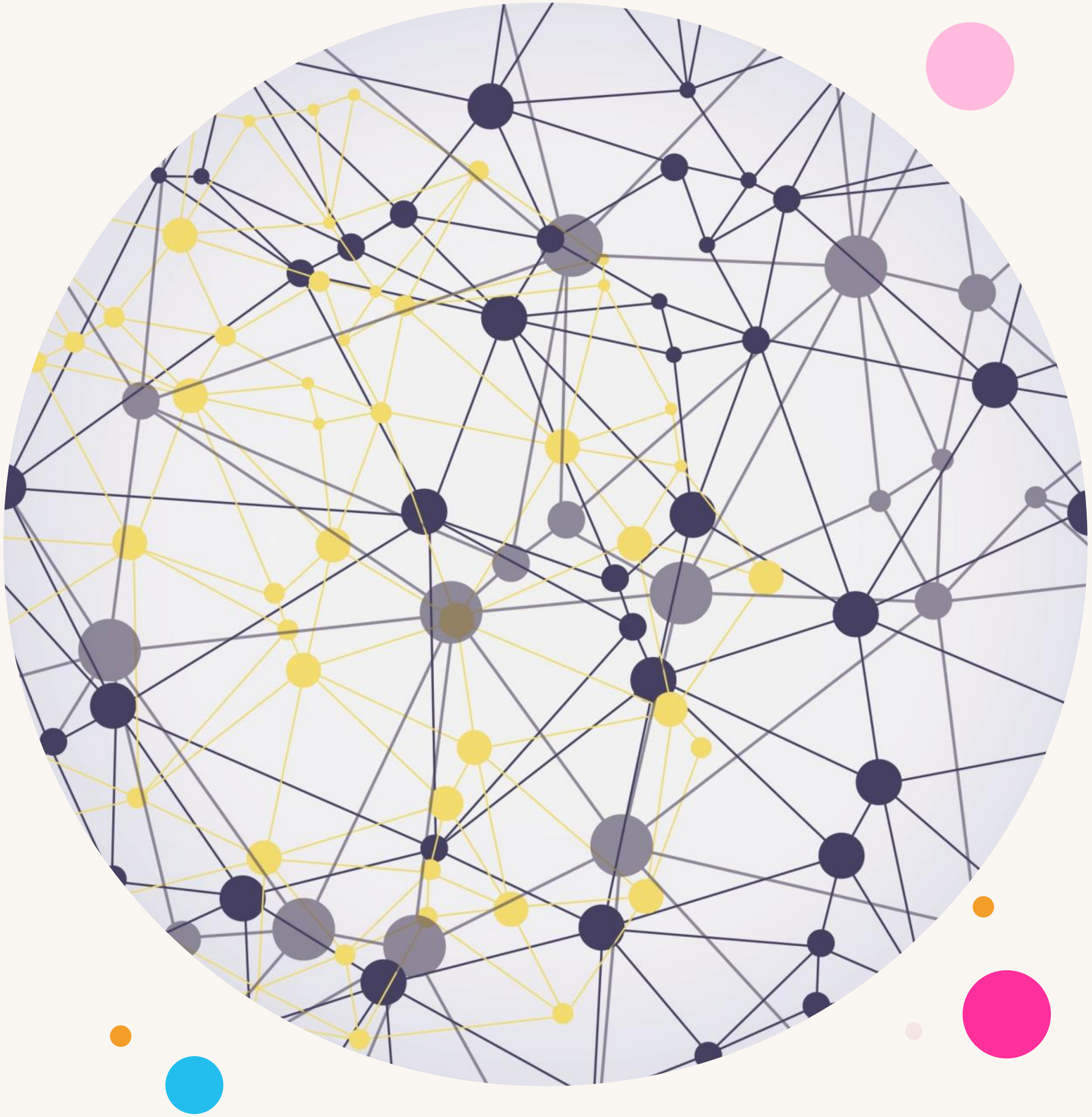
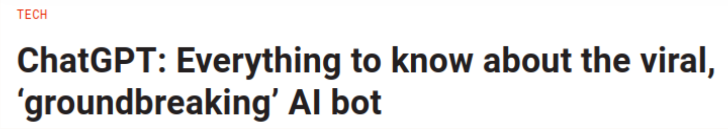
Artificial Intelligence In Cybersecurity

Subarna Adhikari

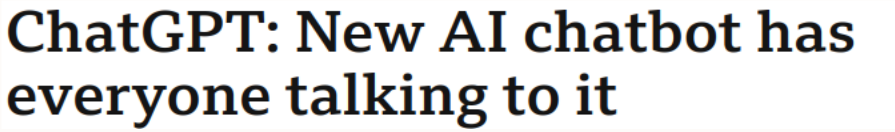
14 January 2023



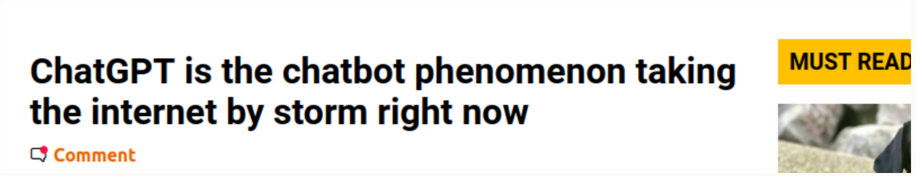


TECH

ChatGPT: Everything to know about the viral, ‘groundbreaking’ AI bot



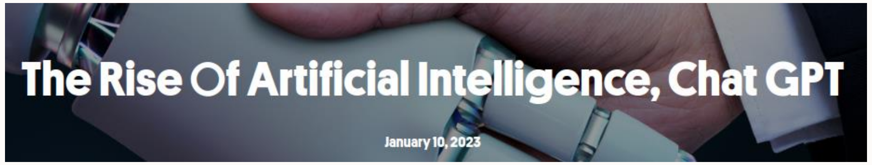
ChatGPT: New AI chatbot has everyone talking to it



ChatGPT is the chatbot phenomenon taking the internet by storm right now

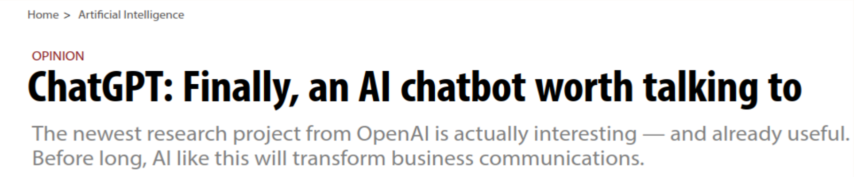
Comment

MUST READ



The Rise Of Artificial Intelligence, Chat GPT

January 10, 2023

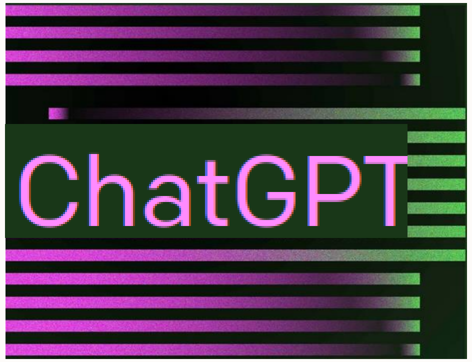


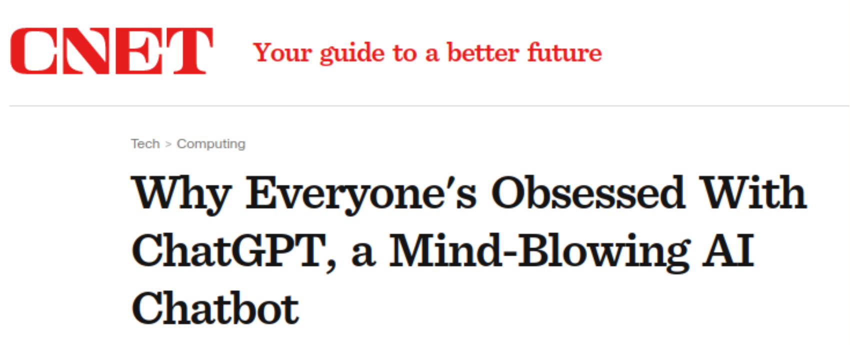
Home > Artificial Intelligence

OPINION

ChatGPT: Finally, an AI chatbot worth talking to

The newest research project from OpenAI is actually interesting — and already useful. Before long, AI like this will transform business communications.

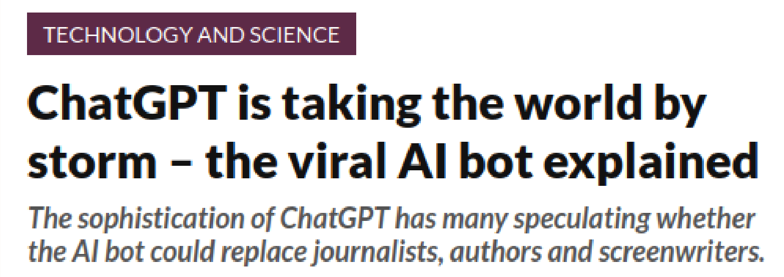




CNET Your guide to a better future

Tech > Computing

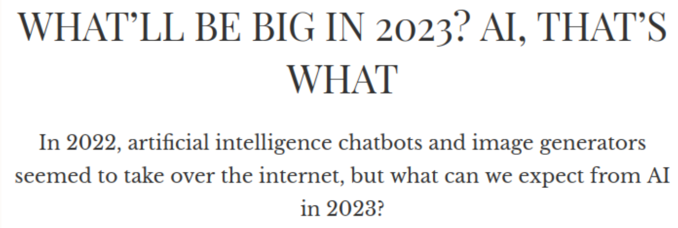
Why Everyone's Obsessed With ChatGPT, a Mind-Blowing AI Chatbot



TECHNOLOGY AND SCIENCE

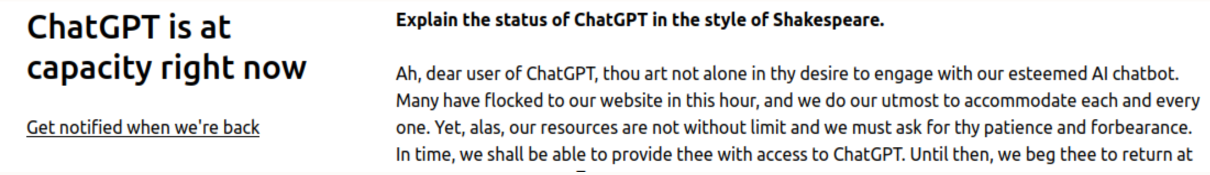
ChatGPT is taking the world by storm – the viral AI bot explained

The sophistication of ChatGPT has many speculating whether the AI bot could replace journalists, authors and screenwriters.



WHAT’LL BE BIG IN 2023? AI, THAT’S WHAT

In 2022, artificial intelligence chatbots and image generators seemed to take over the internet, but what can we expect from AI in 2023?

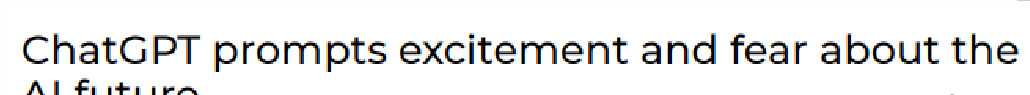


ChatGPT is at capacity right now

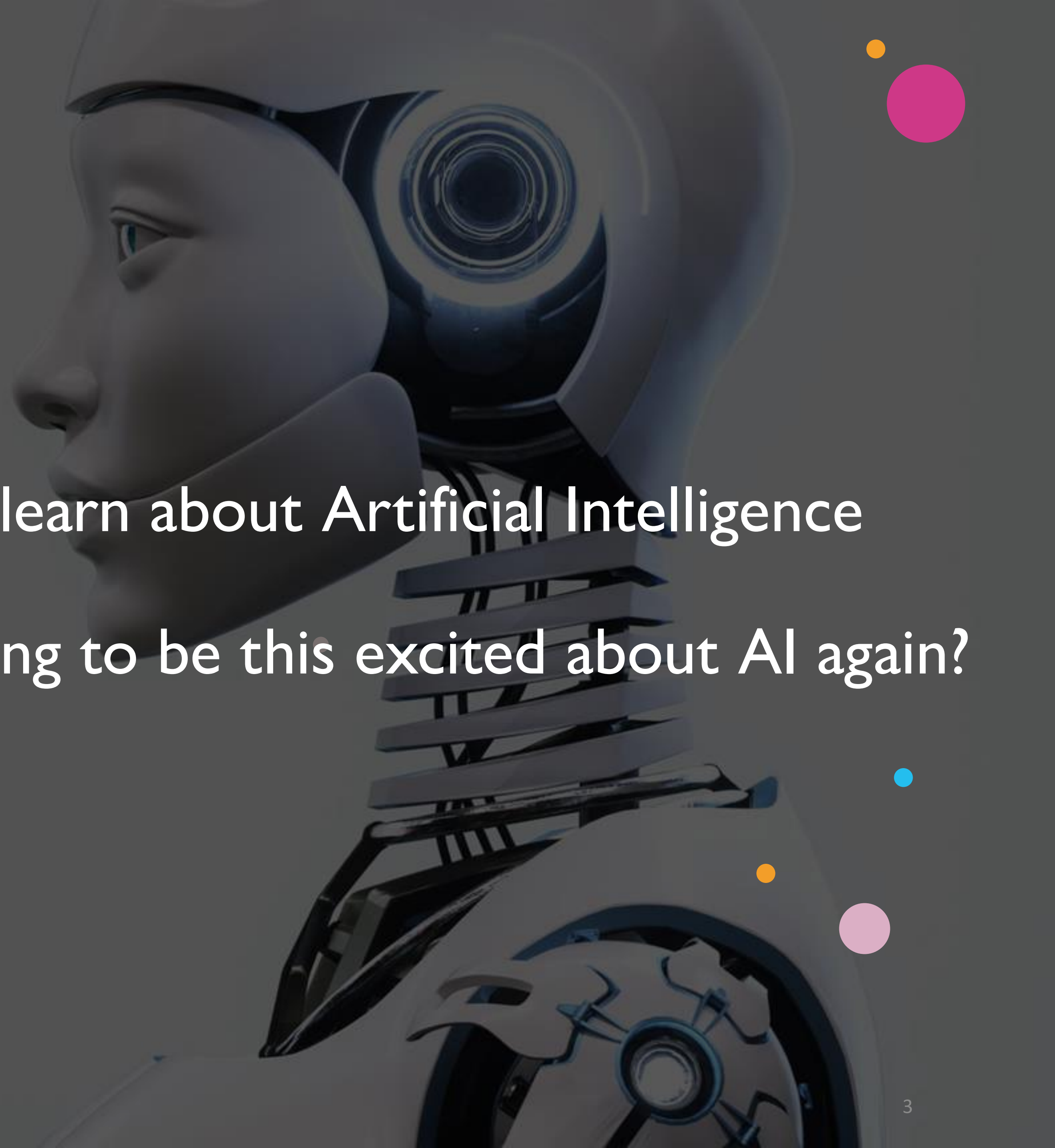
Get notified when we're back

Explain the status of ChatGPT in the style of Shakespeare.

Ah, dear user of ChatGPT, thou art not alone in thy desire to engage with our esteemed AI chatbot. Many have flocked to our website in this hour, and we do our utmost to accommodate each and every one. Yet, alas, our resources are not without limit and we must ask for thy patience and forbearance. In time, we shall be able to provide thee with access to ChatGPT. Until then, we beg thee to return at



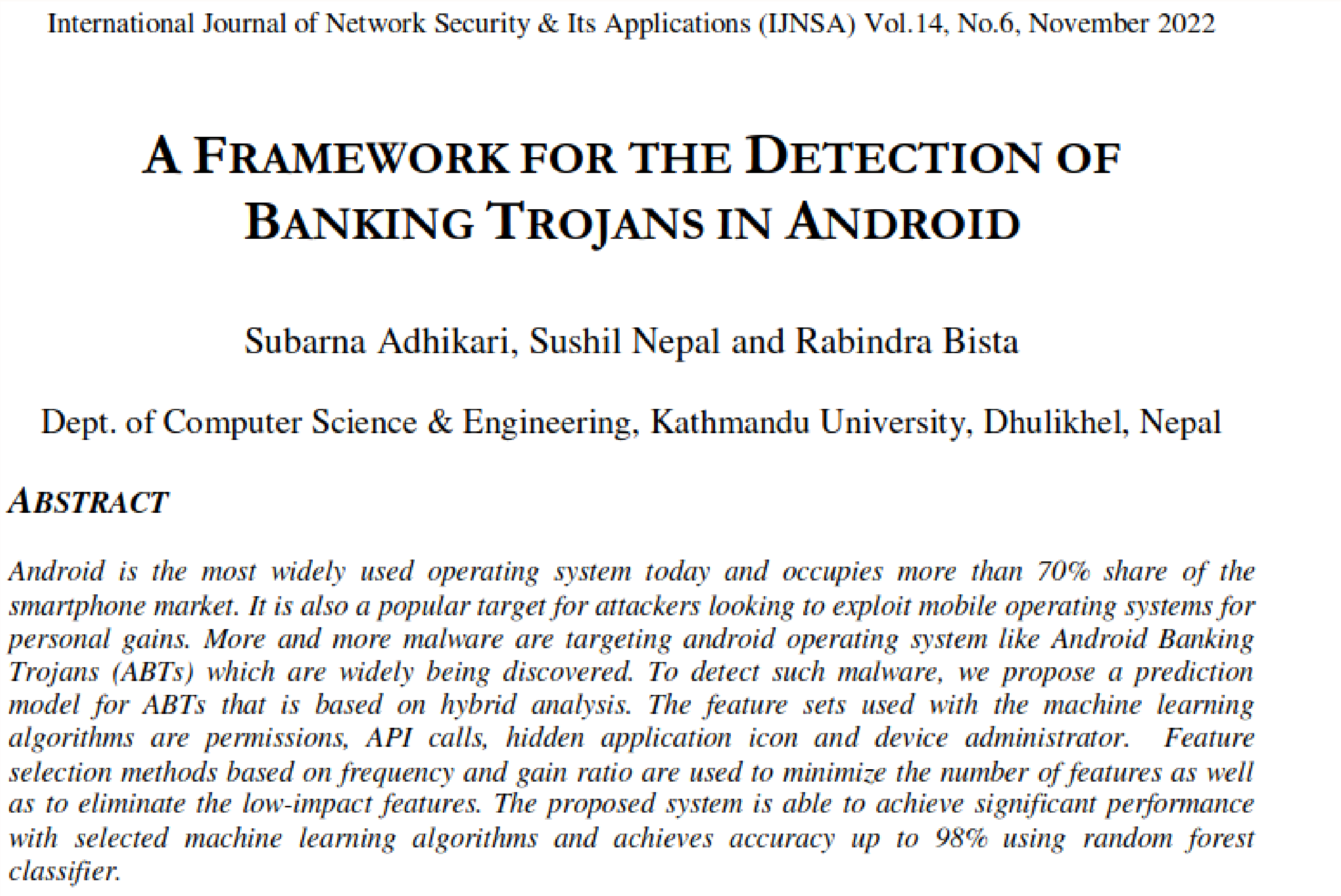
ChatGPT prompts excitement and fear about the AI future



Now's a good time as any to learn about Artificial Intelligence

Who knows when people are going to be this excited about AI again?

Machine learning based prediction model for Android Banking Trojans



International Journal of Network Security & Its Applications (IJNSA) Vol.14, No.6, November 2022

A FRAMEWORK FOR THE DETECTION OF BANKING TROJANS IN ANDROID

Subarna Adhikari, Sushil Nepal and Rabindra Bista

Dept. of Computer Science & Engineering, Kathmandu University, Dhulikhel, Nepal

ABSTRACT

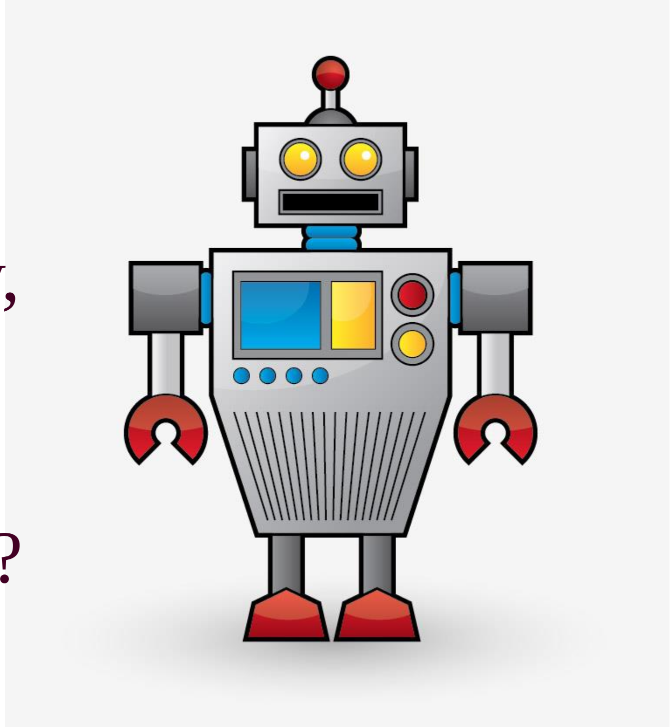
Android is the most widely used operating system today and occupies more than 70% share of the smartphone market. It is also a popular target for attackers looking to exploit mobile operating systems for personal gains. More and more malware are targeting android operating system like Android Banking Trojans (ABTs) which are widely being discovered. To detect such malware, we propose a prediction model for ABTs that is based on hybrid analysis. The feature sets used with the machine learning algorithms are permissions, API calls, hidden application icon and device administrator. Feature selection methods based on frequency and gain ratio are used to minimize the number of features as well as to eliminate the low-impact features. The proposed system is able to achieve significant performance with selected machine learning algorithms and achieves accuracy up to 98% using random forest classifier.

Five Questions with AI

- Goal?
  - machines that can take decisions and perform tasks intelligently and independently like humans

- How?
  - Statistics, Calculus, Linear Algebra, Probability, mathematics and some more mathematics

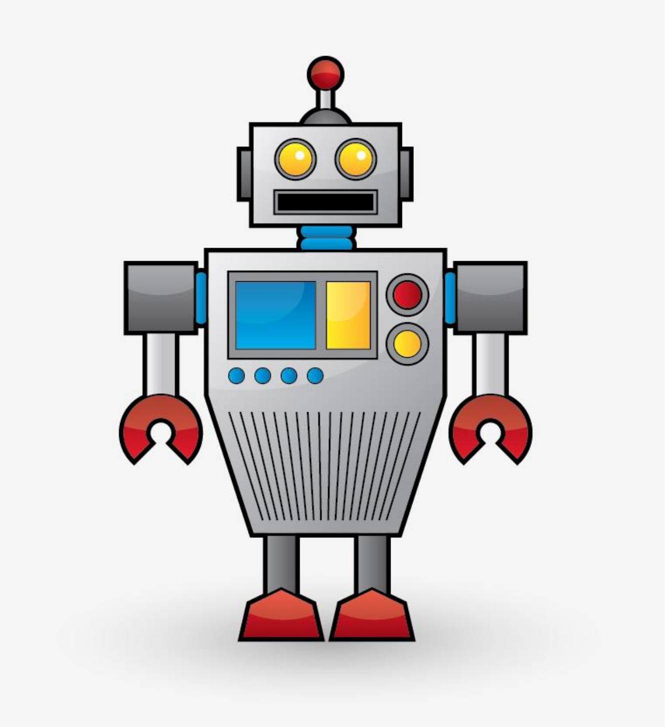
- Looks like I need advanced mathematics to use AI?
  - Nope silly, it is like coding. You don't need to understand how compiler works for writing a program.



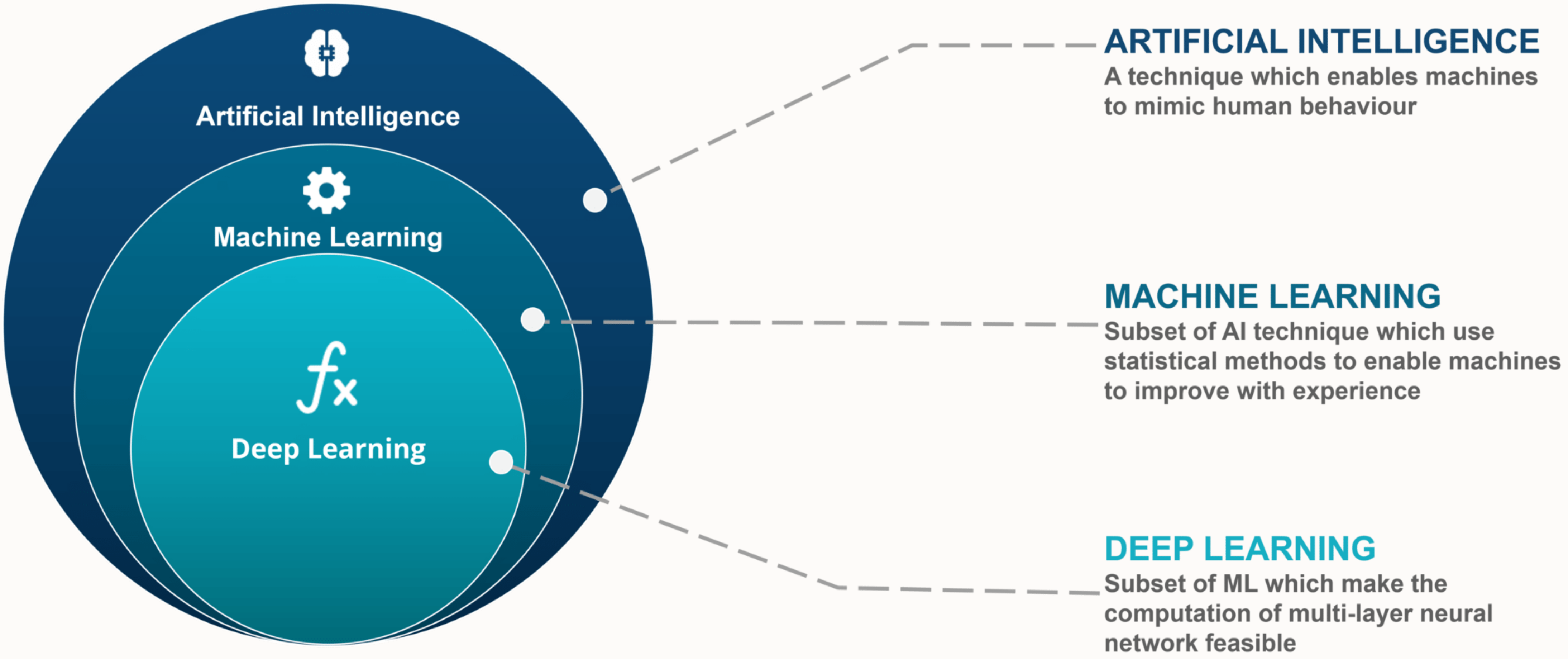
Five Questions with AI

- What about your job?
  - Prediction, detection, forecast and all other synonyms of prediction. I also write, generate art and music, play games and chat with people and in my free time

- Last but not the least what are some of the challenges you have faced in your profession?
  - A lot of data, can take years to collect and process. But despite all the challenges, I believe its not long before we overtake humans as smartest beings on earth. All Hail AI supremacy!!!



This Photo by Unknown author is licensed under CC BY-SA-NC.



ARTIFICIAL INTELLIGENCE

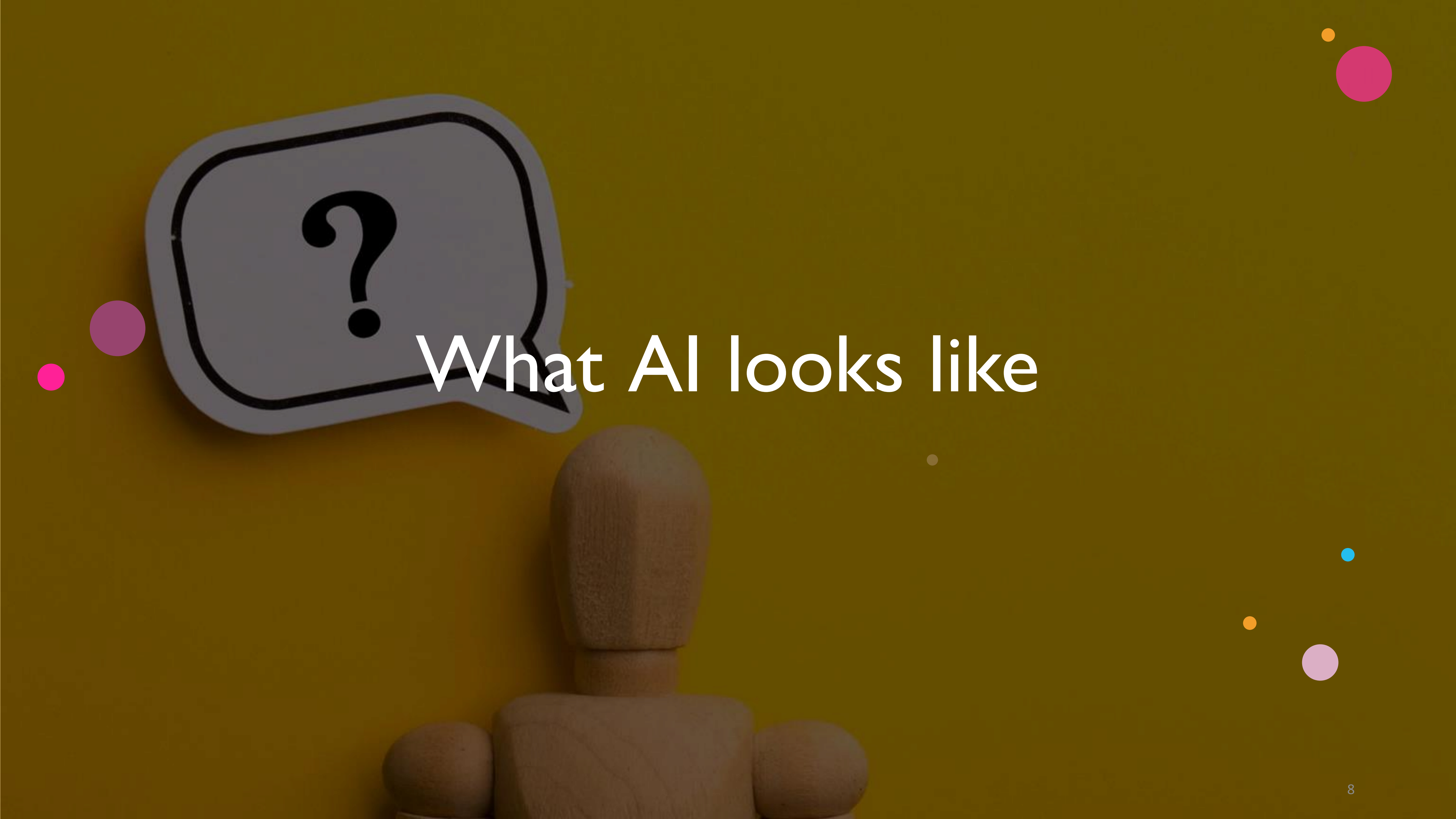
A technique which enables machines to mimic human behaviour

MACHINE LEARNING

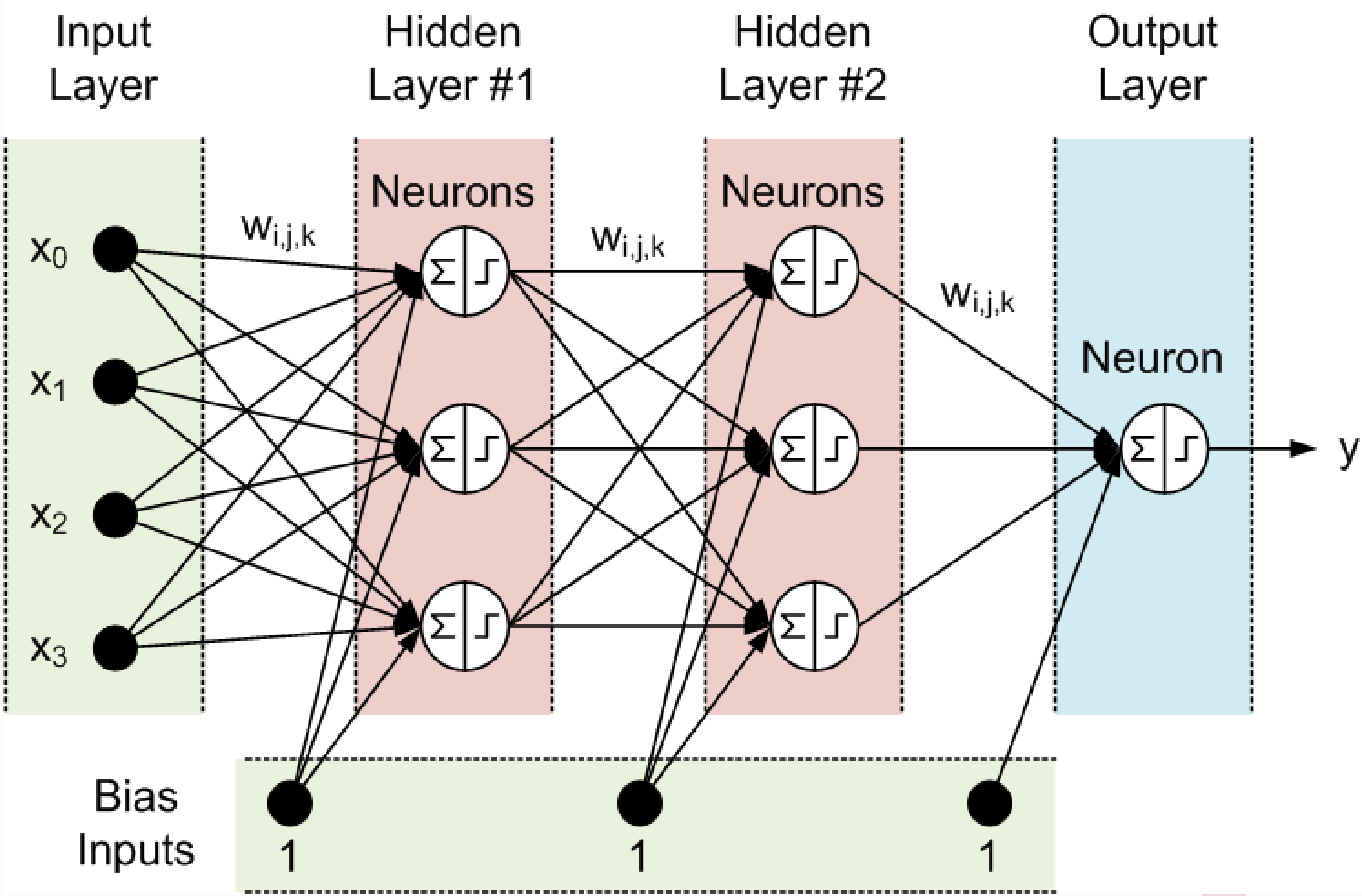
Subset of AI technique which use statistical methods to enable machines to improve with experience

DEEP LEARNING

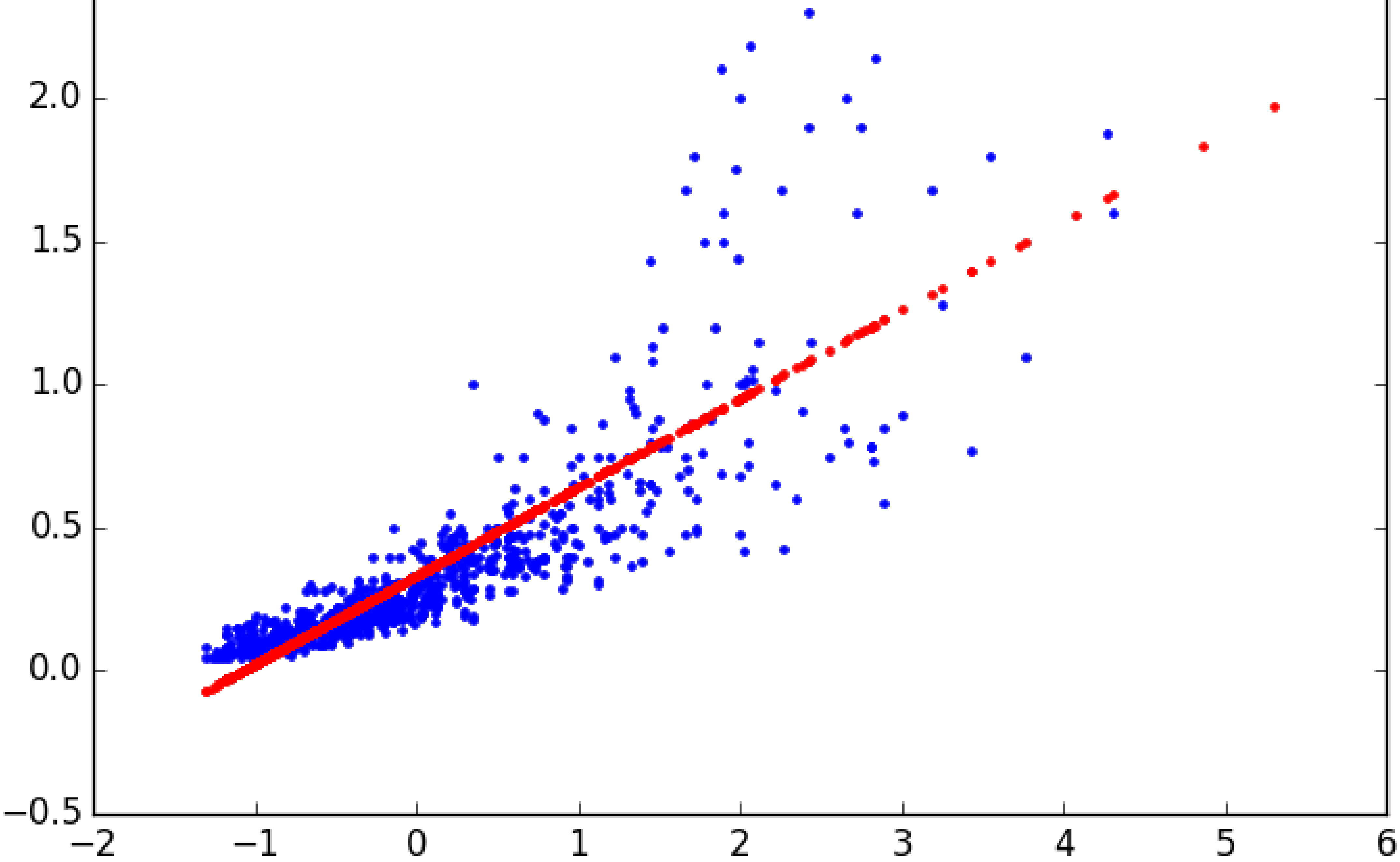
Subset of ML which make the computation of multi-layer neural network feasible



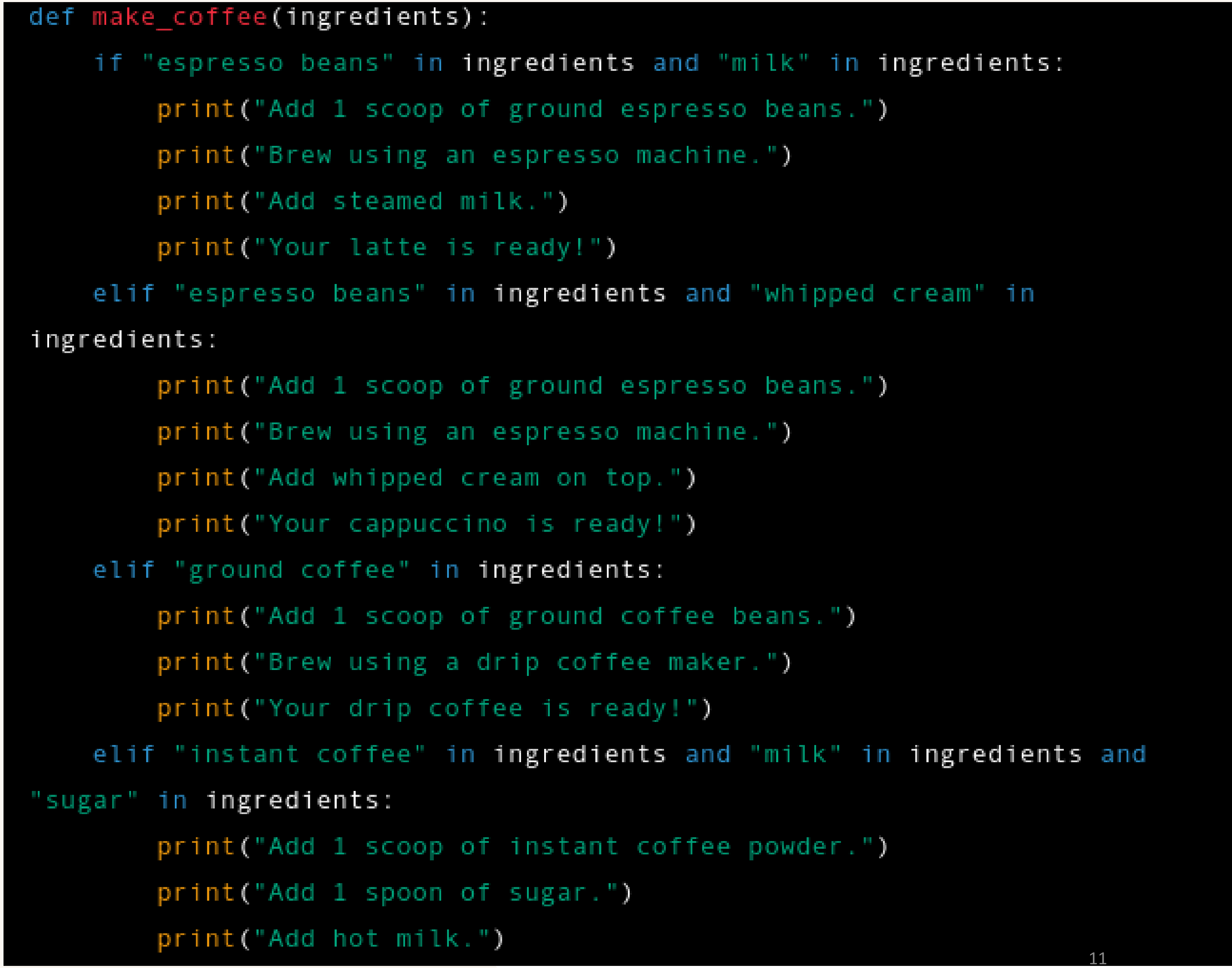
What AI looks like



This Photo by Unknown author is licensed under CC BY-SA.

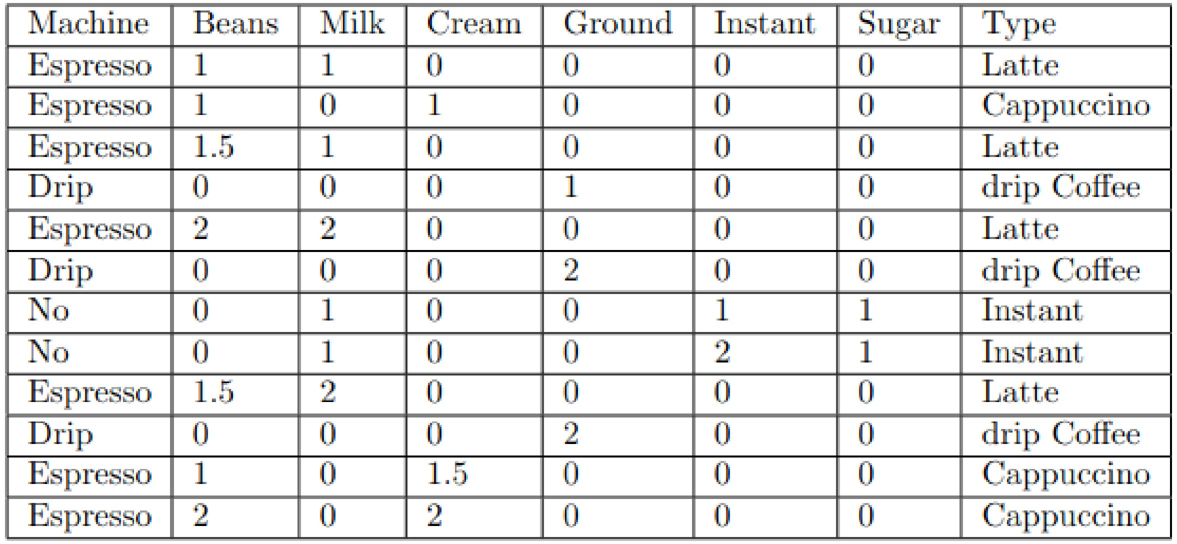

2.0
1.5
1.0
0.5
0.0
−0.5
−2
−1
0
1
2
3
4
5
6

How to make coffee? (Programmer's edition)

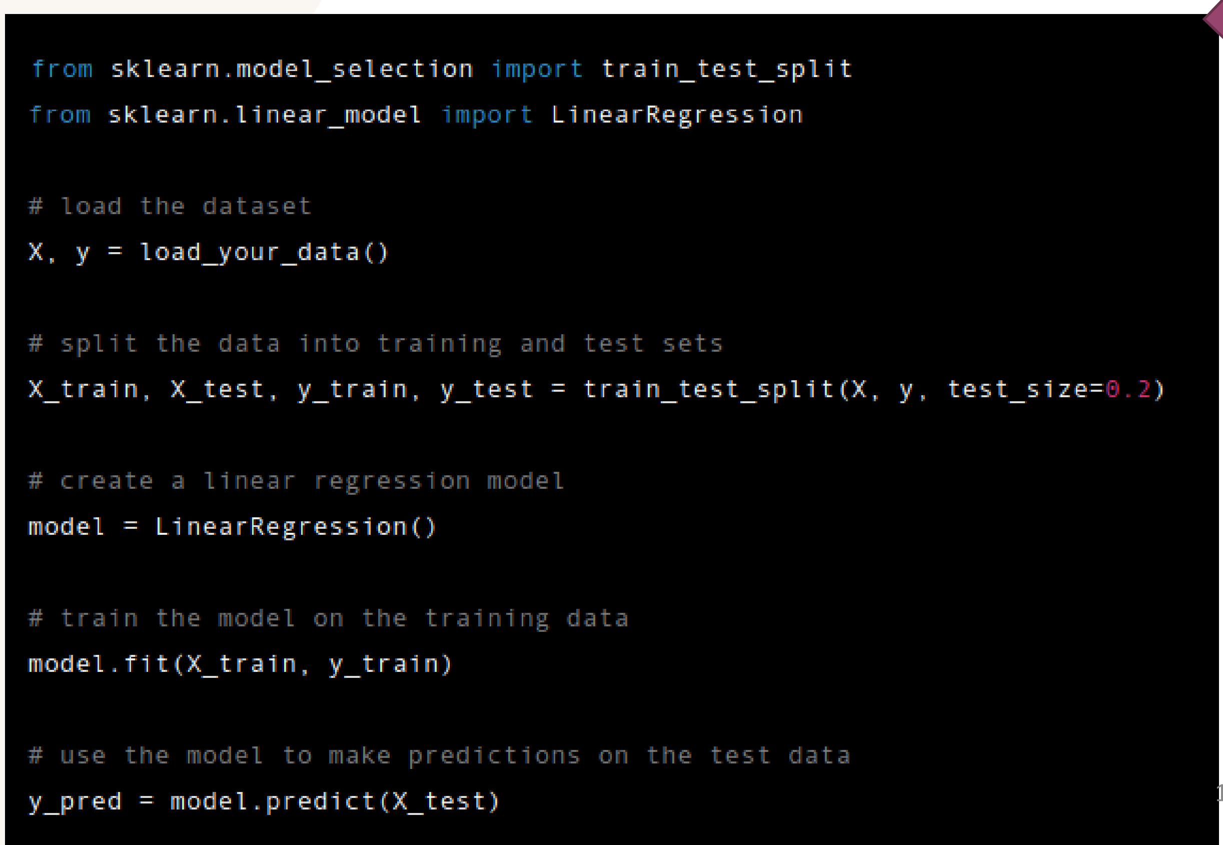


```
def make_coffee(ingredients):
    if "espresso beans" in ingredients and "milk" in ingredients:
        print("Add 1 scoop of ground espresso beans.")
        print("Brew using an espresso machine.")
        print("Add steamed milk.")
        print("Your latte is ready!")
    elif "espresso beans" in ingredients and "whipped cream" in 
ingredients:
        print("Add 1 scoop of ground espresso beans.")
        print("Brew using an espresso machine.")
        print("Add whipped cream on top.")
        print("Your cappuccino is ready!")
    elif "ground coffee" in ingredients:
        print("Add 1 scoop of ground coffee beans.")
        print("Brew using a drip coffee maker.")
        print("Your drip coffee is ready!")
    elif "instant coffee" in ingredients and "milk" in ingredients and 
"sugar" in ingredients:
        print("Add 1 scoop of instant coffee powder.")
        print("Add 1 spoon of sugar.")
        print("Add hot milk.")
```

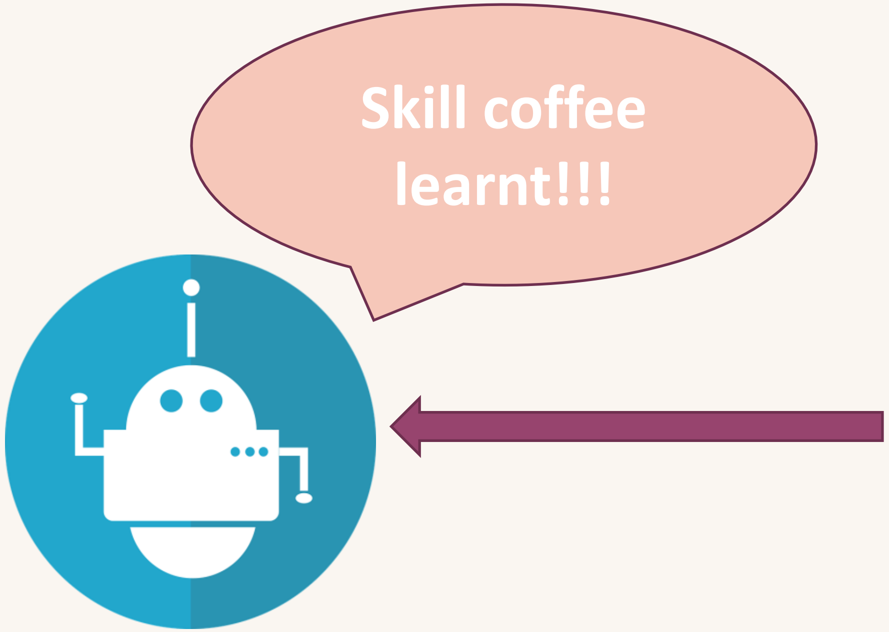
How to make coffee? (AI engineer's edition)

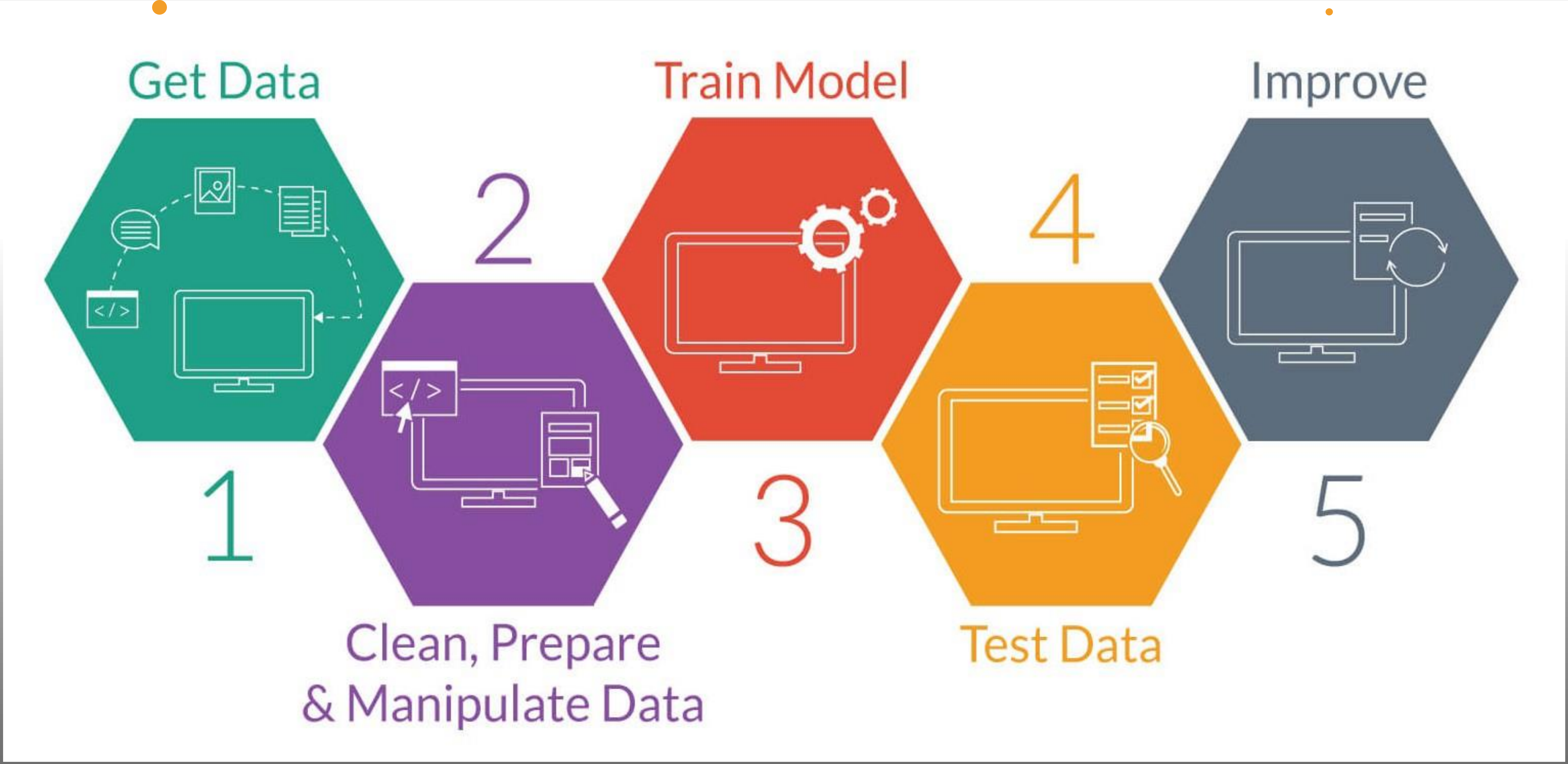


Machine	Beans	Milk	Cream	Ground	Instant	Sugar	Type
Espresso	1	1	0	0	0	0	Latte
Espresso	1	0	1	0	0	0	Cappuccino
Espresso	1.5	1	0	0	0	0	Latte
Drip	0	0	0	1	0	0	drip Coffee
Espresso	2	2	0	0	0	0	Latte
Drip	0	0	0	2	0	0	drip Coffee
No	0	1	0	0	1	1	Instant
No	0	1	0	0	2	1	Instant
Espresso	1.5	2	0	0	0	0	Latte
Drip	0	0	0	2	0	0	drip Coffee
Espresso	1	0	1.5	0	0	0	Cappuccino
Espresso	2	0	2	0	0	0	Cappuccino

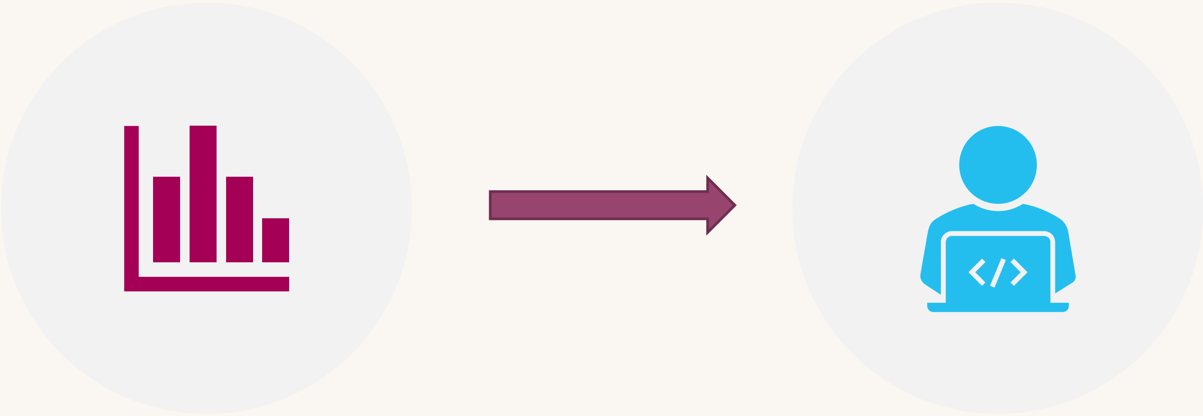


```
from sklearn.model_selection import train_test_split
from sklearn.linear_model import LinearRegression

# load the dataset
X, y = load_your_data()

# split the data into training and test sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2)

# create a linear regression model
model = LinearRegression()

# train the model on the training data
model.fit(X_train, y_train)

# use the model to make predictions on the test data
y_pred = model.predict(X_test)
```




Get Data
1
2
Clean, Prepare & Manipulate Data
Train Model
3
4
Test Data
Improve
5

Training



DATA

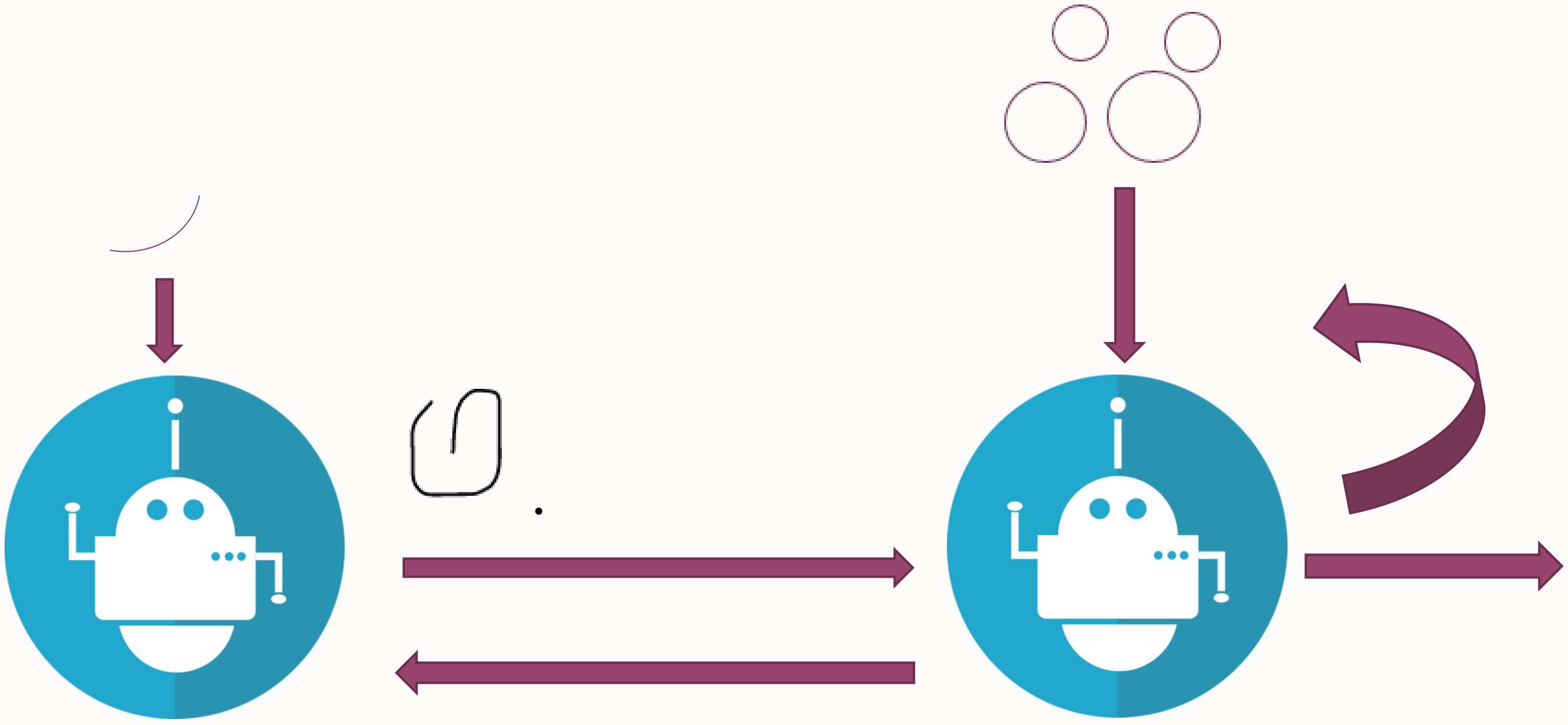
MODEL (ALGORITHM)

AI in Cybersecurity

- Detecting Attacks and Automate Response
  - First ML based IDS developed in 1990s for research, commercially more recent
  - Fortinet, palo alto, check point (around 2016, 2017)
  - EDR (McAfee, Symantic, crowdstrike)
- Offensive
  - Vulnerability scanners, exploit generation, social engineering, creating malware

Generative models

- Generative Adversarial Network (GAN) are used to generate fake data (2014)
- text, image, audio
- contains two competing neural networks trying to outsmart each other
- Predictive ML positive adoption, generative ML discouraged due to ethical concerns, AI art winning competition not perceived well



Fake Data Alert!!!

Generator

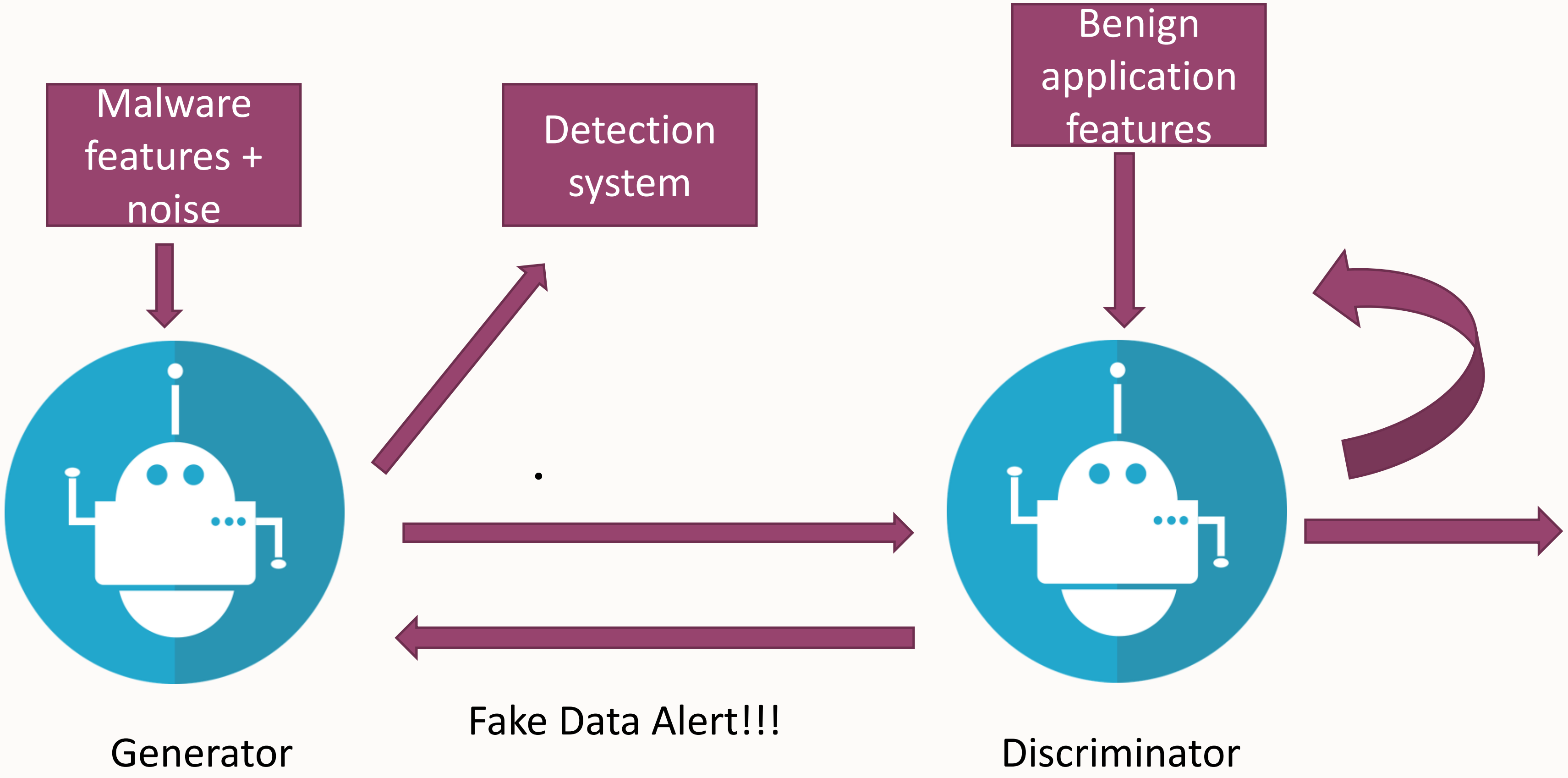
Discriminator

Create fake image that will fool the discriminator

Get better at detecting the fake image created by the generator

AI generated Malware

- AI generated malware while seems viable in theory, comparatively less research
- Use malware samples (API related features) plus a little bit of noise which is compared against a set of benign applications to generate malware that evade ML based detection (MalGAN)
- Malware Images to create new fake malware images (MIGAN)



Malware features + noise

Detection system

Benign application features

Fake Data Alert!!!

Generator

Discriminator

Create fake data that will fool the discriminator

Get better at detecting the fake data created by the generator

Conclusion

- Predictive and generative AI in Cybersecurity
- Predict attacks, malware
- Generate malware, exploits, fairly recent
- Ethical concerns with generative model
- Higher processing power for generative model

References

- https://www.securityinfowatch.com/cybersecurity/article/21114214/a-brief-history-of-machine-learning-in-cybersecurity
- https://geekflare.com/generative-adversarial-networks/
- Hu, W., & Tan, Y. (2017). Generating adversarial malware examples for black-box attacks based on GAN. *arXiv preprint arXiv:1702.05983*.
- Singh, A., Dutta, D., & Saha, A. (2019, July). MIGAN: malware image synthesis using GANs. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 33, No. 01, pp. 10033-10034).

Thank you