MACHINE LEARNING IN CYBER SECURITY

Sumanth Simha C

Samarth S

BMS College of Engineering

What Is Machine Learning

- Herbert Alexander Simon: “Learning is any process by which a system improves performance from experience.”
- “Machine Learning is concerned with computer programs that automatically improve their performance through experience. “

Herbert Simon
Turing Award 1975
Nobel Prize in Economics 1978

Why Machine Learning?

- Develop systems that can automatically adapt and customize themselves to individual users.
- Discover new knowledge from large databases (data mining).
- Ability to mimic human and replace certain monotonous tasks - which require some intelligence.
- Develop systems that are too difficult/expensive to construct manually because they require specific detailed skills or knowledge tuned to a specific task (knowledge engineering bottleneck).

Different Machine Learning Techniques

1. Bayes Classifier
2. K Means
3. Support Vector Machines
4. Linear Regression
5. Logistic Regression
6. Decision Trees
7. Random Forests
8. Artificial Neural Nets

Different Machine Learning Approaches

1. Supervised Learning
2. Unsupervised Learning
3. Reinforcement Learning

Steps in Machine Learning

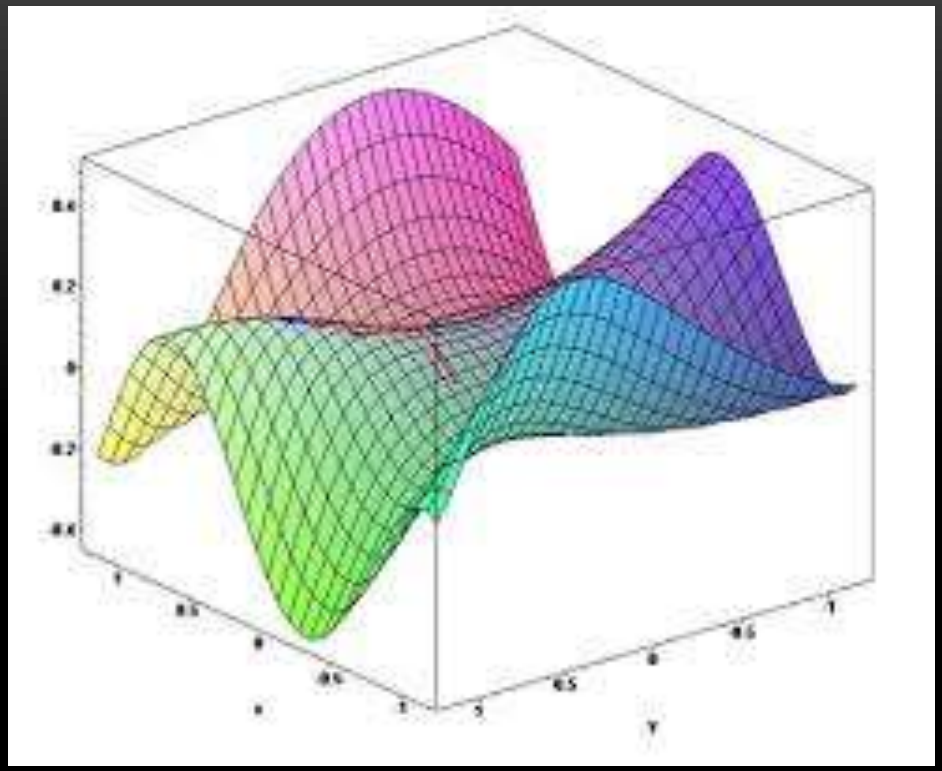
1. Data Collection
2. Data Cleaning
3. Feature Engineering
4. Learning
5. Deployment

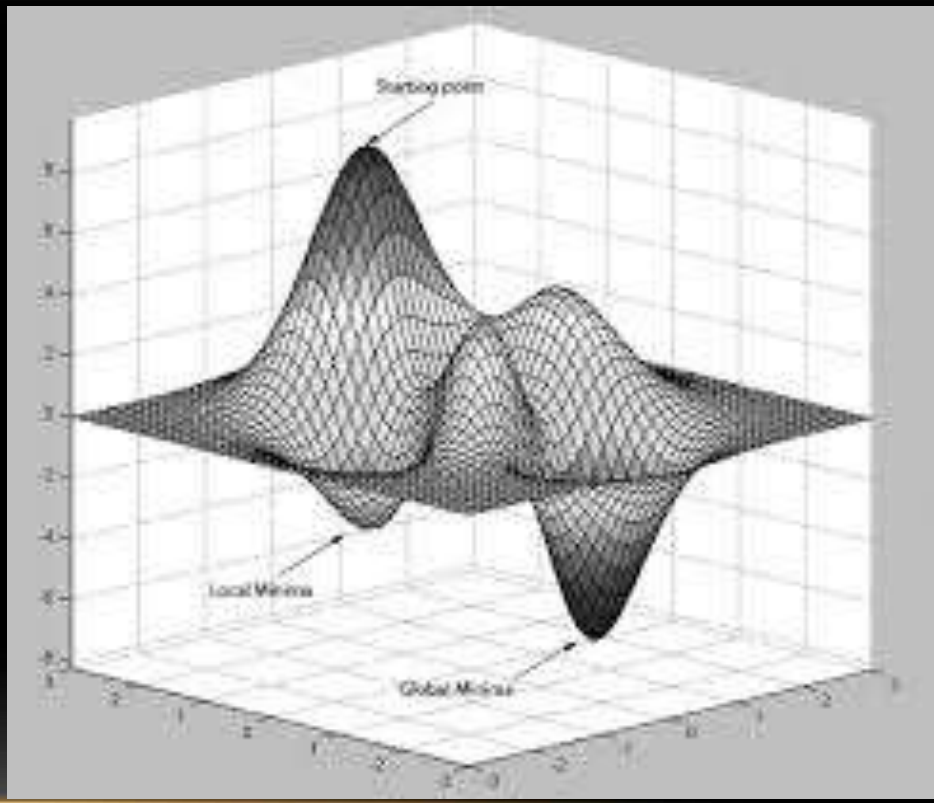
Machine Learning Terminologies

1. Features
2. Support Vectors
3. Clustering
4. Classification
5. Probability Distribution

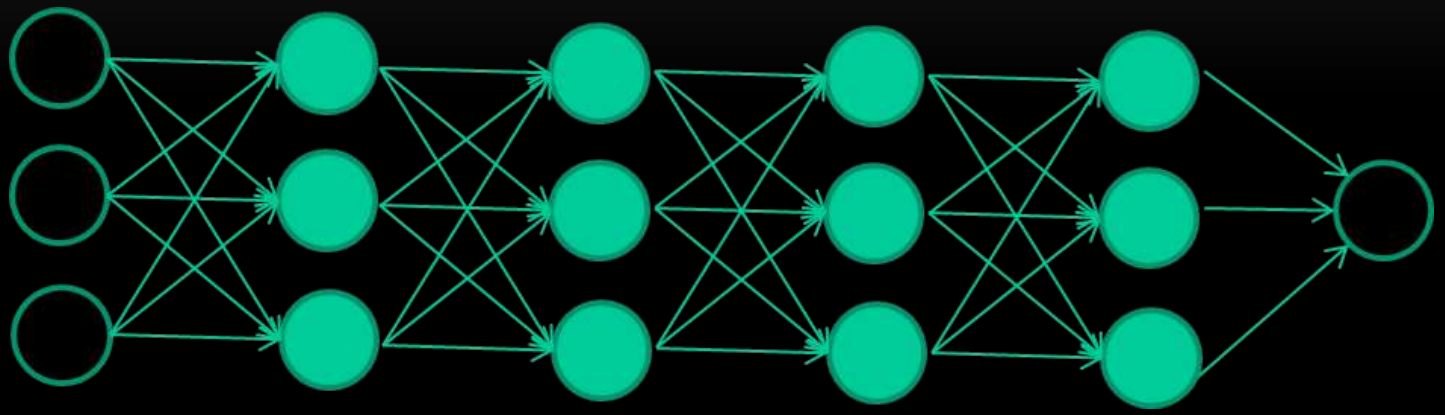
Neural Network Techniques

1. Single Layer Perceptrons
2. Multi Layer Perceptrons
3. Convolutional Neural Nets
4. Recurrent Neural Networks
5. Deep Learning

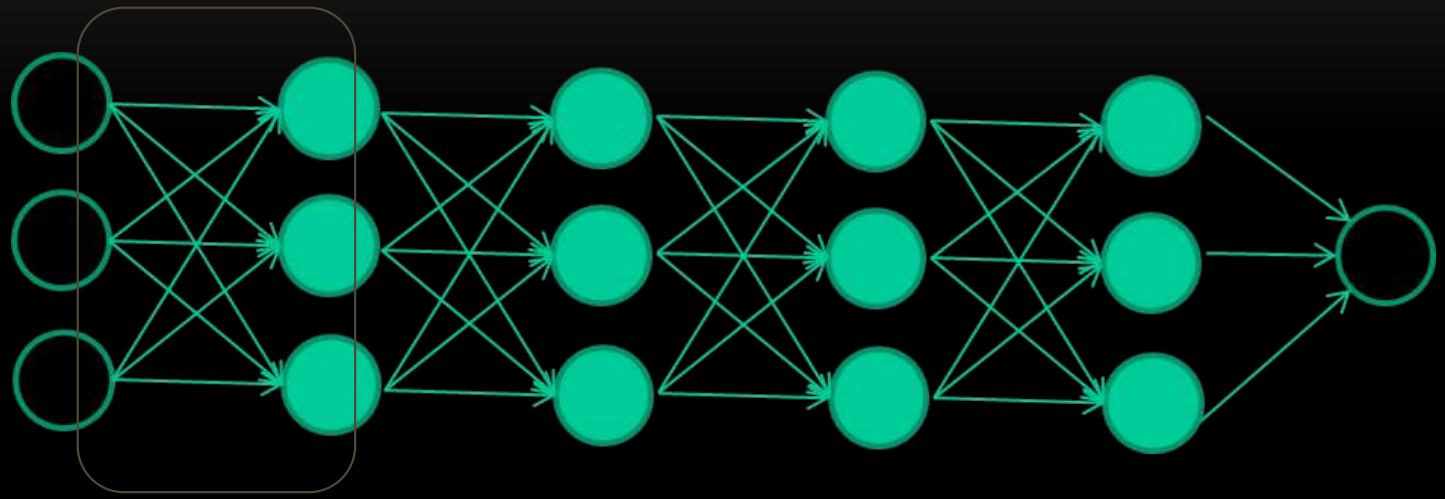



Starting point
Local Minima
Global Minima

THE NEW WAY TO TRAIN MULTI-LAYER NNS…

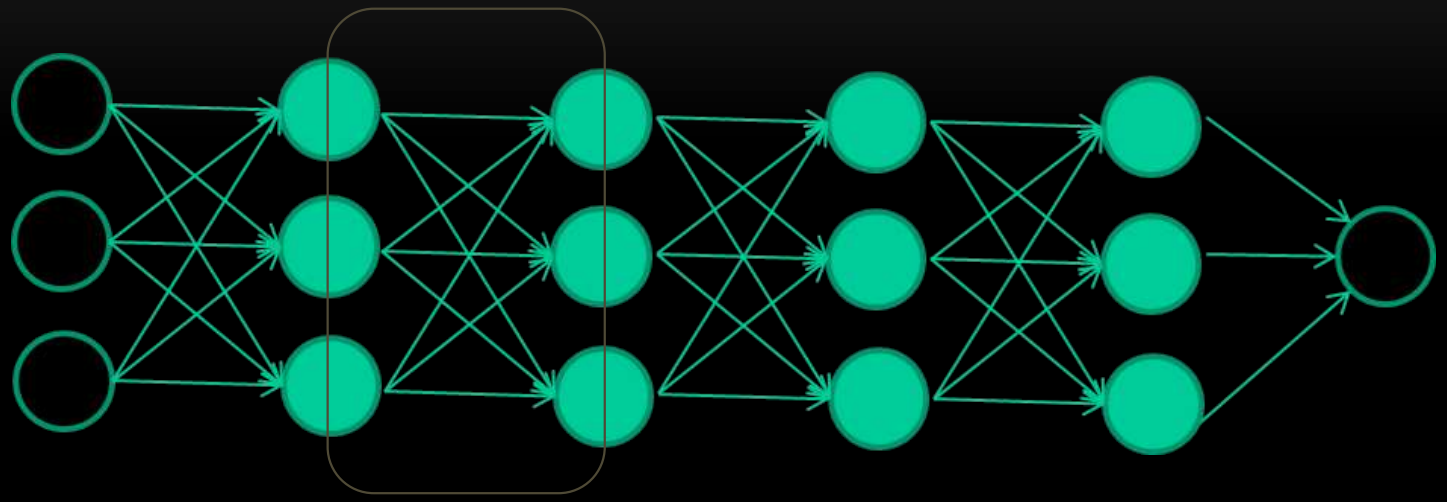


THE NEW WAY TO TRAIN MULTI-LAYER NNS…



Train **this** layer first

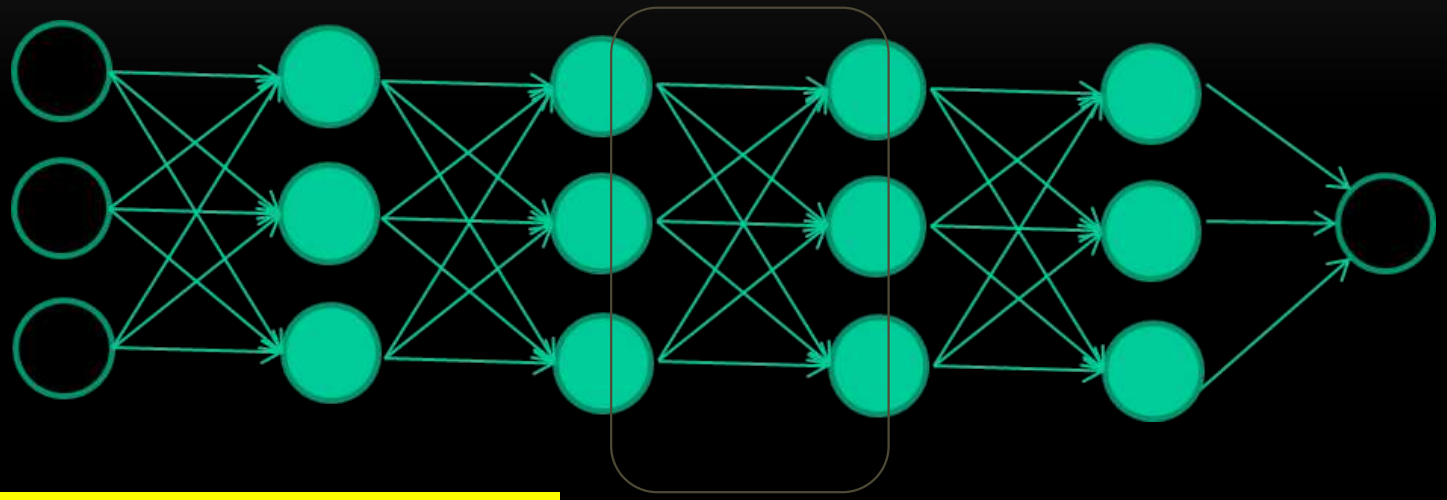
THE NEW WAY TO TRAIN MULTI-LAYER NNS…



Train **this** layer first

then **this** layer

THE NEW WAY TO TRAIN MULTI-LAYER NNS…

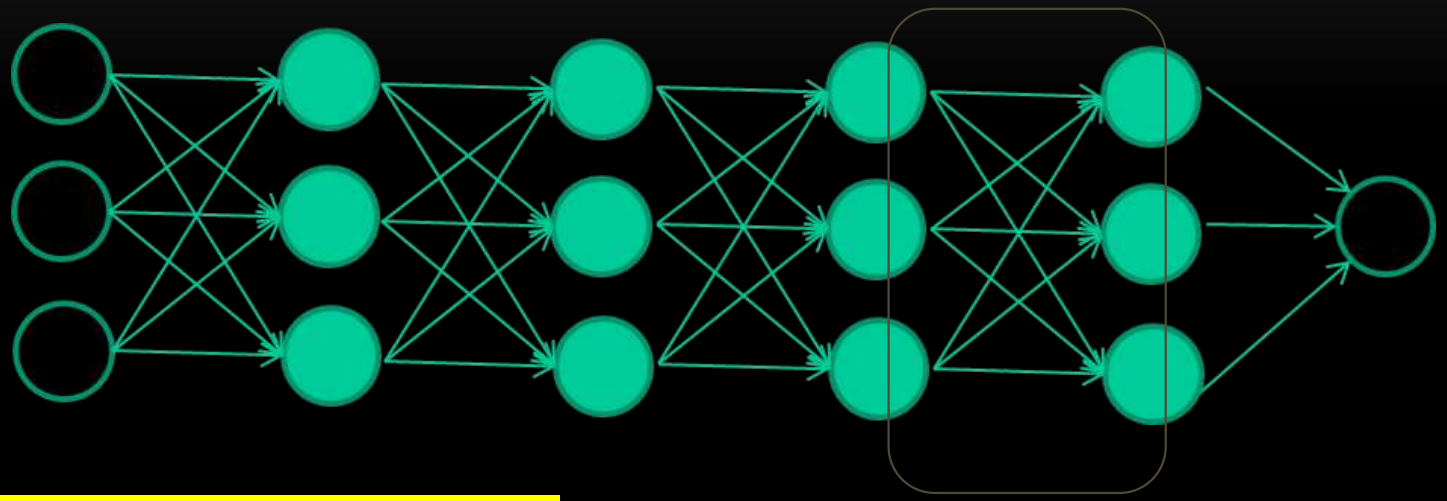


Train **this** layer first

then **this** layer

then **this** layer

THE NEW WAY TO TRAIN MULTI-LAYER NNS…



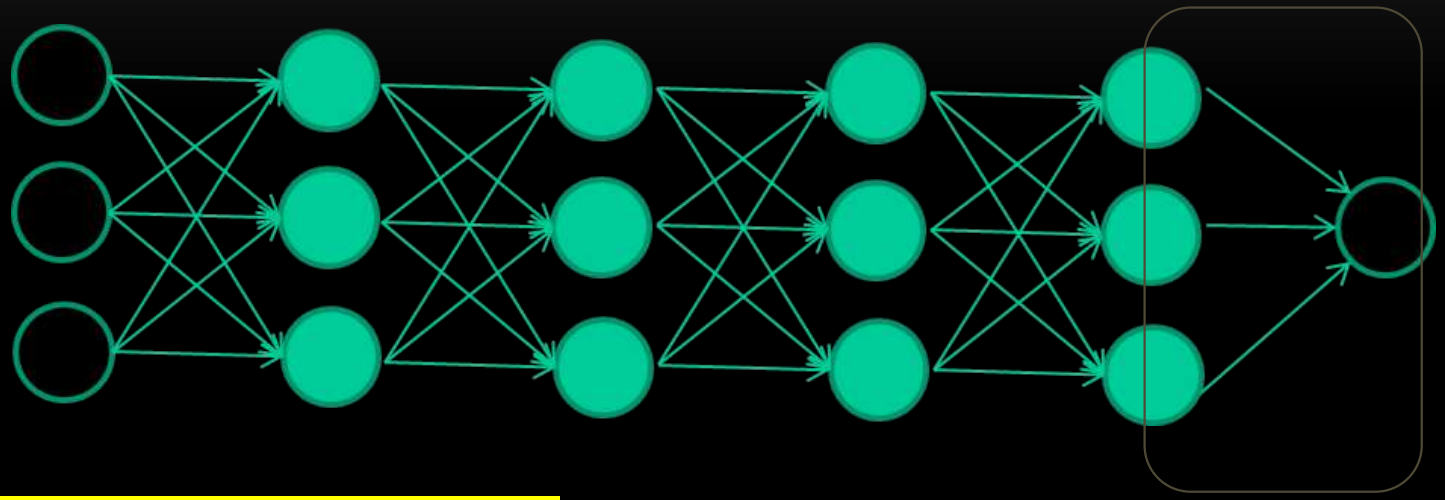
Train **this** layer first

then **this** layer

then **this** laver

then **this** layer

THE NEW WAY TO TRAIN MULTI-LAYER NNS…



Train **this** layer first

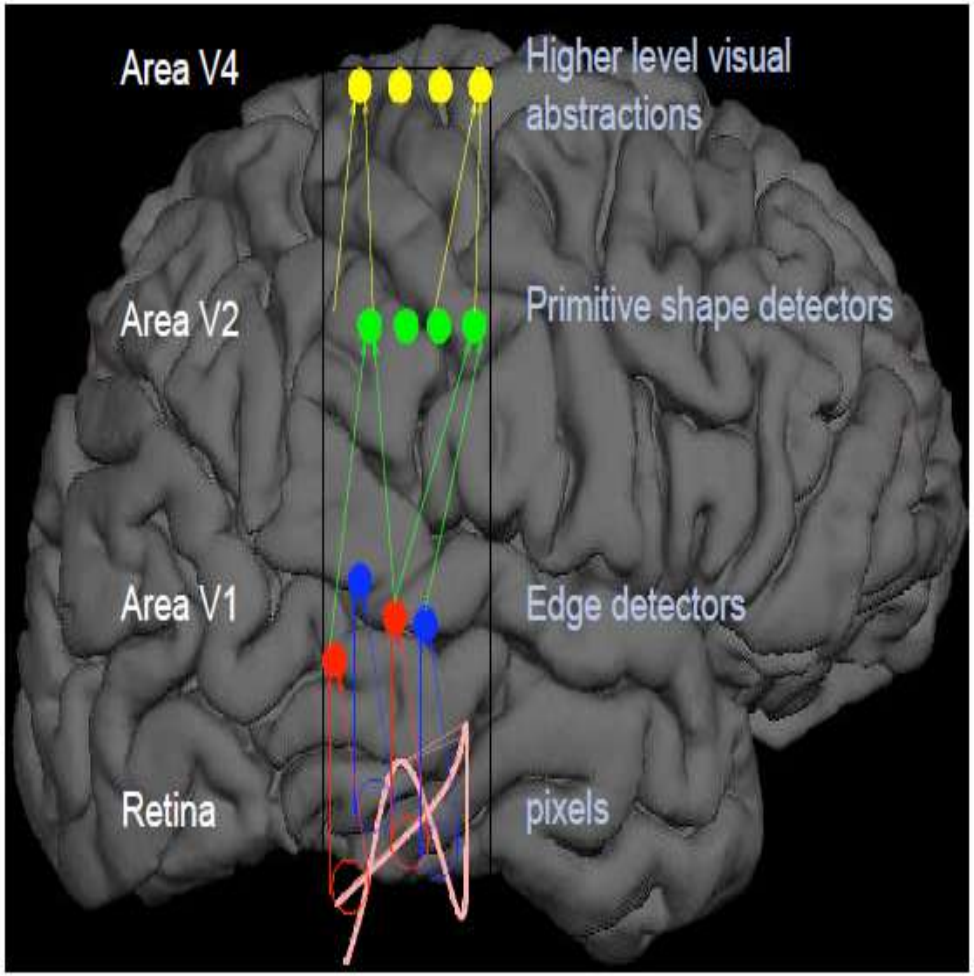
then **this** layer

then **this** laver

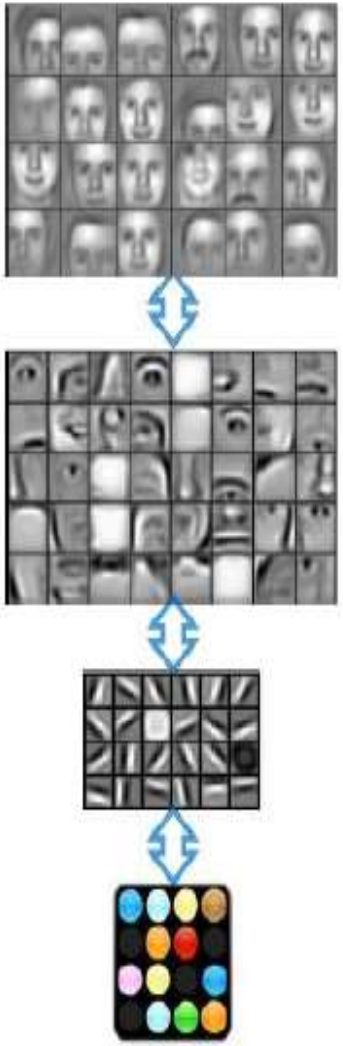
then **this** laver

finally **this** layer

Deep Architecture in the Brain



Feature representation



3rd layer
"Objects"

2nd layer
"Object parts"

1st layer
"Edges"

Pixels

Application Of Machine Learning In Cyber Security

1. Spam Filtering
2. Password Validation
3. Traffic Analysis
4. Malware Detection
5. many more…...

CAPTHA BYPASSING USING MACHINE LEARNING

- A **CAPTCHA** (an acronym for "**C**ompletely **A**utomated **P**ublic **T**urin**g** test to tell **C**omputers and **H**umans **A**part") is a type of challenge-response test used in computing to determine whether or not the user is human.

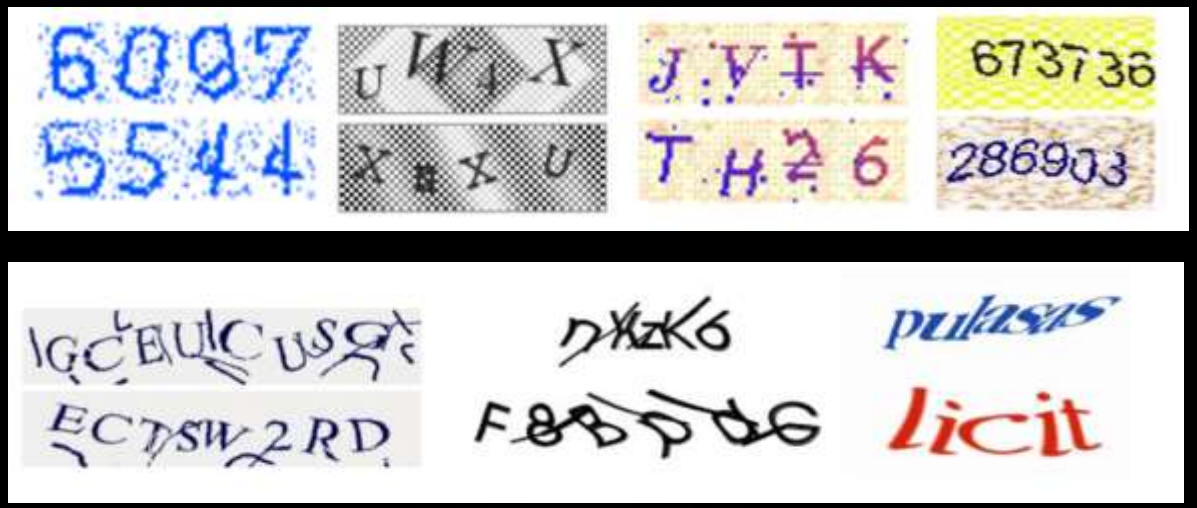


Figure 2: Similar images challenge by reCaptcha.

1. Academic studies show that ***Deep Learning based approaches*** has significantly high accuracy rate for information retrieval problems.

2. The tags retrieved by different softwares which work on ***Deep Learning Framework*** is given below :

	GRIS	Alchemy	Clarifai	TDL	NeuralTalk	Caffe
	wine and blood	wine, glass	glass, red wine, wine, merlot, liquid, bottle, still, glassware, alcohol, drink, wineglass, beverage, pouring, white wine, cabernet, taste, leaded glass, dining, party, vino	red wine, goblet, wine bottle, punching bag, beer glass, perfume, balloon	a glass of wine sitting on top of a table	red wine, wine, alcohol, drug of abuse, drug, red wine, punching bag, beaker, cocktail shaker, table lamp

3. As a consequence, with using explained methods above, referenced study has **70.78 %** successfully solving rate on image reCaptcha challenges doing this work automatically. And this system also applied to Facebook image captcha challenges, and **83.5 %** success rate has been achieved.

REFERENCES

- https://www.normshield.com/machine-learning-in-cyber-security-domain-5-captcha-bypassing/
- https://www.coursera.org/learn/neural-networks