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 ………

**2.1Introduction**

The branch 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**

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)

* 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**

Data can then eventually be transferred from supervised learning to various machine learning types. Supervised learning refers to the process by which models are trained on a dataset, where for each input, there is a corresponding target output label. This allows a model to learn a mapping from inputs to outputs through identifying patterns and relationships in the data.

**Main Applications:**

Examples of supervised learning applications are:

**Classification**: Assigning data points to a finite number of labels. Diagnosis of medical diseases from images and classification of mail as either "spam" or "not spam".

**Regression**: Forecasting continuous value estimates such as for prices of houses, stock market values, or probable temperatures at a future date.

Some **Familiar Algorithms** Include:

**Decision Trees**: They represent very simple and powerful models that divide data into branches depending on feature values.

**Support Vector Machines (SVMs**): Work for classification tasks but are especially good when applied to high-dimensional spaces.

**Neural Networks**: These are models that can work on a wide variety of complicated, nonlinear relationships (Goodfellow et al., 2016).

It is more effective when more amounts of labeled data are available for supervised learning, but it handles overfitting and bias carefully (Hastie et al., 2009).

**2.2.1.2 Unsupervised Learning: Discovering Hidden Patterns**

This form of unsupervised learning does not carry any labels along with the data. Rather, it finds hidden structures or patterns in data without explicit guidance. This approach is quite suitable for exploratory data analysis and feature extraction.

**Key Applications**:

Clustering: Assigns similar values into groups. Examples would be clustering customers based on purchasing behavior, or a cluster of documents that have been organized by topic.

Dimensionality Reduction: Dimensionality Reduction is a reduction of some features in the dataset while retaining essential information. Hence, it helps improve computation efficiency and visualization.

Popular Algorithms:

k-Means Clustering: A very simple but efficient algorithm in partitioning data points into clusters.

Principal Component Analysis (PCA): A technique of dimension reduction while keeping the variation in datasets (Bishop, 2006).

It is one of the good unsupervised learning techniques for the case where one would not have many labeled data or gain knowledge about the way in which the arrangement structure of the data is built.

**2.2.1.3 Reinforcement Learning: Learning Through Interaction**

Reinforcing learning is a very alive sort of learning, in which the agent learns through the acting reinforcement through the environment. As agents receive reinforcement from their actions, he must pay attention to maximization.

Key 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.

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.