OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Mini Review

How Machine Learning Could Affect Information Security?

Daniel Cavanaugh*

Department of Engineering, New Jersey Institute of Technology, New York, USA

ABSTRACT

Although machine learning as a concept has been around since the very early days of computing, it is safe to say that its impact, as well as general interest in the topic has never been larger. Large streaming services and online stores use neural networks to form recommendations and has made innovations such as facial recognition possible. From the first neural network machine called SNARC in 1951, to beating humans at chess, all the way to newer, ambitious projects like Neura link, machine learning has been constantly changing and improving, but what does that mean for the field of information security?

Although the possible implications of this technology in pretty much any field are not certain, there are some ideas about how machine learning could further improve the security tools available to us as well as some fears about its misuse.

Keywords: Data mining; Data mining system; Database; Data sets

INTRODUCTION

In this paper I will first explain machine learning in greater detail and provide a brief overview of the different kinds of machine learning. After that, I will go over a few possible use cases of machine learning which would benefit information security before concluding with some of the ways this technology can be used for malicious behavior.

Machine learning is a kind of AI centered around processes which take data and learn from it in order to improve accuracy automatically over time. This is done through taking a data set, (which could be a set of images or network traffic, for example), and feeding it into a machine learning application. The machine learning application runs a selected machine learning algorithm on the input and tries to produce a desired output.

Machine learning algorithms can generally be categorized into algorithms which work on labeled data and algorithms which work on unlabeled data. Common labeled data algorithms include regression algorithms, decision trees, and instance-based algorithms whereas common unlabeled data algorithms include clustering algorithms, association algorithms, and neural networks.

The selected algorithm is trained on sets of data and has its output compared with the desired results. Tweaks are made to the process in order to make the actual output more similar to the desired output. Ideally, the application's accuracy will improve overtime. If training is successful, the application will be presented new data it has not been trained on and will still produce accurate results, or at the very least results which require less training to get right.

The methods used in conjunction with these algorithms are typically described as falling into three primary categories. The first is supervised machine learning, which trains itself on a data set labeled with information the machine learning model is being built to determine. An example of this process might be giving a data set of various labeled pictures of fruits to a model designed to identify bananas. This method requires less data than other models, however, getting properly labeled data can be very time consuming and there is a danger of overfitting or creating a model that is too closely tied to the data set, making it less accurate when exposed to new data [1].

The second is unsupervised machine learning. Unsupervised machine learning uses a large amount of unlabeled data and extracts features from it that are needed to label, sort, and classify it in real time. This type of machine learning is focused

Correspondence to: Daniel Cavanaugh, Department of Engineering, New Jersey Institute of Technology, New York, USA, Tel: 7087184484; E-mail:cavanaughd18@students.ecu.edu

Received: April 13, 2021; **Accepted:** April 27, 2021; **Published:** May 04, 2021

Citation: Cavanaugh D (2021) How Machine Learning Could Affect Information Security? J Inform Tech Softw Eng.11:258.

around identifying patterns and relationships in data. This requires a lot of data. The final of the three is Semi-supervised learning, which works kind of how it sounds. It uses a smaller labeled data set to guide classification as well as a larger unlabeled data set. This can help with a lack of labeled data [2].

Two other terms you might hear are reinforcement machine learning and deep learning. Reinforcement learning is like supervised learning, however, instead of using sample data, the model learns through trial and error over time with a sequence of successful outcomes being reinforced during the training. Deep learning is an ambitious subset of machine learning that seek to define an artificial neural network that is designed to learn in the same way a human brain learns. It requires massive amounts of data through multiple calculation layers and adjustments in each successful layer to improve the outcomes. These models are typically unsupervised or semi-supervised and can use reinforcement learning [3].

LITERATURE REVIEW

Now that we have covered the basics of what machine learning is and how it works, we can start to go into a few potential use cases within the work of information security. One use case includes a cognitive security manager. This security manager, either on its own or part of a larger autonomic network management system could be trained to detect malicious network activity.

This would likely be achieved through processing large amounts of traffic data in real time in order to discover critical incidents. Eventually, this type of monitoring system could be able to predict user behavior as well as identify and automatically respond to behavior which is malicious. It is also possible that this could be used to identify possible attacks which an enterprise is more likely to face and prioritize measures which prevent them [4].

Machine learning could also be trained to detect and respond to malware. After being trained to recognize attributes associated with malware through training on malware, such an application may be able to detect new malware that hasn't been seen before or even recognized by human beings simply based on the way it behaves. This same idea could be applied to analyzing data elements of network traffic in order to detect encrypted malware in traffic on the network [5].

In a similar fashion, machine learning could be used to train an application to mitigate the damage caused by phishing attacks. Algorithms could be trained to recognize signs of phishing emails to make sure that they are properly intercepted and marked before sensitive information is divulged. This also applies to spam filtering in general and could greatly improve the systems we have in place.

While these systems might be more efficient and may make the lives of some employees easier and the wallet of some employers fatter, these are, of course, imperfect security solutions. Firstly, there are several barriers to adoption of machine learning systems for information security. Often, the sheer amount of data needed can be expensive and hard to come by. Any of these applications, (whether it be a network monitoring or malware detection system), would need lots of data to be accurate and even with clever methods of constructing data, a lot of real world data may still be necessary which can mean a lot of very expensive trial runs.

Also, there needs to be a way to ensure that the data is good data. You may have heard the phrase "garbage in, garbage out." That applies here. Training an algorithm on bad data will make good results unlikely. It's also important to be aware of false positives, which can stem from bad data, lack of data, or just not enough trial runs. If there is even a small chance of a false positive, depending on your use case, it can be devastating.

Finally, even if we all eliminate the problems of data collection and false positives, there will understandably be many people who do not trust a computer to make these kinds of sensitive security decisions. It is true that we trust calculators and GPS systems to be more accurate than human beings, but for many people this can seem like a stretch. Regardless, this technology seems to keep improving and shows no sign of stopping short of this point [6].

DISCUSSION

Theoretically, just as machine learning systems could be used to better detect malware, they may be used to try and keep up with and circumvent those protections more efficiently than a human being could. Malware that could rewrite itself frequently to try and keep up with antivirus software and other counter measures through many generations could become very troublesome to deal with.

In addition to this, Machine learning applications could be exploited in more direct and simple ways, such as feeding in bad data either through giving it nonsense data that resembles non-existent things that the application must classify thus producing less accurate results or through poisoning or otherwise compromising existent good data. The risk of exploitation increases when using a commonly used machine learning application as your base those hackers might already be familiar with. It is also important to secure any sensitive data that may be used in the training process as data extraction attacks may be utilized to gather this data.

Machine learning can be used to train endpoint security setups in identifying anomalies and malicious activities based on what it has already experienced and flagged. Since machine learning thrives on volumes and larger datasets, endpoint security can be continuously strengthened against newer threats based on past data and repositories.

CONCLUSION

In this article we discussed machine learning, what it is, the ways it can work, and how it could be relevant to future developments in information security. Overall, like with any development, further integrating machine learning systems into how we do security could have major benefits, but also potential for abuse. It is important to keep an eye out for what might be over the horizon and adapt to change, because it is always inevitable.

REFERENCES

1. Alauthman M, Almomani A, Alweshah M, Omoushd W, Alieyane K. Machine Learning for Phishing Detection and Mitigation. CRC Press. 2019;48-74.
2. Ayoubi S, Limam N, Salahuddin MA, Shahriar N, Boutaba R, Estrada-Solano F, et al. Machine learning for cognitive network management. IEEE Communications Magazine. 2018;56(1):158-165.
3. IBM Cloud Education. What Is Machine Learning?. 2020.
4. Mikhailovich KM, Valerievna MA, Andreevich PP, Alexandrovich UI, Vladimirovich KA. Guidelines for Using Machine Learning Technology to Ensure Information Security. ICUMT. 2020;285-290.
5. Szyszka E. Machine Learning in Information Security. 2020.
6. What Is Machine Learning in Security? 2021.