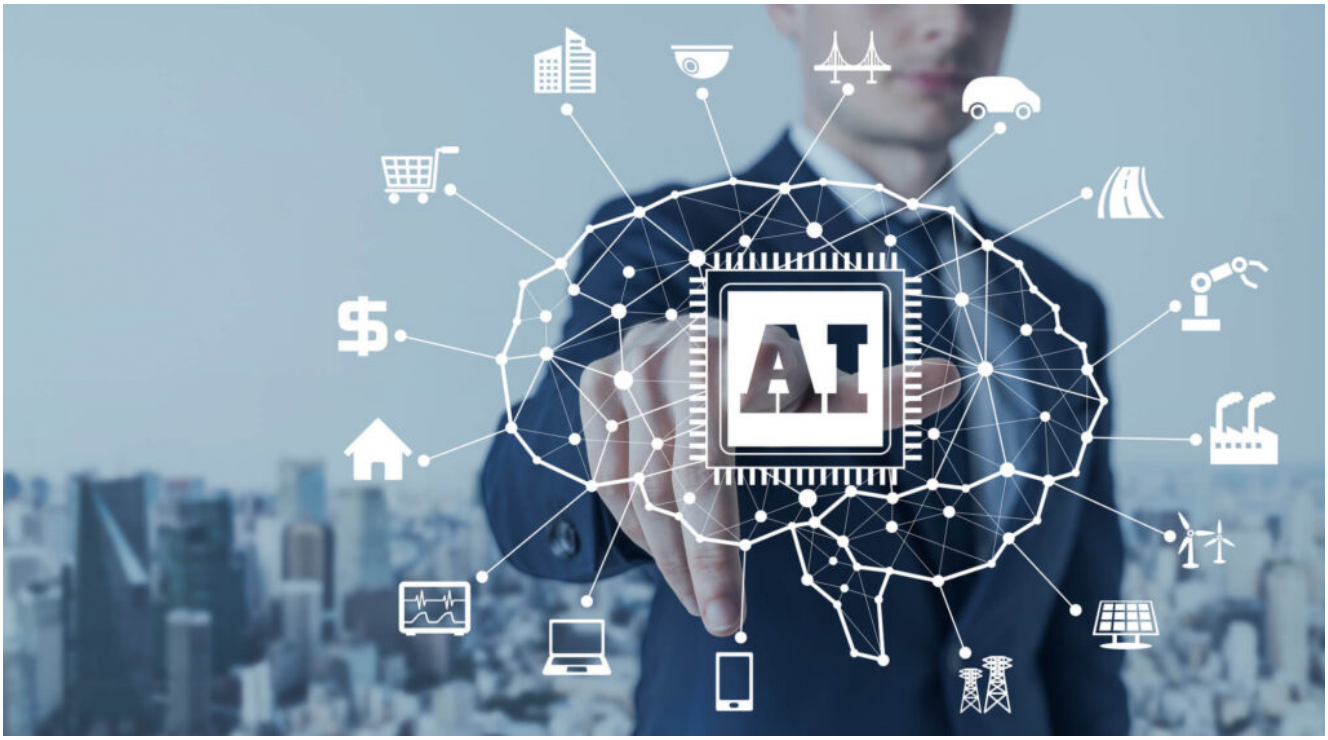
Artificial Intelligence and Machine Learning in Cybersecurity



World is an ever changing place. Contemporary world has revealed new notions such as Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL). AL, ML and DL have the capacity of various uses including increasing the potential to increase the efficiency and output in multiple fields. Machine Learning is commonly known in the world of cybersecurity when it comes to general application of Artificial Intelligence. Artificial Intelligence, Machine Learning and Deep Learning share many traits which seem similar and are often confused with one another.

The main purpose and goal of Artificial Intelligence is to develop computer programs having the ability to achieve intelligent functions just as they are carried out by human brains. It cannot be said when the first ever programming idea related to Artificial Intelligence was formulated but it can

be traced back to the late 1940s and early 1950s. One significant development in the world of Artificial Intelligence was the creation of LISP or list processing language by John McCarthy in the year of 1957. Then in 2016, Sophia, a programmed humanoid, was introduced to the world. Artificial Intelligence also has some day-to-day occurrences in our daily lives including speech recognition, mapping, finding best possible routes when travelling, smart phones and devices that can perform independently etc.

Machine learning is defined "as the ability (for computers) to learn without being explicitly programmed." Machine Learning has the capability to learn from large amount of data available using algorithm that are man built to complete tasks and it can also be seen as a data mining since it processes large amount of data. There are two kinds of learnings that fall under Machine Learning; Supervised Learning and Unsupervised Learning. In Supervised Learning, computer is given parameters to equate the data whereas in Unsupervised Learning, computer does that comparison and finds relationship from the data available independently. One of the pioneer of Machine Learning, Arthur Samuel, stated in his 1959 IBM paper that "programming computers to learn from experience should eventually eliminate the need for much of this detailed programming effort." Machine Learning programs independently improves basing upon old and new data with a little help of humans. Machine Learning helps in designing cybersecurity algorithms that flag the unauthorized and unnecessary access. It also helps in flagging the security risks if there is any breaching or hacking taking place.

Machine Learning shows great commitment in cybersecurity and Artificial Intelligence. Machine Learning has the ability to extend great help when it comes to IT or cybersecurity. Machine Learning can acquire results from the past existing data to recommend the appropriate responses and predictions. It can build profiles of the hackers and how they attempt to

breach from previous data breaches. As per Amir Kanaan, as it expands its knowledge, it can start to make proactive recommendations on how to reduce risk. Also, the advantages of Machine Learning in security can help us in areas such as Anti-malware, Dynamic Risk Analysis, and anomaly detection.

According to Rob Sobers, some benefits of Machine Learning include:

Classification: Programs classify data based on predetermined parameters.

Clustering: For data that does not fit preset parameters, Machine Learning group's data based on their similarities or anomalies.

Recommendations: Programs learn from past choices, inputs and associations to recommend approaches and decisions.

Generative frameworks: Based on past data inputs, programs generate possibilities that can be applied to data that had not encountered those specific inputs before.

Predictions: Programs forecast based on data sets and past outcomes.

Machine Learning can be very beneficial in case of cybersecurity because it can generate an alert when there is a data breach, theft or other attacks that can cause strain financially. Machine Learning also helps in minimizing the workload for security teams, decreases the risks of human error and cater the specific requirements. Although Machine Learning has benefits, it is not entirely invincible. Machine Learning and Artificial Intelligence are becoming an essential part in the world of cybersecurity to run the matters more smoothly and timely. It is still not clear if Machine Learning will complete take over the tasks that require human brain. Complete reliance on Machine Learning and Artificial Intelligence can cause a false sense of safety and security,

which is why it is important for both humans and technology to work hand-in-hand to stand against ever powerful cybersecurity threats.