MACHINE LEARNING IN CYBER SECURITY

Analyzing the current machine learning practices in cyber security

CS4991 Capstone Report, 2021

Callie Hartzog
Department of Computer Science
University of Virginia
School of Engineering and Applied Science
Charlottesville Virginia USA
cah6rxg@virginia.edu

ABSTRACT

Society is connected through technology, but unfortunately every piece of software is susceptible to "attacks" in the form of hacking. With processes such as banking and personal information all stored online, hackers are even more incentivized to steal data. The field of cybersecurity has risen out of concerns over hacking. However, for a team to inquire into a piece of software it can be a tedious and lengthy process to find any security breaches. Rather than relying on engineers to manually test software, machine learning practices can be used to streamline cybersecurity testing and identify vulnerabilities faster than a human can. We can utilize recurrent neural networks to identify common security breaches in software and then learn how to identify new breaches rather than having cybersecurity professionals test software manually.

1 INTRODUCTION

Cybersecurity has been a concern of companies and software engineers as long as private information has been stored digitally. As societies around the world progress towards more technological driven practices and lifestyles, the concern over the safety and security of sensitive data increases. A by-product of the upsurge in use of technology is the emergence of cyber criminals. Often called hackers, cyber criminals gain illegal access to data and often use this data for profit. Social security numbers, banking information, passwords, and other susceptible personal data is all stored online and at risk of being stolen by hackers. In the past two years, cyber-attacks have increased by 400 percent and are unlikely to fall moving forward (Riley, 2021). Good cybersecurity practices are essential to protecting data and thwarting the attacks of hackers. Rather than having software engineers manually inspect technology to assess potential vulnerabilities, machine learning techniques can be used to streamline cybersecurity and improve the rate at which threats to security are detected.

2 MACHINE LEARNING IN CYBER SECURITY

A huge vulnerability in current technology is found in Internet of Things (IoT) devices. IoT devices are often common household appliances such as doorbell cameras, smart thermostats, and wireless gaming devices. Their direct access to the internet allows for a variety of attacks from hackers if they are not secured properly (Sivanathan et al., 2020, p. 1). The most common practice for securing IoT devices is the use of firewalls, which protects the device from external access but fails to protect it against any internal attacks. There has been a more recent movement within the cyber security community to secure IoT devices using intrusion

detection systems that are implemented using machine learning algorithms (Smys et al., 2020, p. 1).

The use of recurrent neural networks (RNNs) to train computers to recognize cybersecurity threats in programs has become another popular way to secure various devices and computer systems. Recurrent neural networks are a type of neural network that allows the computer to retain information it has previously learned, as seen in Figure 1. A computer is trained to recognize patterns, classify images, or sort data based on given parameters. It then can use its knowledge to apply the same practice towards previously unseen data (Zahangir et al., 2019, p. 28).

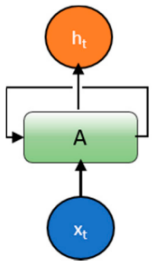

Figure 1: A basic recurrent neural network (Zahangir et al., 2019).

There a several different sets of data that can be used to train algorithms to detect security threats. When using a data-set of 22 different attack types to train a recurrent neural network, Xin et al. (2018) initially received a test accuracy of 83.28% (p. 12). This is a good base line for using RNNs to identify security threats but through optimizations the accuracy can increase. Considering the algorithms are being used to secure systems that potentially contain very sensitive and important data, achieving an accuracy closest to 100% in detecting security risks is extremely important.

3 SHORTCOMINGS OF MACHINE LEARNING ALGORITHMS

Both a benefit and deterrent to the use of machine learning is the number of different types of algorithms that can be implemented. Depending on the device or system that is being secured, the machine learning algorithm that yields the most accurate risk detection results may vary. This provides a wide array of options that may best fit securing a certain device, but also requires more testing to determine which algorithm is the most accurate for each situation.

Alqahtani et al. (2020) used seven different algorithms [Decision Tree (DT), Random Forest (RF), Random Tree (RT), Decision Table (DTb), Artificial Neural Network (ANN), Naive Bayes (NB), and Bayesian Network (BN)] and trained them on the same data set to implement various intrusion detection systems and compare the resulting accuracies (p. 2). In Figure 2 all the accuracies were either 90% or above but they differed widely within the 90-100% range.

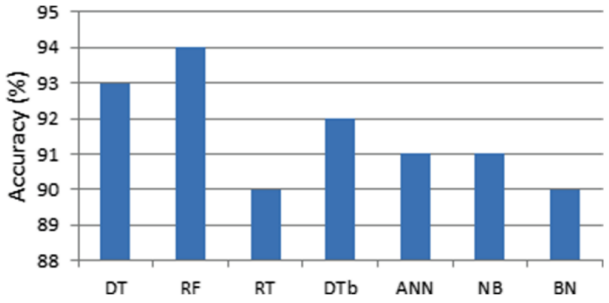

Figure 2: Accuracy results of different machine learning algorithms (Alqahtani et al., 2020).

Another issue with machine learning is that the accuracy of an algorithm is only as good as the data it is trained on. There are many pre-existing data sets that contain features useful to training machine learning algorithms to detect cyber security threats, such as the KDD Cup 99

and ADFA data sets. The KDD Cup 99 dataset contains a wide variety of attack types, which is useful for creating a blanket protection system that can identify many different kinds of attacks. However, datasets like the ADFA data set are more targeted. The ADFA data set focuses on detecting intrusions from the host level, such as an internal attack originating from an individual gaining access to admin controls of the system. In addition to these data sets, algorithms can be trained by collecting data directly from a computer system. This makes the algorithm more aligned with the specific system at hand as it analyzes incoming and outgoing traffic to the system, then learns to form typical use patterns that will be the basis to predict if abnormal use occurs (Yavanoglu & Aydos, 2017, p. 5-6).

Over the years these data sets have been improved through the addition of new features and attack patterns. The quickest and most efficient way to improve the accuracy of these algorithms is to improve the data sets they are being trained on. This can be achieved by researching in depth the typical attacks systems face by hackers and adding data on these attacks to the data bases so they are as robust as possible.

4 FUTURE RESEARCH

Using machine learning algorithms is a great start to strengthening cyber security practices. However, there are potential issues that could be further addressed once the algorithms are implemented. One area of research would be training the algorithms to disregard adversarial data. For example, a hacker may gain access to the training data of an algorithm and alter it. They could artificially insert data that trains the algorithms to mark certain cyber attacks as non-threats. Ensuring that this practice does not occur would also help to prevent any future attacks.

5 EVALUATION OF COURSE CURRICULUM

The machine learning and cyber security elective courses prepared me with the knowledge and background necessary to complete this project. Within the machine learning courses at the University of Virginia I learned how to implement various neural networks. Most importantly, I learned the mechanisms and knowledge behind how machine learning algorithms functioned. The cyber security course also helped me to realize that there were inefficiencies in our current practices that could be improved upon through the use of machine learning. Additionally, my personal interest in machine learning fueled my interest and led me to research many machine learning concepts on my own.

REFERENCES

[1] Alqahtani, H., Sarker, I.H., Kalim, A., Minhaz Hossain, S.M., Ikhlaq, S., & Hossain S. (2020) Cyber intrusion detection using machine learning classification techniques. *Computing Science, Communication and Security, 1235*(1), 121-131. https://doi.org/g3mh

[2] Riley, T. (2021, February 22). The Cybersecurity 202: Cybercrime skyrocketed as workplaces went virtual in 2020, new report finds. *The Washington Post*. https://wapo.st/3EFGNw5

[3] Sivanathan, A., Gharakheili, H. H., & Sivaraman, V. (2020). Managing IoT cyber-security using programmable telemetry and machine learning. *IEEE Transactions on Network and Service Management, 17*(1), 60-74. https://doi.org/gwv5

[4] Smys, S., Basar, A., & Wang, H. (2020) Hybrid intrusion detection system for Internet of Things (IoT). *Journal of ISMAC*, *2*(4), 190-199. https://doi.org/gksp9n

[5] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018) Machine learning and deep learning methods for cybersecurity. *IEEE Access, 6*(1), 35365-35381. https://doi.org/gf9fq3

[6] Yavanoglu, O., & Aydos, M. (2017). A review on cyber security datasets for machine learning algorithms. 2017 *IEEE International Conference on Big Data (Big Data),* 2186-2193. https://doi.org/gmt5j4

[7] Zahangir, M. A., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, S., Hasan, M., Van Essen, B. C., Awwal, A. A. S., & Asari, V. K. (2019). A state-of-the-art survey on deep learning theory and architectures. *Electronics, 8*(3), 292. https://doi.org/gfw52f