Chapter 2 Deep Learning ............................................................................. 32

Introduction ........................................................................................................... 32

Machine learning ................................................................................................... 32

Types of machine learning ............................................................................. 32

2.2.1.1 Supervised learning…………………………………………………..33

2.2.1.2 Unsupervised learning………………………………………………..33

2.2.1.3 Reinforcement………………………………………………………..33

Machine learning algorithms .......................................................................... 34

2.2.2.1 Linear Regression…………………………………………………….34

2.2.2.2 Logistic Regression…………………………………………………..35

2.2.2.3 Support vector machines…………………………………………......35

2.2.2.4 K-Means………………….…………………………………………..36

Machine learning applications ....................................................................... 37

Deep learning ......................................................................................................... 37

Artificial neural networks............................................................................... 38

Activation functions ....................................................................................... 40

Deep learning architectures ............................................................................ 42

2.3.3.1 Recurrent Neural Networks…………………………………………..43

2.3.3.2 Long Short-Term Memory Networks ………………………………..44

2.3.3.3 Gated Recurrent Units………………………………………………..45

Page | 7

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.

**FINIS**

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.

**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).

**Finis jusqua ici**

**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.

The Most Famous Algorithms:

**Q-Learning**: A model-free algorithm which learns values for actions available in a certain state.

**Deep Q-Networks (DQNs**): Combines Q-learning with deep neural networks in order to high-dimensional state spaces (Sutton & Barto, 2018).

Reinforcement learning is the right approach for sequential decision making and long-term planning.

2.2.1.4 **Beyond the Basics**: Hybrid and Specialized Approaches

Even basic machine learning might be furthered by the three primary types, by combining those different approaches into one formalism or by providing a special model specifically to solve a more complicated problem.

**Semi-supervised Learning**: Adds a small amount of labelled data to a large amount of unlabelled data. Usually useful when it is expensive to label data or takes a lot of time.

**Transfer Learning**: Uses a known domain to improve performance in a new one. For example, a model trained on image recognition can be converted for medical imaging tasks (Goodfellow et al., 2016).

Self-Supervised Learning: This means data from the outside realm lets the model create its own labels for learning purposes; exposure to supervised learning terms would be avoided this way.

**References**

* Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
* Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. Springer.
* Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
* Sutton, R. S., & Barto, A. G. (2018). *Reinforcement Learning: An Introduction*. MIT Press.