**Understanding Machine Learning and Its Applications**

**Saba Gour1**

1Software Engineer, Seattle, Washington, USA

**ABSTRACT**

Machine learning (ML) can be described as a machine’s ability to learn. Let us take an example of the assembly line in a car manufacturing plant. We utilize robotics and very specific instructions are given to the robots to carry out mechanical functions. The robots are machines on an assembly line and instructions are given through embedded programming. This is a kind of artificial intelligence but with very strict use cases. If machines on an assembly line where following an algorithm that gave them the freedom to change or improve their operations by themselves, then that would become an example of machine learning. Because the machines have self-learning capabilities to enhance their style of working. Thus, machine learning is a powerful concept and is driven by different algorithms. We need to carefully evaluate our business needs to understand if ML would be a good fit as ML has specific use cases and in a lot of other scenarios traditional rule-based programming would be sufficient. In this paper, we will explore the different types of machine learning algorithms and how they can be effectively applied to solve problems which could not be solved with existing software engineering approaches.

**Keywords:** Machine learning (ML), algorithms, supervised learning, unsupervised learning, artificial intelligence (AI)

1. **INTRODUCTION**

In the traditional programming approach, an engineer implements rules. There are a finite number of parameters, that need to be evaluated, and accordingly certain output will be derived. If any of these parameters are not as expected, then errors are thrown which are the edge cases and if parameter values change then the output will change which is expected behavior. But these rules are hard coded through programming languages and deployed as software bundles onto machines. Most of our business needs and functions can be covered by this approach. However, there are certain problems for which rules cannot be hardcoded because the number of parameters is just very large and there are complex relationships between these parameters. Let us consider an example of a country that is trying to determine the social security pension for its senior (above 65) population so that they can live a comfortable life in retirement. What parameters would need to be considered to determine their income – age, location, living conditions, other sources of income, family support, medical conditions, financial liabilities, cost of living, inflation, amount of money present with the country’s treasury, country’s economic condition, number of seniors in the country etc. We can see the large number of parameters that need to be considered to arrive at a decision and many of these parameters are interconnected, that is, if one parameter changes, it might impact other parameters as well. The solution to this problem is machine learning (ML). We will see the reasons as to why machine learning can solve such massive problems.

1. **METHODOLOGY**

Machine learning (ML) is a direct approach for solving large scale problems, it should not be used to implement simple business rules and use cases; for those needs we can use traditional rule-based programming techniques. Machine learning is an engineering technique that takes a data driven approach. Large scale problems, like the one we saw above cannot be solved with a rule-based programming approach because defining such complicated and varying relationships between parameters is not possible by applying rules. Thus, a machine learning approach, takes large amounts of data, which in our case would be the data of the senior population in the country. This data would include demographic, medical, social and financial information of the seniors, which would be fed to a machine learning algorithm. This algorithm will evaluate the large amounts of data and arrive at an income level for seniors based on their circumstances. This technique is called regression where many data points are examined to arrive at a value. The data that is fed to a machine learning algorithm is called training data. It’s called training data, because the ML algorithm gets trained on this data to derive meaningful metrics and insights. These metrics and insights are used for varying purposes like improving business operations, reducing marketing costs, effectively training employees, improving infrastructure within a country, to name a few, and in our example to determine fair pension for seniors. There are different machine learning approaches that can be used to solve different kinds of problems. Let us look at them.

* 1. **Supervised learning**

Supervised learning is a kind of machine learning approach that relies upon training data that is prepared by humans. So let us understand what training data is in this scenario. ML analyzes huge amounts of data, recognizes patterns in the data and then makes predictions based on those patterns. This is what makes ML a powerful technique. Training an ML algorithm means feeding the algorithm with data. After the algorithm has been trained on data, it is called an ML model. Thus, in our example of the senior population, we have a trained ML model that is great at predicting pension for seniors, and when it is provided with new data for seniors, it can make better predictions because the more data the model analyzes, the better its predictions become. However, with supervised learning we need to make sure that the data is in a good format, it does not have null values and unnecessary information. A data analyst or data scientist needs to collect data from different sources that is most meaningful for solving the problem, then put it into a standard format and remove all irrelevant details that can cause the predictions to get skewed. For example, data should be collected of males and females both, if a gender is ignored in the data, then predictions can get biased, and they can cause more harm than good. If we feed good data to an ML model, we will get good predictions and vice versa is true as well. Thus, supervised learning relies on humanly collected and transformed training data that will lead to best possible predictions from an ML model.

There are two supervised learning algorithms – classification and regression. We have seen regression algorithm in the example above. However, classification is used to classify images, text and any kind of data into two or multiple categories. For example, in social media we do sentiment analysis, the ML algorithm will go over the comments and determine whether a comment is positive or negative. This would be a simple two-class classification. However, we can have multi-class classifications; a comment could be politically charged, it could spread misinformation, for example it could speak of an accident that has not really happened. Thus, classification algorithm will help us categorize information more accurately and we can take necessary steps to either block the user, erase the content or address the matter proactively. The more comments the ML model gets trained on, the better classification it will make regarding the sentiment. Sentiment analysis is an important example, as politically charged comments or spreading misinformation on social media can have dangerous consequences in society.

**2.2 Unsupervised learning**

In unsupervised learning, the ML algorithm does not need training data that is collected or transformed by a human. We can have information sources that directly send their data to the ML algorithm without human intervention, and the algorithm will detect patterns automatically in the data and make predictions. The only nuance here is that the predictions made by an unsupervised learning model need to be verified by a human for accuracy. Let us take the example of computer networks, the data from different network devices like firewalls, routers, load balancers, intrusion detection and prevention systems, physical machines, virtual machines can directly be fed to an ML algorithm, the algorithm will be able to detect any anomalies in the data and report them. With large amounts of network data, the algorithm will begin to recognize normal scenarios, thus if an attacker is intruding an organization’s system, it will be reported by the ML model as an abnormality. We have unsupervised learning anomaly detection ML models that are great for detecting network threats, thus enabling the security team to take necessary action to remediate them. The security team will need to verify the threat data before acting upon it. But as the ML model keeps getting trained on different kinds of network data, it will make better predictions on cybersecurity attacks.

In addition to anomaly detection, there are two other unsupervised learning algorithms – clustering and dimensionality reduction. Clustering helps to accumulate similar kinds of data together. For example, users that tend to buy similar items on a shopping website will be identified and clustered together based on their shopping behavior. This helps an organization in understanding its customer base and market segmentation. Dimensionality reduction is used when we have many parameters, and we would like to understand which out of these are the most impactful parameters. For example, an organization is trying to understand which factors are most responsible for increasing employee productivity. Now, there are a bunch of factors to be considered here, but feeding employee survey data to a dimensionality reduction algorithm will give information regarding the factors that have been most impactful. This information will help an organization is training and retaining their employees.

* 1. **Human bias vs machine bias**

Sometimes the reason that we give for using machine learning models is that we want to remove human bias. This may be true, but sometimes we remove human bias only to introduce machine bias. During the covid pandemic, analysis was done on people that were disproportionately impacted by the pandemic; it was found that it is unfortunately the frontline workers and lower income groups. Now, this is a perfect application of machine learning where hospital data of patients is fed to an ML algorithm, and the ML model can detect patterns and make predictions regarding the people that are most impacted. In this case, there was no human bias or machine bias as extensive data from various hospitals was used to train the ML model. But let us consider the case where hospitals from certain regions of the country did not share their data, then in that case, the predictions would not be accurate as a certain group of people have not been included. In this case, we would see machine bias due to lack of training data. This would also be the case if the country is doing analysis on distributing scholarships to students from underprivileged communities. If information from certain communities is excluded from the training data, then predictions made by the ML model cannot be relied upon. Thus, the ML model will end up creating a certain profile of a deserving student from certain communities alone and later, if student data from excluded communities is fed to the ML model it will most likely say that the students do not deserve a scholarship even if they do. Machine bias can be as dangerous as human bias; thus, it is our responsibility to make sure that an ML model is trained on comprehensive data. Let’s take the example of an insurance company that has trained their ML model on comprehensive data from different age groups, ethnic communities, genders, economic status, geographical locations etc. However, when the ML model suggests that an individual is more prone to certain expensive diseases in a few years, then they do not give insurance to that individual. This is an example of human bias, because in this case the ML model is honestly making predictions, but the insurance company is using the ML model in a discriminatory way that cannot be legally permitted. Thus, governance around the use of machine learning and artificial intelligence is essential as these tools should not be used to harm individuals.

* 1. **Deep learning**

Deep learning is a type of machine learning. It utilizes the technique of neural networks. Neural networks replicate how the human brain works. In a human brain, neurons are organized in layers. We may have heard that neurons that fire together, wire together. This means that within our human brain, in each situation some neurons within a layer will be activated together. This causes a neural pathway to be created between these neurons and facilitates better communication between them. Thus, when a human finds themselves in the same situation again, it is more likely that the same group of neurons will be activated again. This is how neural pathways are created to accomplish tasks; it could be writing, running, talking just to name a few. The same concept is applied in neural networks, where a bunch of neurons are used to understand data in layers. Each layer of neurons understands a certain aspect of the data. Deep learning is used to apply machine learning to complex data like images and movies. An image is made of millions of pixels which are analyzed using neurons. Let us consider the example of deep fakes. A deep fake is an image generated by artificial intelligence (AI). Generative artificial intelligence (Generative AI) produces text, images, music, voice and other kinds of media to name a few. If Generative AI is in the wrong hands, it can wreak havoc. How can we distinguish a deep fake from a real image? This is an application of classification algorithm in deep learning where the ML model that utilizes neural networks will be trained on millions of fake and real images. With such a vast amount of training data, the ML model will begin to successfully classify an image as real or fake. It is said that when we come across an image on the web that looks too good to be true; then we need to exercise restraint before believing that the image is true. We need to apply our discretion even more today when we look at images online, as we could be looking at a deep fake.

* 1. **Artificial intelligence**

Artificial intelligence (AI) is often used interchangeably with machine learning. However, it is a bit different from ML. We can safely say that artificial intelligence is the result that we see after applying machine learning algorithms. If a computer can correctly identify the image of a cat, then that to us is artificial intelligence. But behind this AI is machine learning classification algorithm that has been trained on millions of images of cats. Artificial intelligence is a broader idea, and it has been existent since the last few decades. Imagine a vending machine that dispenses snacks on the push of a button. This is a kind of artificial intelligence, but the vending machine does not have the capability to gather customer statistics and make predictions on which snack items need to be stocked more. The vending machine has been programmed through software and hardware to dispense a specific item when a particular button is pushed. This is precisely an example of AI driven by rule-based programming. It is not AI that is driven by machine learning. Accurately predicting the weather for the upcoming month can now be done by feeding the training data of different climate factors to an ML model. This is an example of an AI that is driven by machine learning. Thus, artificial intelligence can be described as the capability of a machine to do a task or predict a result by applying some sort of intelligence, and the intelligence is developed by using machine learning.

* 1. **Applications of machine learning**

Let us consider a scenario where we need to construct buildings in extreme climatic situations, like extreme heat or cold weather. Generally, in such a situation construction is halted as workers cannot work in extreme climate. This prolongs the construction work by a couple of years. Machine learning can be applied to solve this problem. A bot is an agent or a program that is trained to do tasks. The ML algorithm behind this is reinforcement learning. Through reinforcement learning a bot can be trained to perform construction work. Thus, in extreme weather conditions, the construction work can continue by deploying bots. A chatbot, is another example, which interacts with a human and answers their questions in real time. The ML model used for this purpose is a large language model (LLM) that is trained to understand human language and produce text that a human can understand. A chatbot is trained using reinforcement learning, as by answering more and more questions, the chatbot begins to develop intelligence to give better answers. Chatbots have been adopted widely as online customer service agents that interact with customers by collecting some of their basic information and providing them with answers to their queries. However, it can be said that chatbots still have a long way to go in terms of achieving customer satisfaction as the answers are very basic and many times customer queries are more complex and require a human agent. There is a huge push towards developing personal assistants that can help us to learn a variety of subjects from carpentry to coding to history. The idea is to train a chatbot on massive amounts of data on different subjects. Thus, depending upon the query of a human, the personal assistant will respond with the necessary information. However, there is substantial ground to be covered before we can extensively start using such advanced personal assistants. In the example of airline companies, that want to optimize their profits and reduce fuel consumption; machine learning can be used to predict more economical flight paths. The ML algorithm needs to be trained on massive data like current flight paths of the airline, fuel usage, time of the day, flights of other carriers close to the flight paths of the airline, minimum distance to be maintained in the air between aircrafts etc. For this purpose, regression algorithm can be used. To further enhance the metrics, dimensionality reduction can be used to find parameters that have the most impact in making flight paths cost effective and safe. Thus, multiple ML models can be used to improve results that an organization would like to extract from training data based upon their needs. Financial institutions are using machine learning algorithms to find fraudulent transactions. The algorithm used here would be classification as we need to classify a transaction as genuine or fraudulent. The training data to this ML model would be all the financial transactions of an organization. Classification would be supervised learning, wherein a data scientist would carefully collect and format the training data. However, another unsupervised learning technique that could be useful in this scenario is anomaly detection algorithms wherein all the financial transactions of an organization would be fed to the ML model directly without human intervention and the ML model is then left to detect anomalies by itself, we might get interesting findings through this technique which would need to be verified by humans but it would be worth implementing.

1. **RESULTS AND DISCUSSION**

We have studied the specifics of machine learning and the different algorithms that drive machine learning techniques. Depending on our needs we can use certain algorithms that will give us the best results. We can try to train different ML models and then decide which model gives us the output that best suites our situation. Machine learning can be used to solve massive problems that could not be solved with traditional programming methods. There are multiple applications of machine learning in natural language processing (NLP), making predictions with massive number of parameters, distinguishing data into different categories, combining similar data through clustering and reducing the number of parameters to the most impactful ones.

1. **CONCLUSION**

Some form of artificial intelligence has always existed in technology. Traditionally, artificial intelligence was a computer program that could achieve a certain output based on a small number of parameters. It could be an ATM machine, an online application for booking train tickets or asking questions to the personal assistant on your phone using your voice. These solutions which were under the umbrella of artificial intelligence could not solve problems at scale and make predictions. It is artificial intelligence driven by machine learning that can be trained on massive amounts of data to make predictions that can be used in different fields like business, sports, weather, economic planning and medical research to name a few. Machine learning has the capability of processing large amounts of data, analyzing it, detecting anomalies, finding useful metrics and making predictions. Machine learning is a technique that is revolutionizing our world; however, it needs to be used with discretion. A lot of organizations are in a rush to adopt artificial intelligence (AI) within their systems, but a thorough feasibility study needs to be done before using AI, as it might not be the best fit to solve your problem. Even if machine learning is the solution to your problem, it needs to be implemented responsibly as poor use of AI can cause more harm than good. Thus, as we continue to adopt artificial intelligence driven by machine learning within our software architectures, we should be doing a careful analysis of the problem at hand to determine if machine learning is the best solution.

1. **REFERENCES**
2. Emmanuel Ameisen, “Building Machine Learning Powered Applications. Going from Idea to Product”, First Edition, Feb. 2020, pp. 23 - 125
3. Giuseppe Bonaccorso, “Machine Learning Algorithms – Second Edition: Popular Algorithms for Data Science and Machine Learning”, Second Edition, Aug. 2018, pp. 220 - 331