2.3.3.4 Transformers ………………………………………………………..46

Deep learning applications ............................................................................. 49

Conclusion ………

**Chpter2**

**2.1Introduction**

The field of **AI**, using the strongest tools available in computer science, works toward imitating intelligence in a human being. Such systems can perform various tasks usually attributed to human cognitive abilities, such as decision-making, pattern recognition, and problem-solving. AI has come a long way over the years, fueling innovations such as self-driving cars, intelligent virtual assistants, and highly advanced recommendation systems, hence revolutionizing industries and daily life.

In this chapter, basic machine-learning (ML) methodologies are looked into, a major subfield of AI. We will describe the three paradigms of learning: supervised learning, unsupervised learning, and reinforcement learning. Standard algorithms in machine learning will also be addressed followed by a transition into deep learning (DL), which is an enhanced version of ML that exploits multi-layer neural networks. The immediate goal in this instance is to firmly establish some of the fundamental concepts of these methods and their frameworks, in preparation for their application to real-world problems, including cybersecurity and SQL injection detection.

2.2 ma**chine learning**

The field of machine learning is concerned with the question of how to construct computer programs that automatically improve with experience. In recent years many successful machine learning applications have been developed, ranging from data-mining programs that learn to detect fraudulent credit card transactions, to information-filtering systems that learn users' reading preferences, to autonomous vehicles that learn to drive on public highways. At the same time, there have been important advances in the theory and algorithms that form the foundations of this field.(1)

[1]( Mitchell, T. M, Machine Learning. McGraw-Hill, 1997.)

**Or wla**

Machine learning (ML) is a branch of artificial intelligence focused on developing algorithms and systems that can learn and improve from experience without being explicitly programmed. This field seeks to create computer programs capable of adapting to new data, identifying patterns, and making data-driven decisions. Over the years, machine learning has enabled groundbreaking applications across various domains, such as fraud detection systems that identify suspicious credit card transactions, personalized recommendation engines that adapt to user preferences, and self-driving cars that navigate complex environments. These advancements have been driven by significant progress in the theoretical foundations and algorithmic techniques that underpin machine learning(1) (2) mixed

* Mitchell, T. M. (1997). Machine Learning. McGraw-Hill.9(1)
* Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.(2)

**2.2.2 Machine Learning Types**

Whatever may be the nature and form of learning, machine learning always refers to a very wide-open field wherein computers learn from data to improve performance over time. **In machine learning, this kind of learning process is usually classed into three main parts which are supervised learning, unsupervised learning, and reinforcement learning**. Each type serves a certain distinct purpose and is used with certain types of problems. Besides those three types, hybrid approaches such as commodity inclusion and special techniques have also emerged to maintain and solve more complex issues.

Kbira bzf 9adrin na9sou fiha

**2.2.1.1 Supervised Learning: Learning from Labeled Data**

Supervised learning is a fundamental paradigm in machine learning where labeled data is used to train models. Under this paradigm, the input data have known target outputs, thereby allowing the model to learn the relationship between input and output. By spotting patterns and correlations in data, supervised learning algorithms can then make predictions or determine classifications on fresh, never-before-seen data.

**Main Applications:**

Examples of supervised learning applications are:

**Classification:**

In a classification problem, the intention is to assign a set of data points to defined predefined categories or labels. Examples include classifying an email as spam or not spam with the model trained, or diagnosing different medical conditions based on patient data. The well-known algorithms used for classification are decision trees, support vector machines, and neural networks.

**Regression**:

The regression task is concerned with the prediction of a continuous quantity. This may include estimating house prices, stock market trends, and variations in temperature. Algorithms such as linear regression and polynomial regression are commonly used in this scenario.

**2.2.1.2 Unsupervised Learning: Discovering Hidden Patterns**

Unsupervised learning is a type of machine learning ([ML](https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML)) technique that uses artificial intelligence ([AI](https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence)) algorithms to identify patterns in data sets that are neither classified nor labeled. Unsupervised learning models don't need supervision or preexisting categories while training data sets, making them ideal for discovering patterns, groupings and differences in [unstructured data](https://www.techtarget.com/searchbusinessanalytics/definition/unstructured-data). It's well-suited for processes such as [customer segmentation](https://www.techtarget.com/searchcustomerexperience/definition/customer-segmentation), exploratory data analysis, [dimensionality reduction](https://www.techtarget.com/whatis/definition/dimensionality-reduction) and image recognition.

Unsupervised learning algorithms can classify, label and group the data points contained within data sets without requiring any external guidance to perform that task. In other words, unsupervised learning enables a system to identify patterns within data sets on its own.

In unsupervised learning, an AI system groups unsorted information according to similarities and differences even though no categories are provided.

AI systems capable of unsupervised learning are often associated with [generative learning models](https://www.techtarget.com/searchenterpriseai/definition/generative-modeling), although they might also use a retrieval-based approach, which is most often associated with [supervised learning](https://www.techtarget.com/searchenterpriseai/definition/supervised-learning). [Chatbots](https://www.techtarget.com/searchcustomerexperience/definition/chatbot), self-driving cars, [facial recognition](https://www.techtarget.com/searchenterpriseai/definition/facial-recognition) programs, [expert systems](https://www.techtarget.com/searchenterpriseai/definition/expert-system) and robots are among the systems that use supervised or unsupervised learning approaches. Unsupervised learning is also known as *unsupervised machine learning*. (3)

(3)( https://www.techtarget.com/searchenterpriseai/definition/unsupervised-learning)

**2.2.1.3 Reinforcement Learning: Learning Through Interaction**

Reinforcement learning problems involve learning how to map situations to actions to maximize a numerical reward signal. These problems are inherently closed-loop, as the system’s actions influence its future inputs. Unlike other forms of machine learning, the learner is not explicitly told which actions to take but must discover the best ones through trial and error. In more complex scenarios, actions impact not only immediate rewards but also future states and long-term rewards, making decision-making more challenging (4)

(4)( Reinforcement Learning: An Introduction Second edition, in progress Richard S. Sutton and Andrew G. Barto c 2014, 2015).

**2.2.2 Machine learning algorithms**

**2.2.2.1** Logistic regression

Logistic regression is a supervised machine learning algorithm used for classification tasks, predicting the probability that an instance belongs to a specific class. It is a statistical method that analyzes the relationship between independent variables and a categorical outcome.

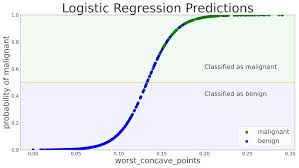
Unlike linear regression, logistic regression applies the sigmoid function to map input values to a probability ranging between 0 and 1. Instead of fitting a regression line, it models an "S"-shaped curve to distinguish between classes.

**Key Points:**

* Logistic regression predicts the output of a categorical dependent variable.
* The outcome is discrete (e.g., Yes/No, 0/1, True/False) but represented as a probability between 0 and 1 (5)

(5)( https://www.geeksforgeeks.org/understanding-logistic-regression/).

**Ttbdl ay flou**

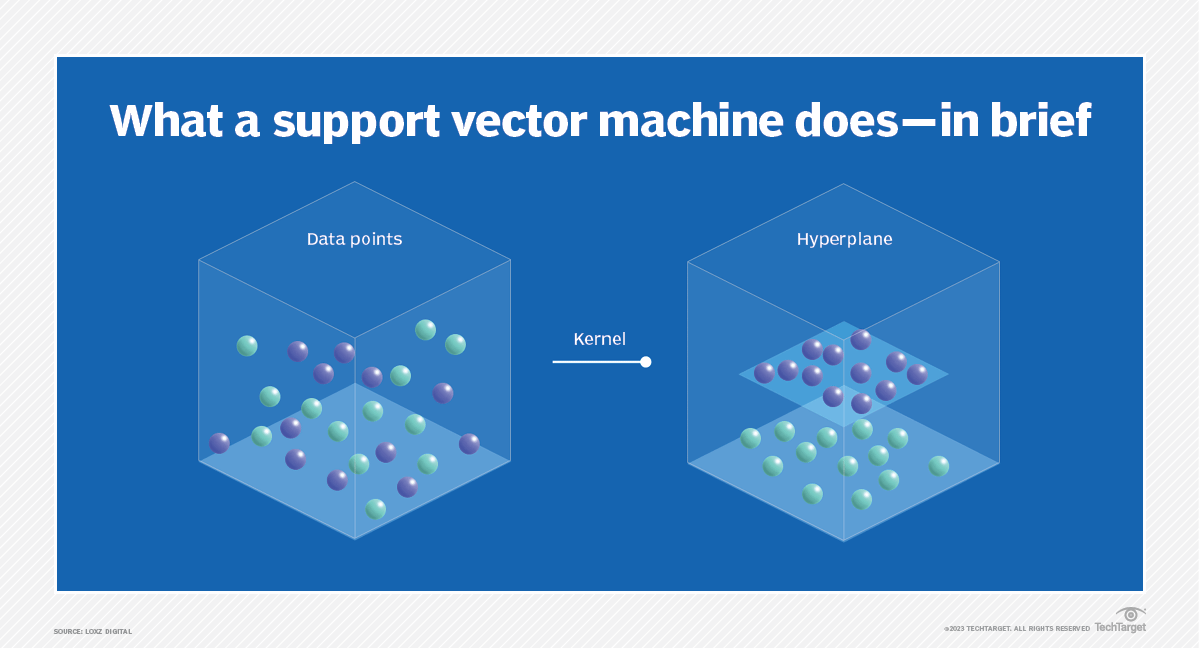


2.2.2.2 SVM

SVM (Support Vector Machine) is one of the supervised learning techniques employed for classification and regression tasks. The classification margin between various classes is maximized by finding the optimal hyperplane. Among the significant concepts are \*\*support vectors\*\* (data points that are critical in defining the margin), \*\*hyperplane\*\*, and \*\*kernel functions\*\* (which map the data into higher dimensions for separating it nonlinearly).

SVM uses three kernels-linear SVM, polynomial SVM, and artillery -to handle \*\*linearly separable\*\* and \*\*non-linearly separable\*\* data. It employs a soft margin to maximize the margin and add a penalty when data points are misclassified. The optimization problem is reduced to minimizing a loss function while ensuring that the classification is being done correctly. The \*\*dual problem\*\* allows efficient computation and non-linear classification by means of \*\*kernel trick\*\*. SVM is widely adopted in text classification, image recognition, and bioinformatics.(4)

(4)( https://www.geeksforgeeks.org/support-vector-machine-algorithm/)



**Meme hadi ida lguina makhir**

Figure(<https://www.techtarget.com/whatis/definition/support-vector-machine-SVM#:~:text=A%20support%20vector%20machine%20(SVM)%20is%20a%20type%20of%20supervised,data%20set%20into%20two%20groups.)>

**2.2.3 Machine learning applications**

**Game Playing**- RL is being used to create systems that can contrast and even surpass human capabilities in playing games like chess, Go, and video games (AlphaGo, for example).

**Robotics**: Training robots to be able to perform complex tasks such as walking or grasping objects.

**Autonomous Systems**: To be able to move safely and efficiently by itself, self-driving cars require reinforcement learning.

**APPlications Pas finis**

**2.3 Deep Learnig**

Deep learning is a subfield of machine learning that employs deep neural networks for analyzing and interpreting complex data. Such networks are modeled after the human brain and allow the computer to identify patterns and relationships without human intervention in large amounts of unstructured information. The deep learning model is continuously improving its accuracy by tuning internal parameters with training**.**

Deep learning models can be trained to perform classification tasks and recognize patterns in images, text, audio, and other types of data. This technology also enables automation of tasks that typically require human intelligence, such as image description and audio transcription. Where human brains have millions of interconnected neurons that work together to learn information, deep learning features neural networks constructed from multiple layers of software nodes that work together. (5)

This technique has achieved astonishing outcomes in image recognition, understanding natural language, and processing speech, making it the foundation of contemporary artificial intelligence systems.

(5)( <https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network>)

**2.3.1 Artificial Neural Networks (ANNs)**

Artificial Neural Networks (ANN) are inspired by the way biological neural system works, such as the brain process information. The information processing system is composed of a large number of highly interconnected processing elements (neurons) working together to solve specific problems. ANNs, just like people, learn by example. Similar to learning in biological systems, ANN learning involves adjustments to the synaptic connections that exist between the neurons.



Figur (6)

Here [X1, X2, X3] are the input features to the neural networks represented as X. Whereas the superscript [1] is used to denote the layer. The weights are denoted by [W1, W2, W3] associated with each connection to the neuron from the input of that particular layer. The bias is represented by b associated with the neuron. “z” is the weighted sum of inputs added with the bias which is linear in nature. “a” is the activation function that is applied to z to add non-linearity as complex models can't be represented as a line. (6)

(6)( <https://medium.com/@anushruthikae/basic-notations-and-representation-neural-networks-d46a1be97471>)

The activation function is applied to the weighted sum of inputs to the neuron, including the bias term, and the resulting value becomes the neuron's output, which is then passed to the next layer. Its primary role is to introduce non-linearity into the model, allowing the network to learn complex patterns and approximate any arbitrary function. In this one-layer neural network architecture, the output of the activation function in layer [1] serves as the final output, denoted as y’. This output is used to compute the loss function, L(a, y), which measures the deviation between the predicted and actual output. This deviation is crucial for backpropagation and optimization, which will be discussed in later sections.(6)



An artificial neural network is primarily composed of three layers: the input layer, one or more hidden layers, and the output layer. These layers collectively work to process the information and yield meaningful predictions.

**Input layers** serve as the entry point for data into the neural network. Each neuron in this layer corresponds to either a specific feature of the input dataset or an input vector. For instance, in an image classification problem, all input neurons may specify the intensity of each individual pixel. This layer exists purely for the purpose of passing on the raw input values to the next layer without change.

**Hidden layers** serve to process and transform information passed to them from the input layer. They are called hidden since nothing about their inner workings can be observed directly. In a typical hidden layer, a neuron takes in inputs from the preceding layer, applies a weighted summation, adds a bias, and applies an activation function on the result. Depending on the complexity of the task, a network can have varying numbers of hidden layers with varying numbers of neurons in each layer. DNNs having multiple hidden layers are quite popular in applications such as image recognition, speech processing, and natural language understanding since they can efficiently extract many complex patterns from the data.

**The output layer is** the final layer of the network that provides the prediction made by the model. The structure of this layer is based on the solved problem. In the case of classification networks, each output neuron corresponds to one class; in regression problems, usually only one output neuron provides a continuous value: an activation function is then used in the output layer according to the type of task, e.g., softmax for multi-class classification and any linear function for regression.

These layers are interconnected by **weighted links** that determine the importance of each input. The weights are adjusted during training through a system called **backpropagation** whereby errors are carried backward from the output to the hidden layers enabling the network to learn and enhance its performance with time. Persistent adjustments of these weights equate to an increasing ability of the neural network to predict correctly.

or nkhdmou b article li kayn hna (<https://www.v7labs.com/blog/neural-networks-activation-functions>)

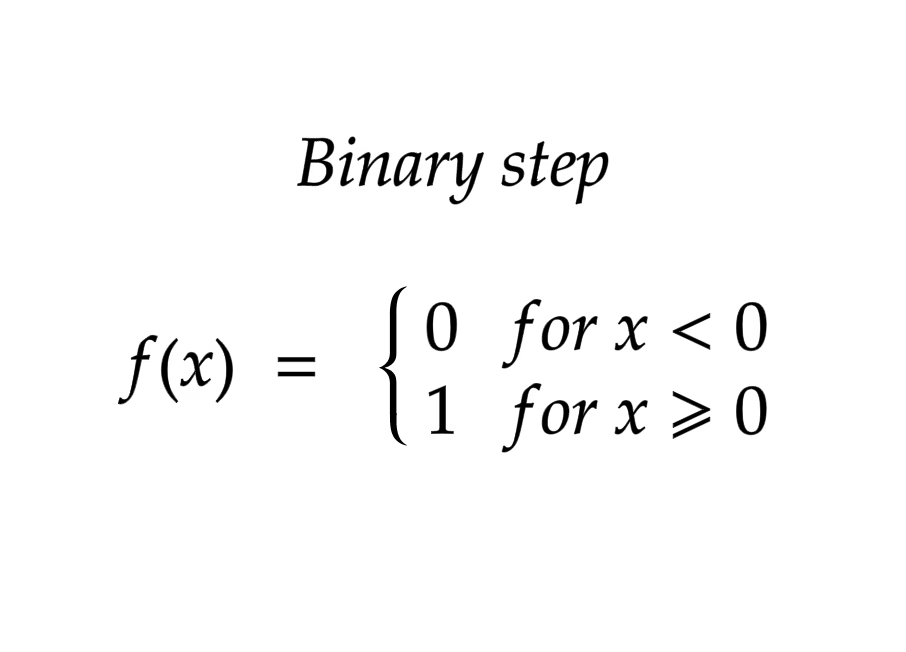
**2.3.2 Activation functions**

Activation functions play a fundamental role in neural networks by determining how neurons process input data and transfer information to subsequent layers. The choice of activation function significantly influences the network's performance and learning capability

**1. Binary Step Function**

The Binary Step Function is a threshold-based activation function that decides whether a neuron is activated or remains inactive. If the input surpasses a predetermined threshold, the neuron is activated; otherwise, it stays dormant, meaning it does not contribute to the next layer.





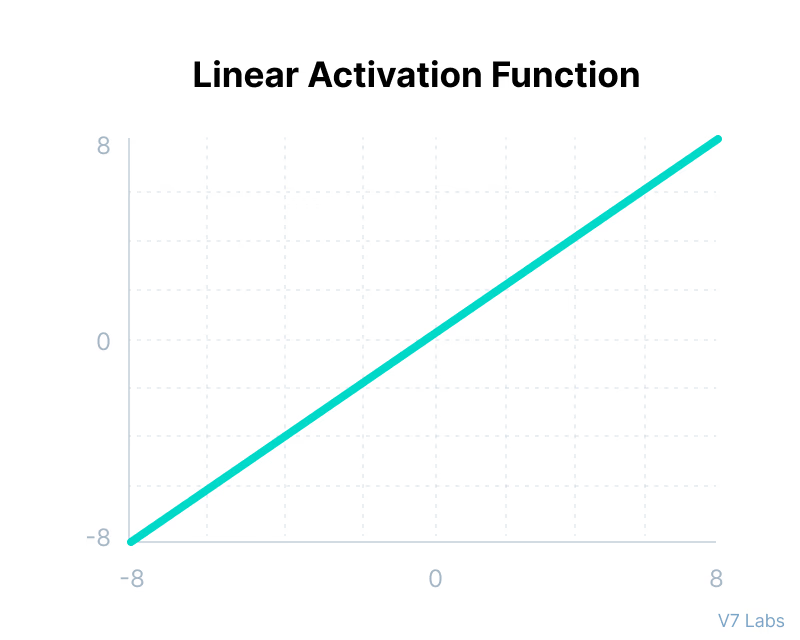
**Limitations:**

* It provides only binary outputs, making it unsuitable for tasks requiring multi-class classification.
* Since its derivative is zero, it obstructs the backpropagation process, hindering learning. (7)

(7)( [https://www.v7labs.com/blog/neural-networks-activation-functions#3-types-of-neural-networks-activation-functions](https://www.v7labs.com/blog/neural-networks-activation-functions" \l "3-types-of-neural-networks-activation-functions))

**2. Linear Activation Function**

Also known as the identity function, the Linear Activation Function outputs the input value without modification, allowing direct propagation of signals through the network.



**Disadvantages:**

* Backpropagation is ineffective since the function's derivative is constant and does not depend on input values.
* Using a linear activation function across multiple layers results in a network that is functionally equivalent to a single-layer model. (7)

### 3. Non-Linear Activation Functions (7)

**. Non-Linear Activation Functions**

A network using only a linear activation function is essentially equivalent to a simple linear regression model, limiting its ability to capture complex patterns in data. Non-linear activation functions enable deep networks to model intricate relationships between inputs and outputs.

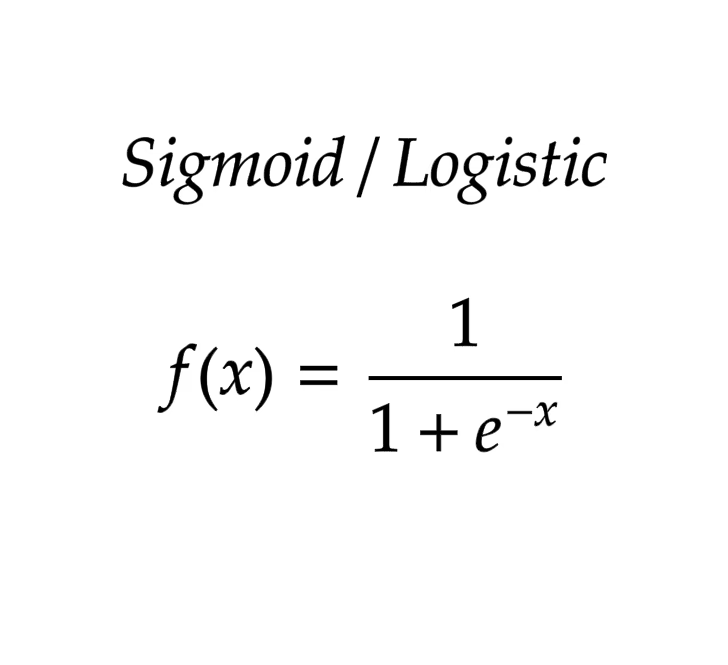
**Advantages:**

* They allow backpropagation by ensuring derivatives depend on input values, facilitating effective weight adjustments.
* They enable the creation of deep networks, where transformed outputs from one layer pass non-linearly to the next.

**4. Sigmoid (Logistic) Activation Function(7)**

This function takes any real value as input and outputs values in the range of 0 to 1.making it useful for probabilistic models and binary classification tasks.

 The larger the input (more positive), the closer the output value will be to 1.0, whereas the smaller the input (more negative), the closer the output will be to 0.0, as shown below.

****



**Advantages:**

* Ideal for probability-based applications due to its constrained output range.
* It is differentiable, ensuring smooth gradient updates during optimization.

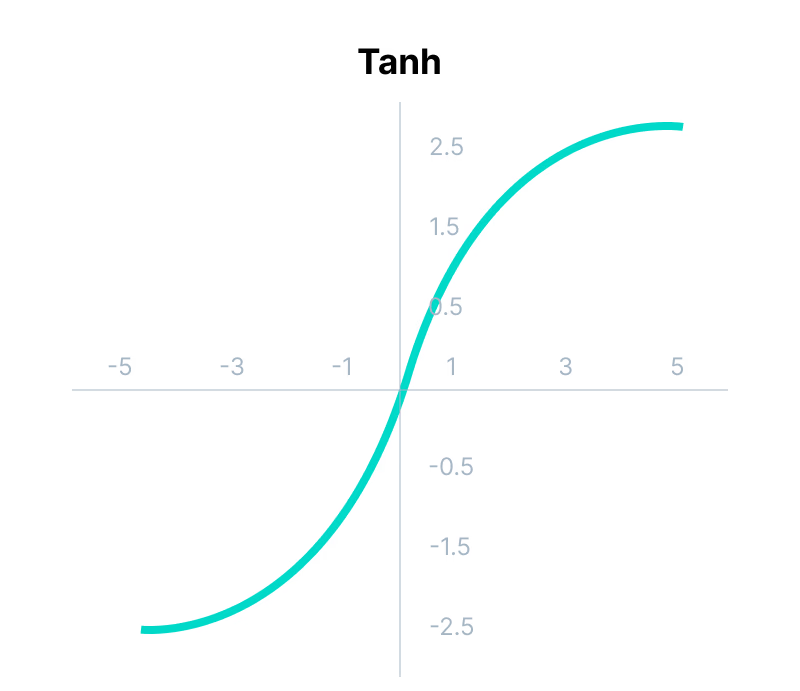
**Limitations:**

* The **vanishing gradient problem** occurs as extreme values lead to near-zero derivatives, hindering learning.
* It is not zero-centered, which can slow down the training process.

**5. Tanh (Hyperbolic Tangent) Function(7)**

The Tanh function is similar to the sigmoid function but maps input values to a range between -1 and 1, providing stronger non-linearity.

****



**Advantages:**

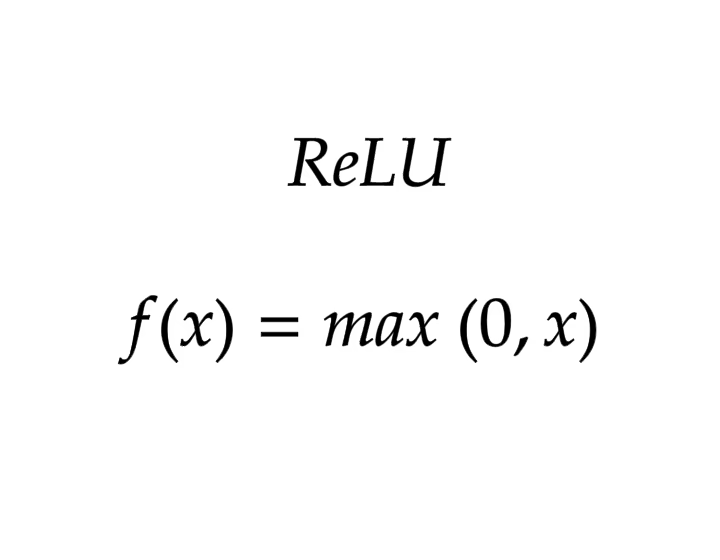
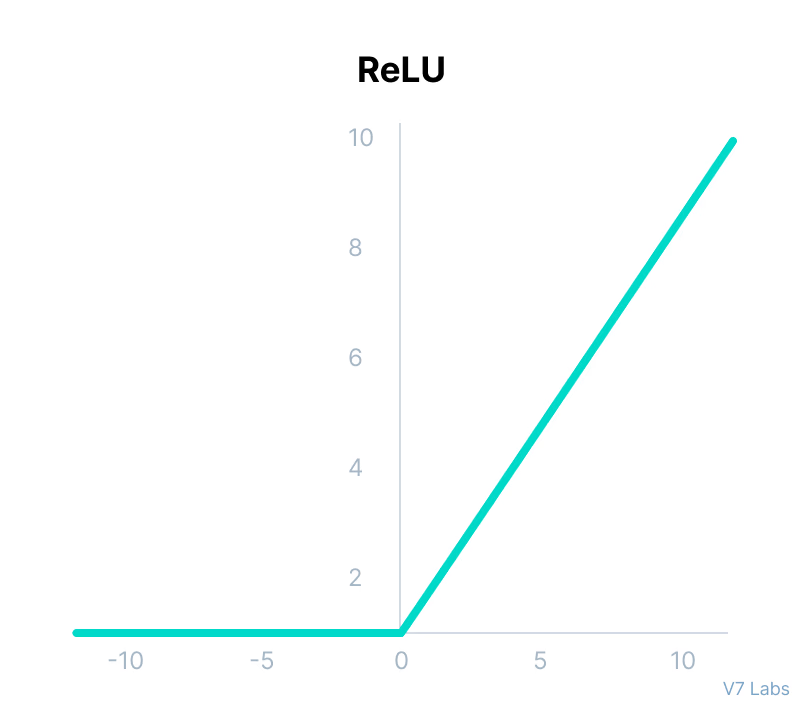
* Outputs are zero-centered, improving convergence speed in deep networks.
* Often used in recurrent neural networks (RNNs) and convolutional neural networks (CNNs).

**Limitations:**

* Still suffers from the **vanishing gradient problem**, albeit less than the sigmoid function.

**6. ReLU (Rectified Linear Unit) Function(7)**

ReLU is one of the most commonly used activation functions in deep learning. It introduces non-linearity by outputting zero for negative inputs while retaining positive values unchanged.



**Advantages:**

* Computationally efficient, as only a subset of neurons activate at a time.
* Helps accelerate gradient descent co=nvergence due to its non-saturating nature.

**Limitations:**

* **Dying ReLU Problem**: Neurons can become permanently inactive for negative inputs, preventing further updates.

**Bzf wa9ila**

**2.3.3 Deep learning architectures**

Deep learning has enjoyed tremendous advancement in the last few years, serving as the major pillar for innovation in many different fields. Each architecture is designed for particular problems, with the performance in each case optimized for the specific needs of the task at hand.

Over the years, many deep learning models have been developed, often extending some fundamental designs. Among these, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory networks (LSTMs) are the most commonly known. In their respective areas, these architectures have been very efficient, thereby enabling progress in image recognition, sequence modeling, and time series analysis.

**2.3.3.1 Recurrent Neural Networks**

Recurrent Neural Networks (RNNs) are neural networks designed to recognize patterns in sequences of data. They’re used for identifying patterns such as text, genomes, handwriting, or numerical time series data from stock markets, sensors, and more.

Unlike traditional [feedforward neural networks](https://www.analyticsvidhya.com/blog/2022/03/basic-introduction-to-feed-forward-network-in-deep-learning/" \t "_blank), where inputs are processed only once in a forward direction, RNNs possess a unique feature: They have loops in them, allowing information to persist.

This looping mechanism enables RNNs to remember previous information and use it to influence the processing of current inputs. This is like having a memory that captures information about what has been calculated so far, making RNNs particularly suited for tasks where the context or the sequence is crucial for making predictions or decisions.(8)

(8)( <https://shelf.io/blog/recurrent-neural-networks/>)



Figur (9)+ expliquation (9)

RNNs are made of neurons: data-processing nodes that work together to perform complex tasks. The neurons are organized as input, output, and hidden layers. The input layer receives the information to process, and the output layer provides the result. Data processing, analysis, and prediction take place in the hidden layer.

### **Hidden layer**

RNNs work by passing the sequential data that they receive to the hidden layers one step at a time. However, they also have a self-looping or recurrent workflow: the hidden layer can remember and use previous inputs for future predictions in a short-term memory component. It uses the current input and the stored memory to predict the next sequence.

For example, consider the sequence: Apple is red. You want the RNN to predict red when it receives the input sequence Apple is. When the hidden layer processes the word Apple, it stores a copy in its memory. Next, when it sees the word is, it recalls Apple from its memory and understands the full sequence: Apple is for context. It can then predict red for improved accuracy. This makes RNNs useful in speech recognition, machine translation, and other language modeling tasks.

### **Training**

Machine learning (ML) engineers train deep neural networks like RNNs by feeding the model with training data and refining its performance. In ML, the neuron's weights are signals to determine how influential the information learned during training is when predicting the output. Each layer in an RNN shares the same weight.

ML engineers adjust weights to improve prediction accuracy. They use a technique called backpropagation through time (BPTT) to calculate model error and adjust its weight accordingly. BPTT rolls back the output to the previous time step and recalculates the error rate. This way, it can identify which hidden state in the sequence is causing a significant error and readjust the weight to reduce the error margin.

## types of recurrent neural networks

RNNs are often characterized by one-to-one architecture: one input sequence is associated with one output. However, you can flexibly adjust them into various configurations for specific purposes. The following are several common RNN types.

### **One-to-many**

This RNN type channels one input to several outputs. It enables linguistic applications like image captioning by generating a sentence from a single keyword.

### **Many-to-many**

The model uses multiple inputs to predict multiple outputs. For example, you can create a language translator with an RNN, which analyzes a sentence and correctly structures the words in a different language.

### **Many-to-one**

Several inputs are mapped to an output. This is helpful in applications like sentiment analysis, where the model predicts customers’ sentiments like positive, negative, and neutral from input testimonials.

(9)( https://aws.amazon.com/what-is/recurrent-neural-network/)

**2.3.3.2 Long Short-Term Memory Networks**

**2.3.3.3 Gated Recurrent Units**

**2.3.3.4 Transformers**

**2.3.3.5 Autoencoders**

**2.3.3.6 Generative Adversarial Networks (GANs**

**Conclusion**