Business School

NAME OF THE COURSE
MADSC202 DEEP LEARNING AND AI

NAME OF THE FACULTY
Dr. ATHANSIOS RIZOS

NAME OF THE STUDENTS
KUMAR GAURAV – 22026384

TITLE OF ASSIGNMENT
MID TERM ASSIGNMENT

USAGE OF DEEP LEARNING IN CRIME PREVENTION AND CYBER SECURITY

CAN REALLY DEEP LEARNING HELP IN THIS FIELD?

Image sources: https://www.wallpaperflare.com/action-crime-drama-interest-mystery-person-series-wallpaper-bxvuu
https://www.wallpaperflare.com/black-and-gray-city-buildings-person-of-interest-new-york-city-

ANSWER IS: YES

INTRODUCTION

- We all know what a crime is, don’t we?
- With increasing population and crime rate it takes more than manual work to contain crimes
- Analyzing and predicting the crime gives more insights helps the government agents to fight crime
- Deep learning is used to predict crime and help in response deployment. It is also used in cyber security

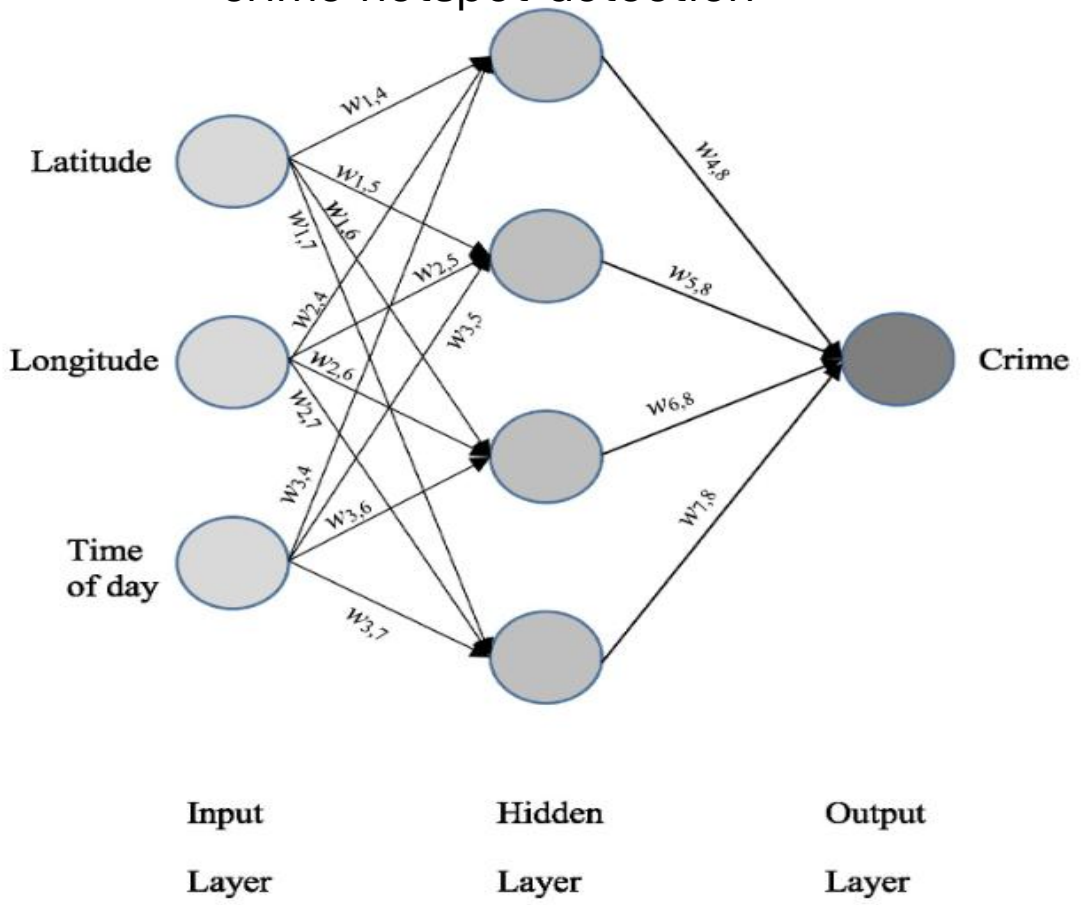
1.DEFINITION OF CASE STUDY, PROBLEM THAT EXISTS AND THE NEED OF DEEP LEARNING, AI

- Crime prevention is an important aspect to protect public safety and national security
- The problem with crime prevention is that crime is happening on a large scale and it becomes impossible to deal with it using human forces
- Hence human beings need the assistance and insights from usage of machines and technologies and therefore deep learning and AI are used in this field.
- This case study explains the need of deep learning can be used in crime prevention, assisting crime investigation and helping response deployment for crime hotspot areas
- It also helps in cyber security in preventing hackers and terrorists

NECESSITY OF DEEP LEARNING IN CRIME PREVENTION AND CYBER SECURITY

- Crime prevention cannot be fully taken on by human resources as it will be similar to searching a key in the dark
- The necessity of deep learning in this field comes into action while predicting how likely an offender will repeat the crime or identifying a criminal using image detection.
- It is also used in assisting police investigation in decision making
- Also used in crime hotspot detection
- Deep learning helps in categorising tips from emergency calls into possible crimes and helping the agents to respond to an unknown crime
- Deep learning is also used in cyber security for Intrusion detection and prevention systems, dealing with malware, spam and social engineering detection, network traffic analysis, user behaviour analytics.

Neural network example of crime hotspot detection



2.PATTERN RECOGNISTION AND WHY IT IS NOT ENOUGH

- Pattern recognistion is a method that uses machine learning algorithm to find any pattern in the data to provide useful insights
- It can be used for finger print analysis etc
- Pattern recognition is used for recognising patterns of crime happening in specific areas using latitude and longitude data which helps in declaring crime hotspot areas
- But it is not enough when it comes to image detection and potential crime prevention as it only provides insights.
- It may act as a step in crime

Example for Pattern detection for crime hotspot detection

Type of crime	Type of NN	Location	Area of prediction	References
All	MLP	Various	N/A	Altameem and Amoon, 2019
All	CNN	Rio de Janeiro	Street	Andersson et al., 2017
All	MLP	United States	N/A	Anuar et al., 2015
Motor vehicle accident	MLP	Taiwan	0.1–4.2 km	Chang, 2005
All	Supervised learning	City in NE United States	Partial city region	Corcoran et al., 2003
Violent crimes	RNN	Guatemala City	Partial city region	Cortez et al., 2018
Felonies	CNN	New York city	0.18 km^2	Duan et al., 2017
All	CNN	Chicago	Partial city region	Esquivel et al., 2019
All	RNN	San Francisco	City	Feng et al., 2019
Burglary, robbery, assault, and larceny	RNN	New York	Partial city region	Huang et al., 2018
Drug	MLP	London	Neighborhood	Intraligi and Buscema, 2013
12 Crimes	MLP	Poland	N/A	Jankowski et al., 2018
All (aggregate)	Supervised learning	India	Country	Jha et al., 2020
Larceny/theft, assault, other	CNN	San Francisco	Partial city region	Jin et al., 2020
All	CNN	Chicago	Partial city region	Kang and Kang, 2017
Crime around transportation hubs	MLP	Chicago	Transportation hubs	Kouziokas, 2017
All	RNN	Various	N/A	Krishnan et al., 2018
Car theft	CNN	Taoyuan City, Taiwan	PCR	Lin et al., 2018
All	MLP	N/A	N/A	Mao and Du, 2019
All	CNN	Los Angeles	N/A (25 pixels)	Nair and Gopi, 2020
Drugs (crack)	Supervised learning	Pittsburgh	2,150 $feet^2$	Olligschlaeger, 1997
Assault, robbery, and murder	Supervised learning	Boston	Neighborhood	Patil et al., 2020
Burglary, robbery, and battery		Belgium	200 $meter^2$	Rummens et al., 2017
Gang related	Supervised learning	Los Angeles	Partial city region	Seo et al., 2018
All	N/A	Cebu City, Philippines	750–1,000 $meters^2$	Tumulak and Espinosa, 2017
All	CNN	Los Angeles	17.8 km^2	Wang et al., 2019
All	RNN,CNN	Los Angeles	Partial city region	Wang et al., 2017a
All	RNN	Chicago	Partial city region	Wang et al., 2017b
All	CNN	San Francisco	Partial city region	Wang et al., 2020
14 Crimes	RNN, CNN	N/A	City	Wawrzyniak et al., 2018
All	CNN	County in China	County	Wu et al., 2018
All	RNN	Chicago and New York	City	Yi et al., 2019
Property crimes	Supervised learning	Boston	Partial city region	Yu et al., 2011
All	MLP	N/A	N/A	Yu et al., 2012
All	RNN	Chicago	N/A	Zhu et al., 2019
All	RNN	Portland	N/A	Zhuang et al., 2017

3. DESCRIPTION OF WHAT MACHINE LEARNING IS AND HOW IT COULD HELP ON SOLVES AND PREVENTS FROM CYBER CRIMES AND WHY IT IS NOT SUFFICIENT, AND WE NEED DEEP LEARNING AND AI TO WORK WITH IT.

What is Machine Learning?

- A subfield of artificial intelligence (AI) and computer science called machine learning focuses on using data and algorithms to simulate how humans learn, gradually increasing the accuracy of the system.

How Machine Learning could help on solves and Prevents from Cyber crimes?

- Machine learning is a subset of artificial intelligence that uses algorithms derived from previous data sets and statistical analysis to make assumptions about computer behavior. The computer can then adjust its behavior and even perform unprogrammed functions. These capabilities have made machine learning an important cybersecurity asset. .
- Detecting Threats.
- Prediction.
- Example – Antivirus

Challenges for Machine learning in cyber crime

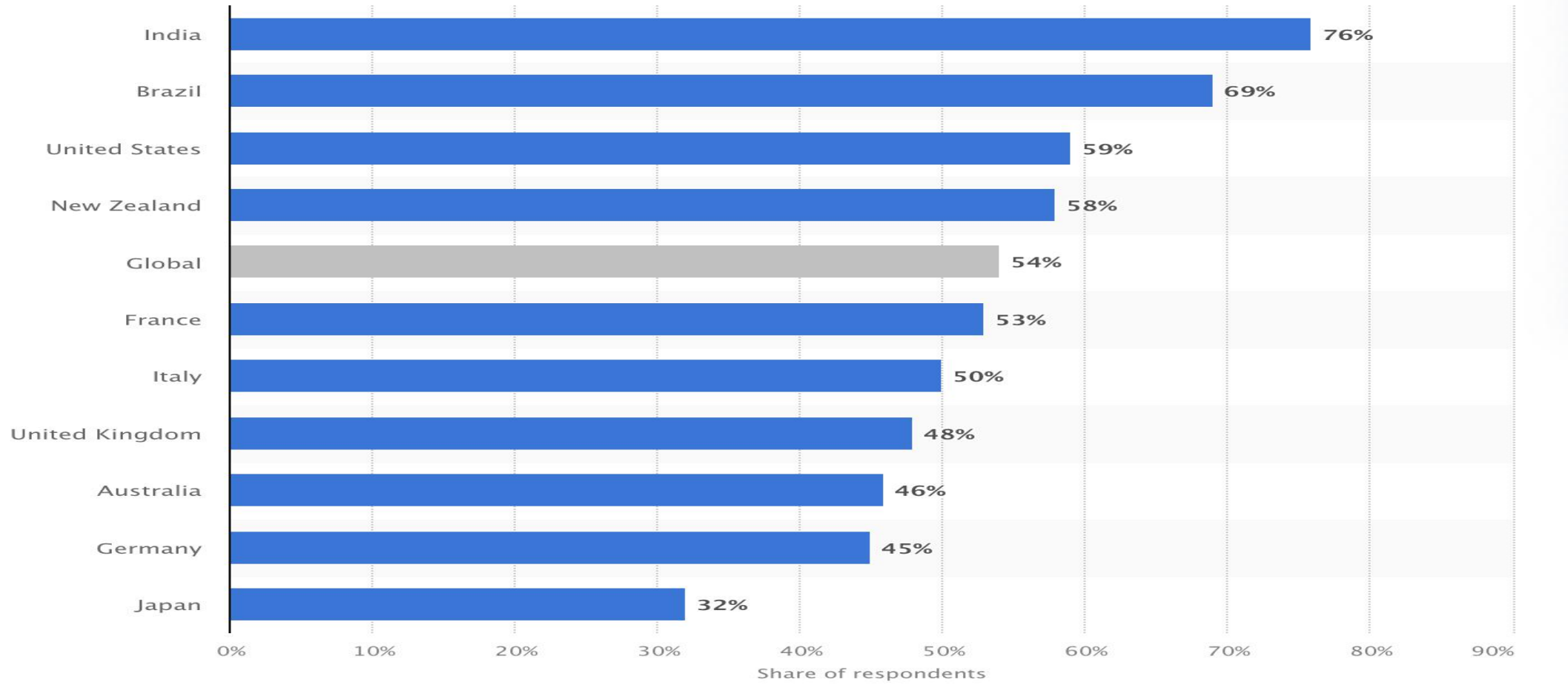
1. Increasing number of connections.

2. Machine learning data requirements.

3. Technical talent shortages

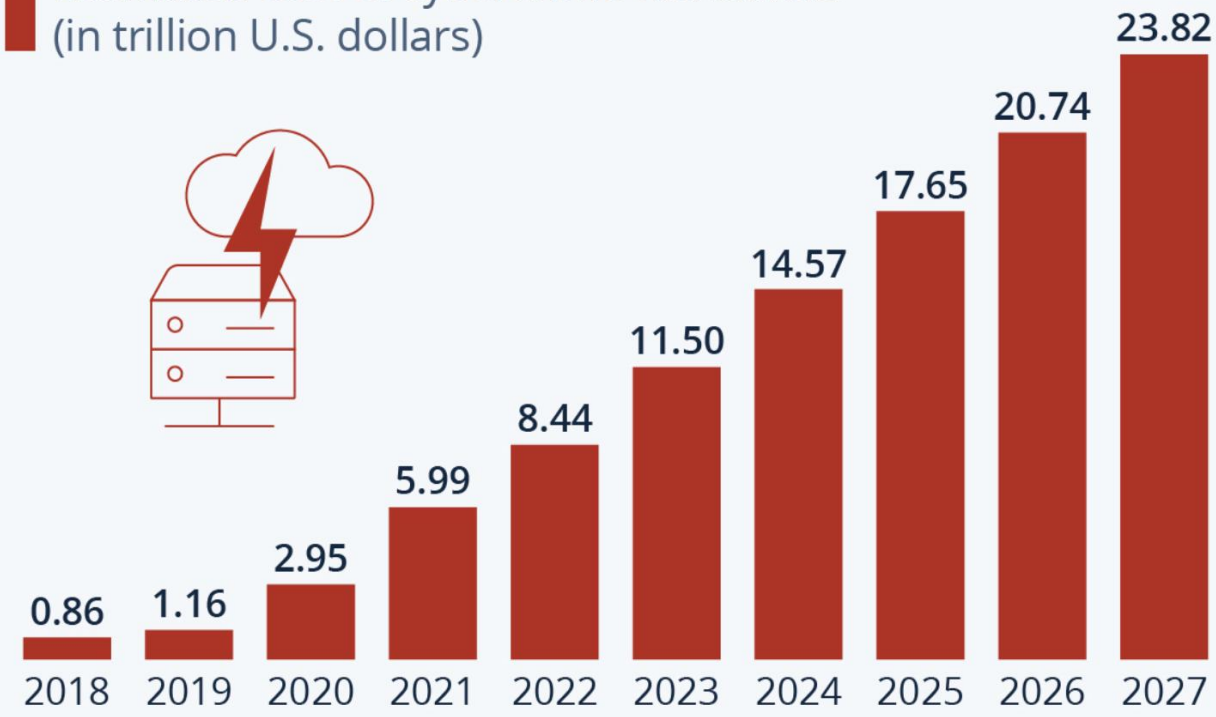
- 85 million technically skilled jobs are expected to go vacant by 2030.

PERCENTAGE OF INTERNET USERS IN SELECTED COUNTRIES WHO HAVE EVER EXPERIENCED ANY CYBER CRIME FROM NOVEMBER TO DECEMBER 2021



Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

Significance of Deep Learning and AI in preventing Cybercrime:

- AI can stop small Ransomware behaviors before it gets into the system.
- During High attack we can find the behaviour of malware.
- NLP in AI is used to collect imformation from of everywhere and make better
- AL Help in cyber security – credit card fraud detection, Spam filter, Secure user authentication, Hacking incident forecasting.

4. REASON WHY DEEP LEARNING IS MORE SUFFICIENT IN ACHIEVING SOLUTION TO PREVENT CRIMES AND CYBER SECURITY?

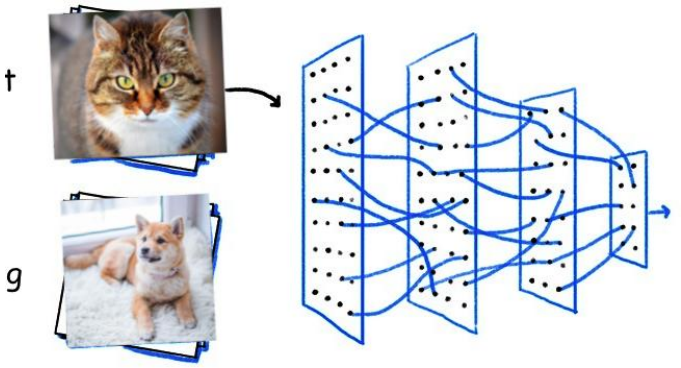
- Ability to proactively detect and stop attacks before they occur.
- Ability to analyse behaviour and patern of malware.
- Spam filter and Traffic Analysis of Network.
- Detect user behavior, Monitor Emails

5 .DESCRIBE BRIEFLY: MULTI–LAYER PERCEPTRON, DEEP NEURAL NETWORKS AND RECURRENT NEURAL NETWORKS.

- What are their similarities and differences?
- What are their advantages and disadvantages?

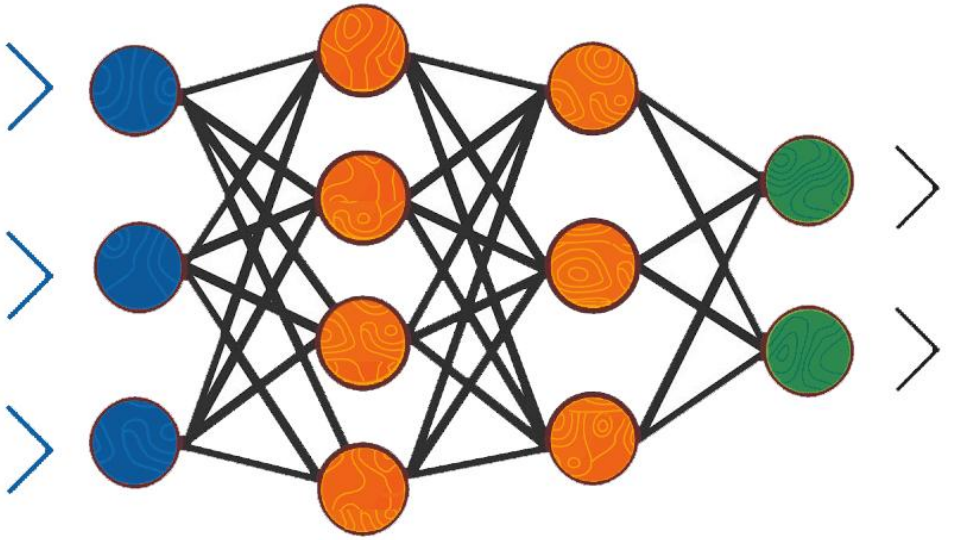
ARTIFICIAL NEURAL NETWORKS

- Machine learning models – inspired by the structure and function of the human brain.
- Applied in various applications including:



MULTI–LAYER PERCEPTRON (MLP)

- Multiple layers of artificial neurons.
- Output of one layer serves as the input to the next layer.
- Used for binary classification, multiclass classification and regression problems.
- Key feature: Capable of learning non–linear relationships between inputs and outputs.

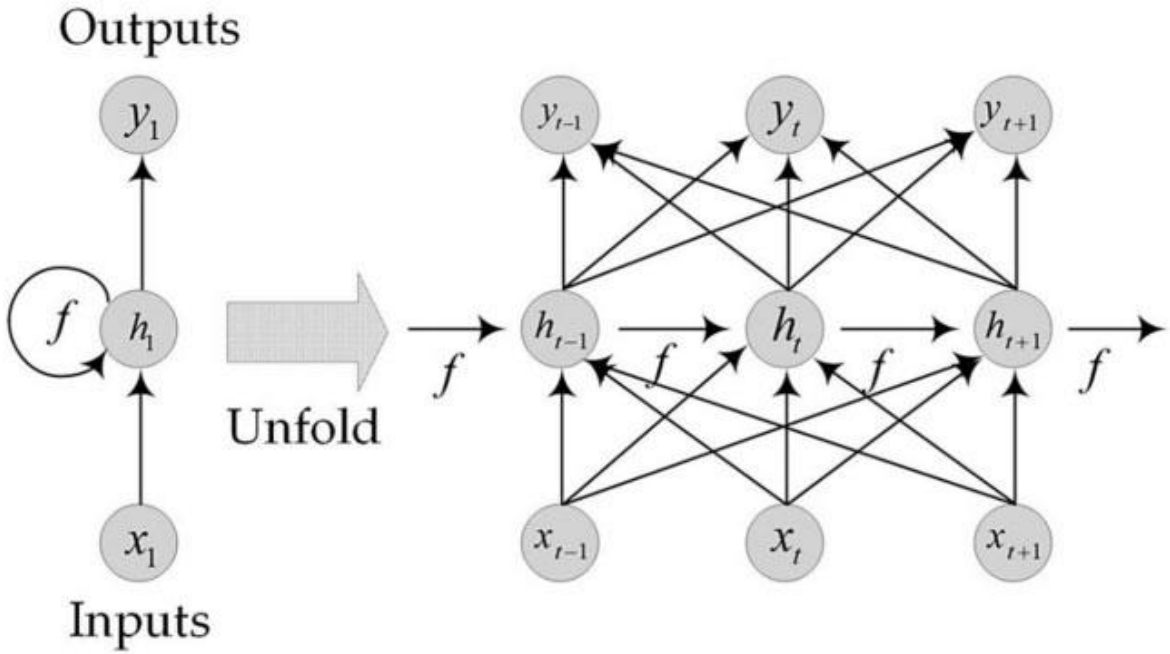


DEEP NEURAL NETWORKS (DNNS)

- A type of MLP with many hidden layers, hence the name – “Deep”
- Perform better than traditional MLPs for various applications including the ones mentioned previously; image classification, speech recognition and natural language processing.
- Key feature: Can learn hierarchical representations of data – Lower layers learn simple features and higher layers lean more complex features.

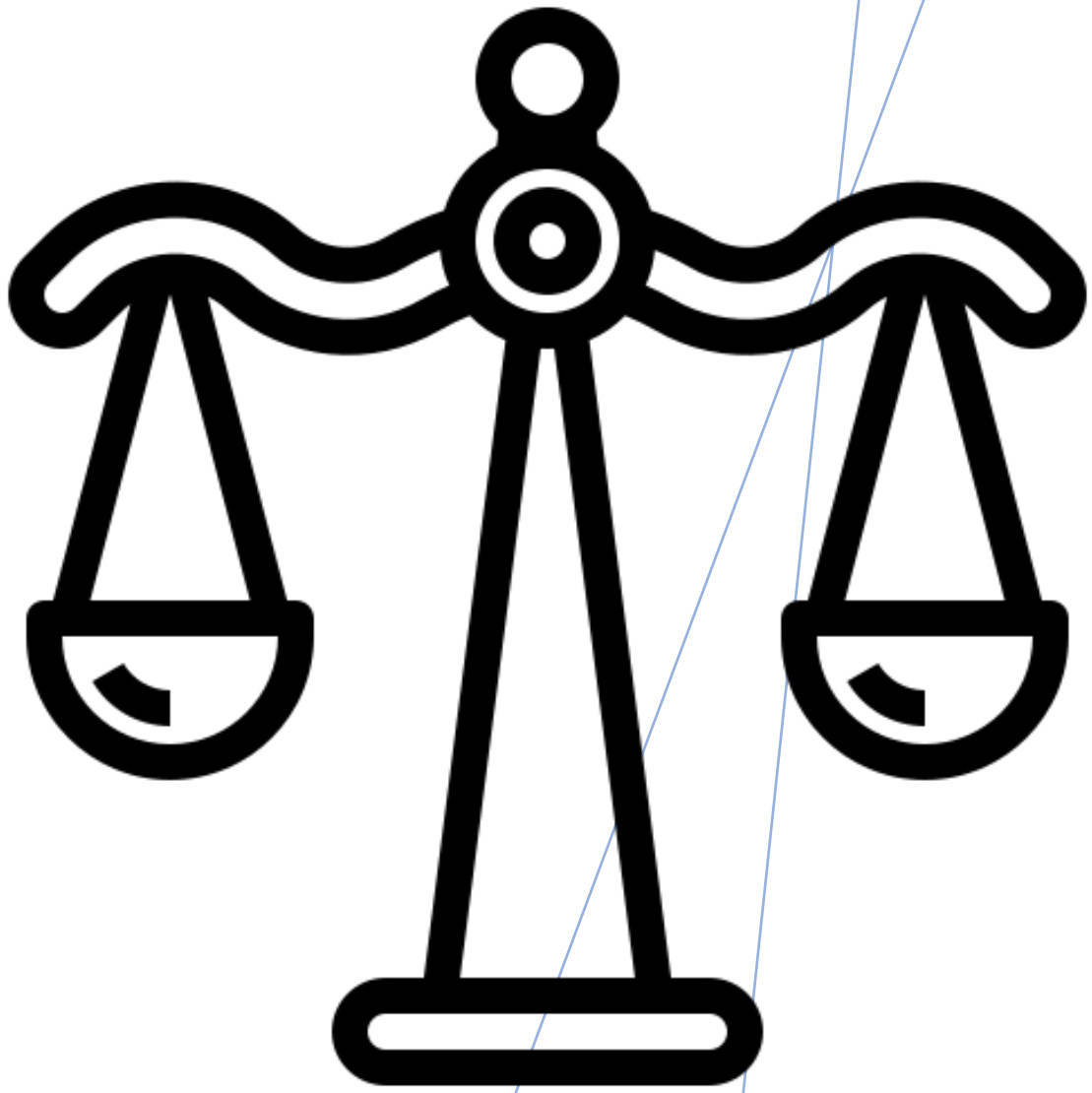
RECURRENT NEURAL NETWORKS (RNNS)

- Type of neural network that can handle sequential data.
- Time–Series Data, Speech Signals, Text Data
- Recurrent connection: The output of a hidden state at time t is fed back as input to the hidden state at time t + 1.
- Why? In order to maintain information from previous time steps and use it to make predictions for future time steps.
- Key feature: Language translation, speech recognition, etc.



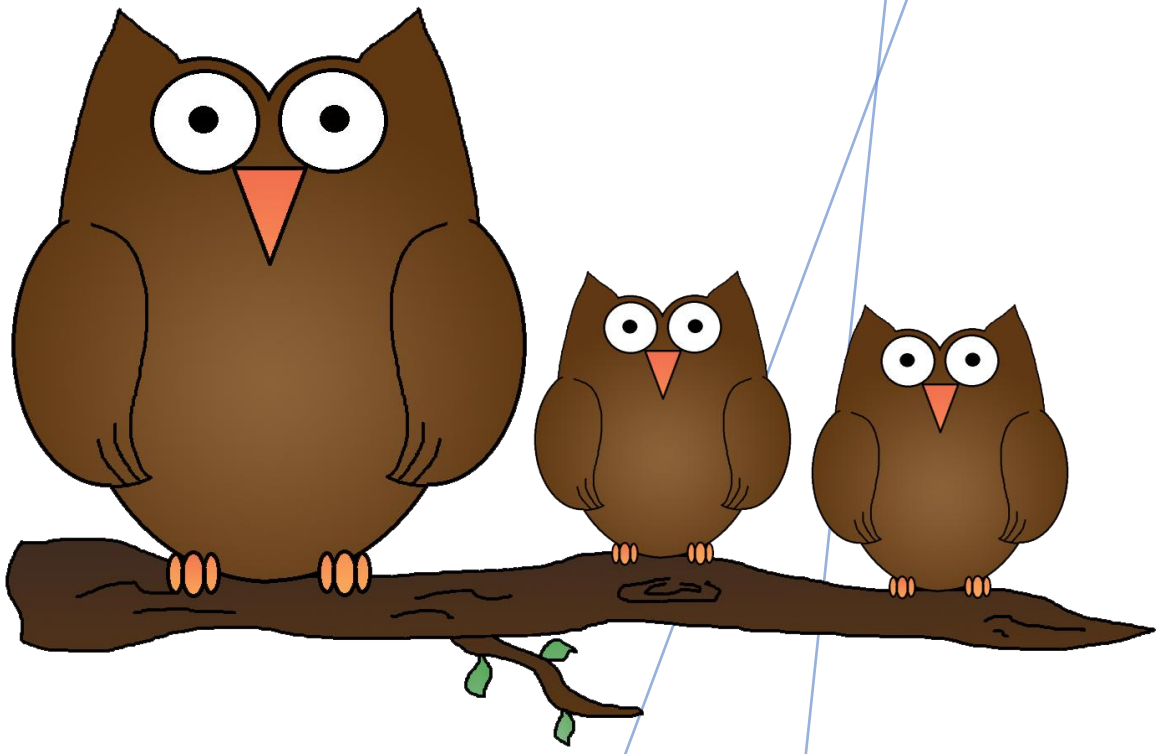
SIMILARITIES

- Capable of learning complex relationships between inputs and outputs.
- They all use gradient–based optimization to update their weights.
- For various applications: Image classification, speech recognition, and natural language processing.



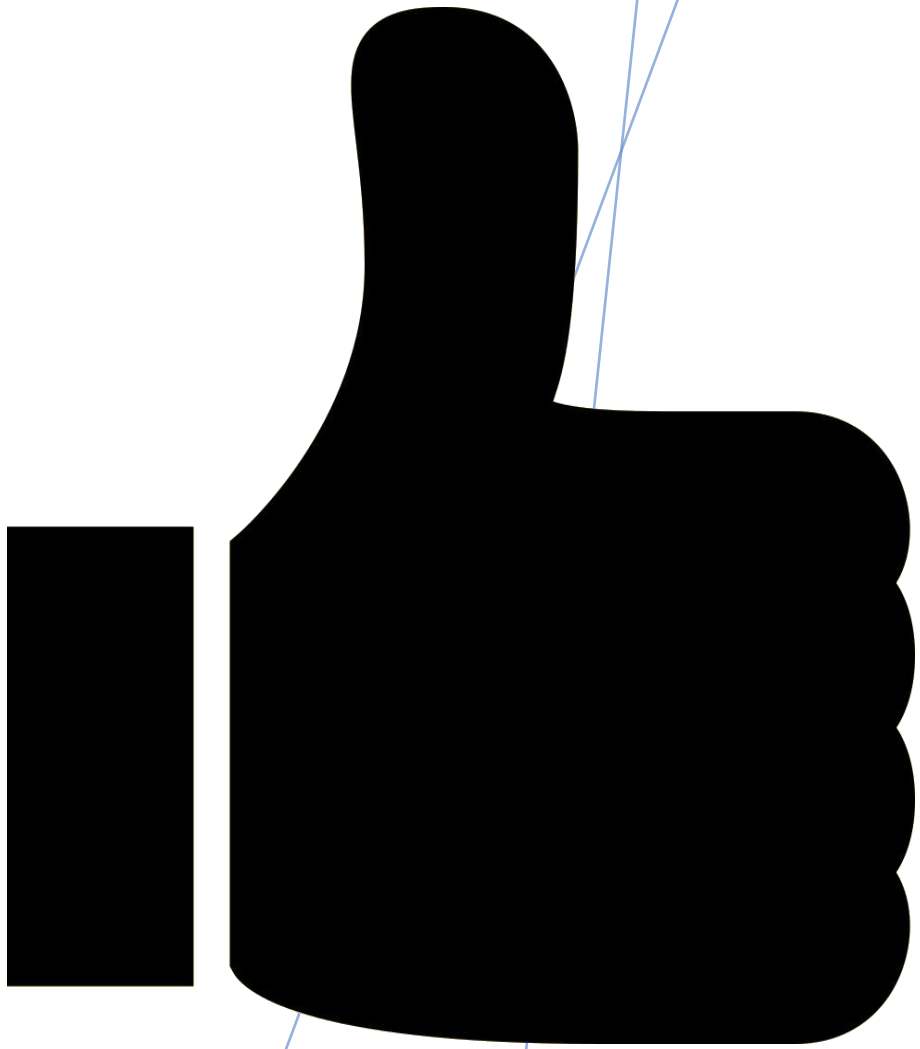
DIFFERENCES

- Limited to feedforward connections.
- DNNs can handle more complex relationships between inputs and outputs – Due to the presence of many hidden layers.
- RNNs are designed to handle sequential data and maintain information from previous time steps.



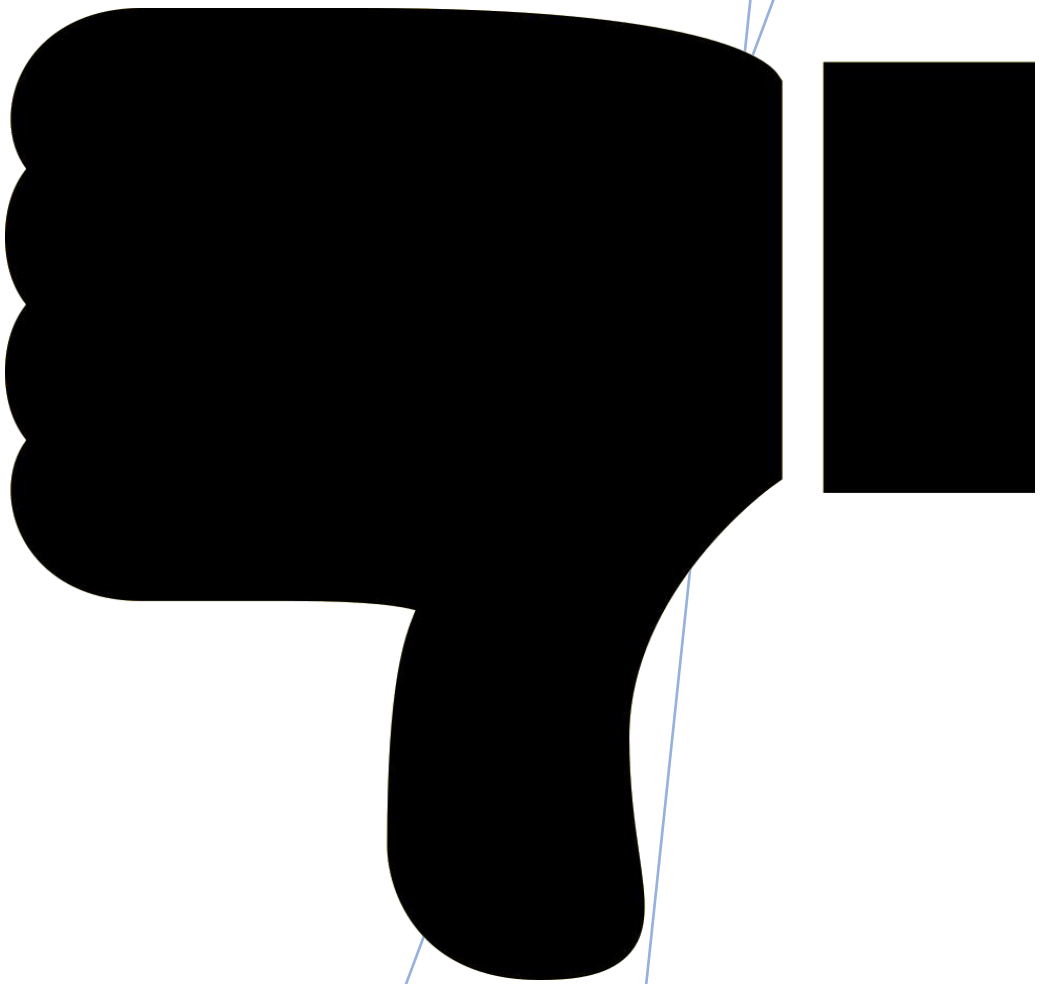
ADVANTAGES

- Handle non–linear relationships between inputs and outputs.
- Ability to learn hierarchical representations of data.
- Ability to perform well for various applications.



DISADVANTAGES

- The need of large amount of labeled training data.
- Difficulty in interpretability.
- Potential for overfitting.



6.DESCRIBE THE KEY EQUATION OF NEURAL NETWORKS AND WHAT IS THE FUNCTIONALITY OF EACH ELEMENT OF IT.

- $\alpha = \varphi\left(\sum_j w_j x_j + b\right)$

x_j the inputs to the unit.

w_j the weights.

b the bias.

ϕ the nonlinear activation function.

α the unit's activation.

- The weights are used to adjust the influence of each input on the output of the neuron.
- The bias is a constant value that is added to the weighted sum of inputs and is used to adjust overall output of the neuron.
- The non–linear activation allows to learn complex relationships between inputs and outputs.

7. DESCRIBE CONVOLUTIONAL NEURAL NETWORKS (CNNS) AND WHAT THEY OFFER VERSUS NEURAL NETWORKS.

- Convolutional Neural Networks are multi–layer neural networks used for image recognition, object detection, image classification and face recognition.

CNN consist of 3 layers;

- Convolutional layer,
- Pooling layer
- Output layer.

CONVOLUTIONAL LAYER

Convolutional layer

- CL makes a set of filters of learnable filters used to detect a pattern present in an image (input). CL uses matrix
- Filter is slided across the width and height of input file
- The process of increasing the step size by which you slide a filter over and input image is called stride.
- Increase in stride decrease the size of image causing loss of some features.
- To preserve the original size of an image, a layer of zeros is added around the edges of an image to enable filter perform full convolutional on edge of pixels. This is process called **padding**.

POOLING LAYER

Pooling layer

- A layer between convolution layers in CNN.
- It reduces the amount of parameter and computation in the network.
- Aims at reducing the spatial size of image as it is done independently on each depth of dimension.
- The commonly applied pulling method used is max pooling.

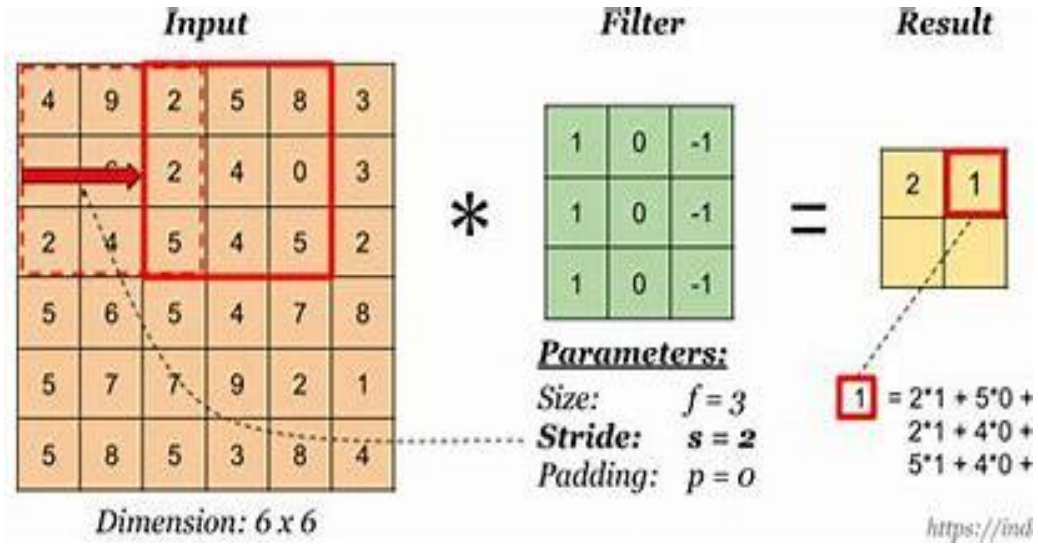
FLATTENING

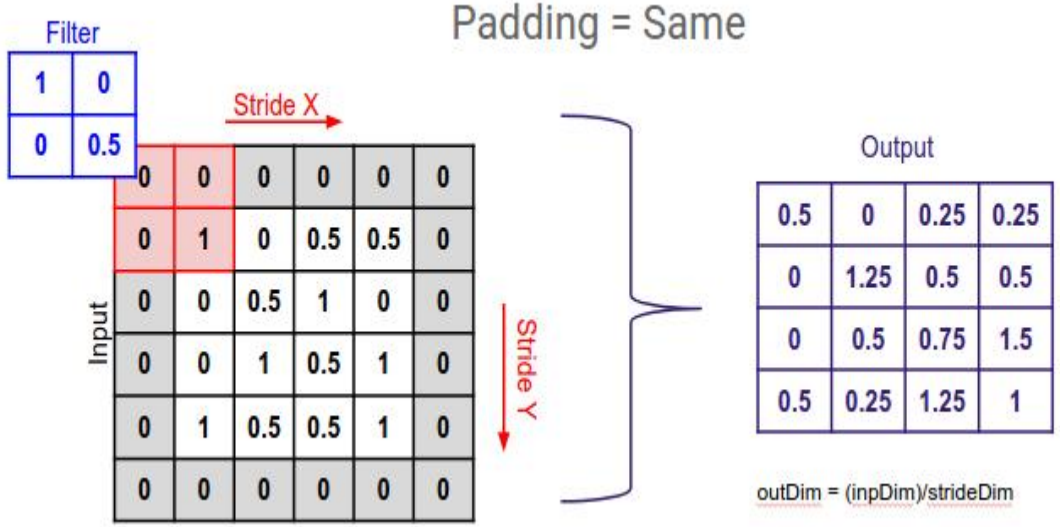
Flattening

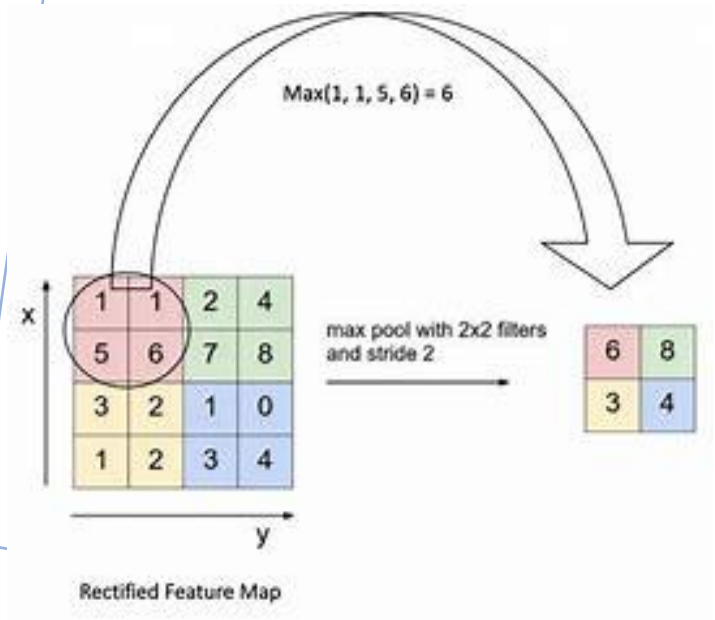
- Once the pooled featured map is obtained, it is transformed into a single column and fed to neural network for processing of output

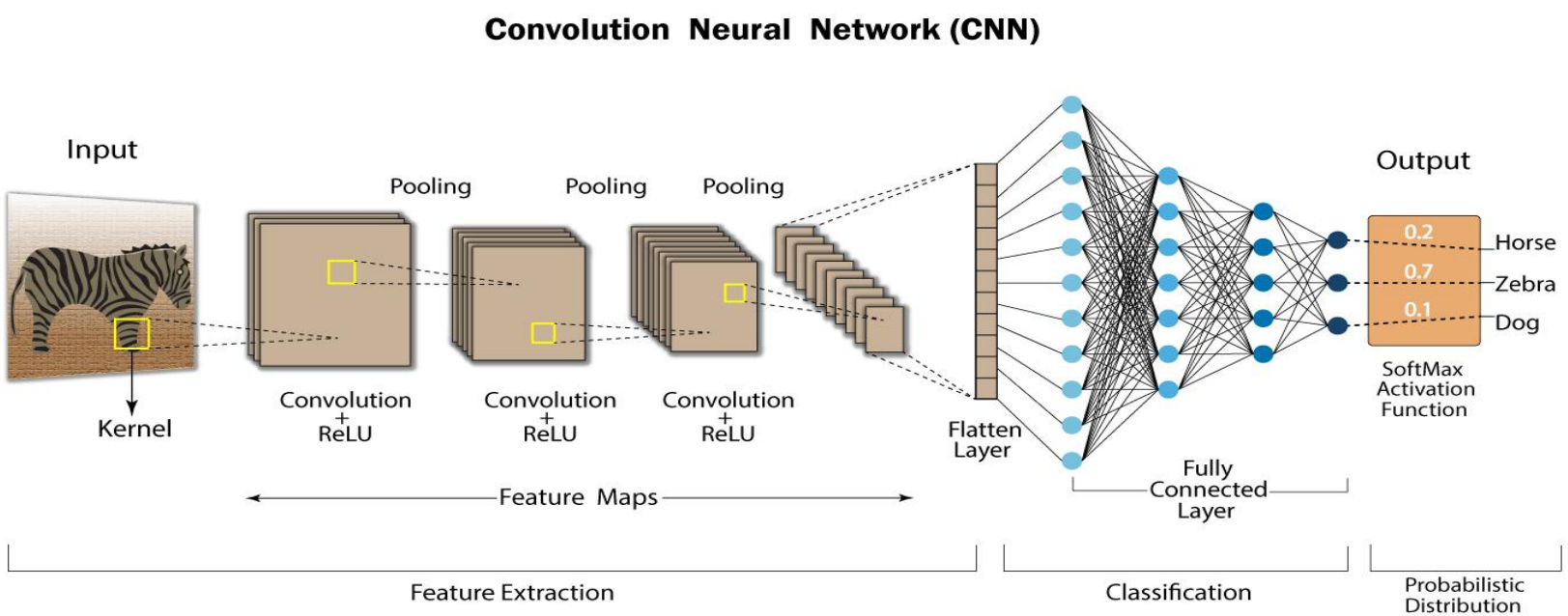
OUTPUT LAYER

- After applying multiple layers of convolution and padding, the result is output.
- Convolution and pooling layers can only reduce the number of parameters from original image.
- A fully connected layer is required to generate an output equal to the class we need.


Input
Filter
Result
Parameters:
Size: f = 3
Stride: s = 2
Padding: p = 0
Dimension: 6 x 6
= 2*1 + 5*0 +
2*1 + 4*0 +
5*1 + 4*0 +


Padding = Same
Filter
Stride X
Stride Y
Input
Output
outDim = (inpDim)/strideDim


Max(1, 1, 5, 6) = 6
max pool with 2x2 filters
and stride 2
Rectified Feature Map
x
y


Convolution Neural Network (CNN)
Input
Kernel
Pooling
Pooling
Pooling
Convolution + ReLU
Convolution + ReLU
Convolution + ReLU
Feature Maps
Flatten Layer
Fully Connected Layer
Output
Horse
Zebra
Dog
SoftMax Activation Function
Feature Extraction
Classification
Probabilistic Distribution

WHAT CNN OFFERS VS NEURAL NETWORKS:

- In neural networks, it has the ability to process temporal information a data that comes in sequence like sentences
- But CNN perform better when comes to computer vision related problems
- CNN has built in convolutional layers which helps to reduce the high dimensionality of an image without losing any information when it comes to image classification

8. DESCRIBE ONE OF THE MAIN NETWORKS FOR DL (LENET, ALEXNET ETC.) HIGHLIGHTING THEIR CHARACTERISTICS AND OVERALL ADDITIONAL OUTCOME THEY HAVE OFFERED TO THE AI.

Alex NET (2012) is a convolutional neural network used to classify and predict dataset.

Characteristics:

- The model is bigger with 7 hidden layers, 650k units, 60M parameters.
- Uses GPU to boost performance hence faster training
- More data (106 images instead of 103)

The goal of ILSVRC is to promote the development of better computer vision and deep learning.

In 2012 AlexNET competed in annual ImageNet Large scale Visual Recognition Challenge (ILSVRC). The main ideas included:

- Deeper network
- Stacked convolutional layers with smaller filters (+ nonlinearity)
- Detailed evaluation of all components

Implementation of the ideas resulted to Improved ILSVRC top-5error rate to 6.7%.

CONCLUSION

- Deep learning and AI are largely growing field and lot more can be done in te future as it becomes one of the best methods in all fields
- Deep learning and AI helps contributes more towards crime prevention and cyber security
- Human forces use the insights to prepare and respond to the attacks
- Key take away would be how these techniques are used in real time

REFERENCES

- Walczak, S (2021) 'Predicting Crime and Other Uses of Neural Networks in Police Decision Making', *Frontiers in Psychology*, Available at: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.587943/full
- Fichtner, E (2022) '5 Amazing Applications of Deep Learning in Cybersecurity',*Datto,* Available at: https://www.datto.com/blog/5-amazing-applications-of-deep-learning-in-cybersecurity
- Browniee, J (2019) 'A Gentle Introduction to the ImageNet Challenge (ILSVRC)',*Machine Learning Mastery,* Available at: https://machinelearningmastery.com/introduction-to-the-imagenet-large-scale-visual-recognition-challenge-ilsvrc/