An Overview of Machine Learning in Intrusion Detection Systems

Darren Pritchard

CS562, Department of Cybersecurity

Old Dominion University

Norfolk, VA, USA

dprit002@odu.edu

***Abstract*—In an increasingly and rapidly changing security environment, attacks are becoming more nuanced and complex, thus requiring better detection methods. Intrusion detection systems seek to take on these issues utilizing machine learning and deep learning methods in order to detect and act upon threats. A collection of methods used by intrusion detection systems are herein collected, described, and explained, and the impact of these systems on network and system security is discussed.**

Keywords- Cybersecurity, Machine Learning, Intrusion Detection, Deep Learning, Artificial Intelligence

I. Introduction

We live in a society of the internet and our lives are, more or less, lived using the internet for 90% of them. As such, we socialize, do business, entertain ourselves, educate ourselves, and so on using the internet. This leaves us incredibly vulnerable to attack and the threat of attack drives a need for better detection of attack. Intrusion detection systems are one answer to this need; they are software suites used to detect and alert cybersecurity professionals of an attack in real-time or with low latency. This research paper will address what exactly is an intrusion detection system, the methods used for intrusion detection within these systems in order to detect threats, and the impact of these software suites on improving security within various networks systems.

II. What Is an IDS?

An IDS, or intrusion detection system, is a software suite used by cybersecurity professionals to monitor and analyze data as it is modified within a system or network. The software suite then notifies the user of abnormal changes to that data that may be indicative of an intrusion or breach. There are different types of IDS, however; The two most prevalent types of intrusion detection system are signature-based intrusion detection systems and anomaly-based intrusion detection systems. Signature-based intrusion systems use known values and types of intrusions in order to detect an intrusion, whereas anomaly-based intrusion detection systems compare known data to unknown data in order to determine an intrusion. Many systems are hybrids between the two, as they use techniques that are used in either system. This will be discussed further in section IIIC, *ensemble learning methods.*

III. Methods for Anomaly Detection

Due to the nature of machine learning and the complex amount of factors in machine learning and artificial intelligence, this paper makes no attempt to ascertain whether a particular method is better than another at training an algorithm used in intrusion detection, as there are a number of different factors in determining the use case for each technique. The techniques and methods mentioned herein are also not exhaustive, and there are more methods that this research may not cover. That being said, there are a number of methods used to train machine learning algorithms to detect and alert the user of anomalies that could be intrusions or breaches which can be separated into one of three categories: Supervised, unsupervised, and hybrid learning methods [2].

A. Supervised Learning Methods

There are a number of methods using supervised learning to train algorithms to accurately detect anomalous behavior that may be considered an intrusion or breach. Many of these methods are used in signature-based detection, which utilizes known and predefined threats. After detection of any of the predefined data associated with a legitimate intrusion attempt, the user of the intrusion detection system is alerted.

The utilization of association rules is a method of intrusion detection based on "rules," which are formed by associating the dataset from real world intrusions or simulations of intrusions with ways to react to those kinds of situations. A good way to think of association rules is to think of an "if, then" statement in programming. The "if" part of the statement is the data from a real world intrusion, whereas the "then" part of the statement would be the actions to take upon the detection of this data. However, association rules can be easily thwarted by slight variations in attack method that have previously been unaccounted for within the dataset used for the training of the machine learning algorithm. This is where fuzzy logic comes into play, as fuzzy logic compensates for these slight variations in attack to still provide accurate intrusion detection [3]. Below in [2, fig. 1] is an example of association rules.

Association Rules	*Meaning*
Command = vi ⇒ time = am	When using vi to edit a file, the user is always editing a tex file, in the morning and at host Bluedawg and 25% of the data has this pattern.
Host = Bluedawg	
Arg = tex	
(confident = 1.0, support = 0.25)	
Command = vi ⇒ time = am	The mail is 75% sent to boss, in the morning and at host Bluedawg and 19% of the data has this pattern.
Host = Bluedawg	
Arg = boss	
(support = 0.25, confident = 0.75)	

Fig. 1. Example of association rules.

Genetic programming algorithms are another example of a supervised machine learning model and do exactly as what it sounds like they would do. Genetic programming algorithms create successive iterations of computer programs in order to learn to detect threats, learning from the failures of the last iteration. It is effectively a searching algorithm that maintains an initial "population" of programs and then based on the results mutates and applies crossover to them in order to improve the effectiveness of its detection methods [5].

Support vector machines, or SVMs, Are another type of supervised machine learning algorithm. They are relatively similar to artificial neural networks, however support vector machines perfrom structural risk minimization, while artificial neural networks perform empirical risk minimization. This allows SVMs to play more nicely with other techniques and algorithms, because the primary concern of SVM systems is structural. In [2], an application study performed by S. Mukkamala et al. in which an SVM was applied to detect patterns associated with intrusions and breaches. They note that the procedure for SVM detection has three steps: First, the input and output is extracted from web servers, user logs, and the authority log. Second, the training of the SVM occurs with data obtained from the first

step, then the ability of the system to classify this data is tested [2].

Decision trees are defined as an unparametric learning method which does not rely on specific data types. This is another type of supervised learning algorithm. They have high classification accuracy and as such are excellent for threat and intrusion detection. Decision trees run from a root node to leaf nodes, which then branch off to other leaf nodes when needed. These types of algorithms are extremely popular due to their high efficiency and skill in handling large amounts of data. Decision trees have an unfortunate tendency to overfit, or following their parameters for classification too closely and missing detections [2].

The final type of supervised machine-learning types to discuss is Bayesian networks. Bayesian networks take their name from Bayesian statistic, which in turn take their name from statistician Thomas Bayes. Bayesian networks have arose in response to a need for rule-based detection that takes context of the data into consideration, as they are known for false alarms in which a user triggers the intrusion detection system while performing a normal action. Bayesian networks solve this problem by running the same data through them first upon detection to find the probability of an actual intrusion [2].

B. *Unsupervised Learning Methods*

Unsupervised detection methods are detection methods which, as can be assumed, do not directly rely on human intervention to learn to detect intrusions. Algorithms which learn using these methods more frequently are used in anomaly-based intrusion detection systems. In these learning methods, data is fed in from datasets, but without labels appended to the data, as opposed to supervised learning where there are labels for data to help decide on the correct course of action. Much like supervised detection methods, the methods herein are not necessarily exhaustive.

Nearest Neighbor based learning is one example of an unsupervised learning technique that measures anomalies based on either the distance of the points of data on a graph from one another, or the relative density of points when grouped together. When it goes over the threshold, it becomes an outlier and thus a possible intrusion. Nearest neighbor techniques are noted for their simplicity, being one of the simplest machine learning models. Below in [2, fig. 2] is an example of COF (connectivity-based outlier factor) and LOF (Local outlier factor) neighborhoods and how they might be visualized using this technique.

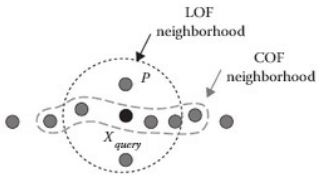

Fig. 2. Visualization of COF and LOF neighborhoods.

Clustering is a technique originating from statistics based around the grouping of unorganized data according to similarity of the data to each other. It is one of the most common methods used in machine learning, and thus in anomaly-based machine learning techniques used in intrusion detection systems. There are a number of different kinds of clustering, such as k-means clustering, where the number of clusters is determined by the division of *n* number of points into *k* number of clusters. The number of clusters in k-means clustering is determined by the nearest mean of grouping of points [6]. Below in [11, fig. 3] is an example of how a k-means clustering algorithm is visualized.

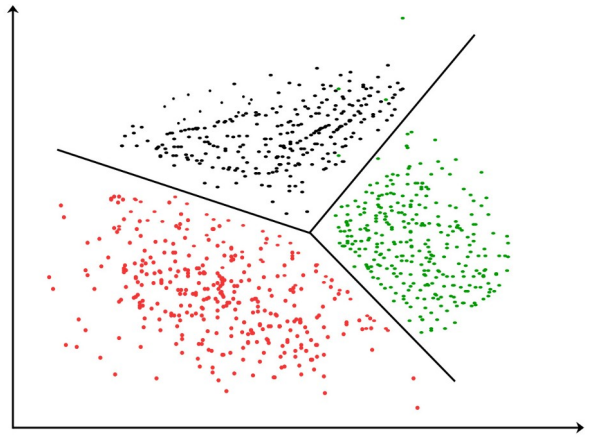

Fig. 3. Visualization example of k-means clustering.

Autoencoding is another form of unsupervised learning used in the intrusion detection systems. An autoencoder is a type of neural network that is designed to take unencoded data, encode it, and then reconstruct it as close as it can get to the original data in order to understand and classify the data. This is also to understand any of the relationships of the data to other data, and also any special relationships specific to that data. Autoencoding is used in networking-based intrusion detection systems to detect threats and intrusions within the network [7].

C. *Ensemble Learning Methods*

Ensemble or hybrid learning methods are a combination of any of the above methods, supervised or unsupervised, in order to create and more robust and precise system. For example, an SVM may be used with unsupervised techniques in order to more efficiently detect and intrusion. This may be done by mixing association rules with clustering, autoencoders or ANNs, or even genetic programming with any of the aforementioned methods. The benefits of such methods is that one technique might cover for the shortcomings of other techniques, such as the tendency for association rules to fail in detecting minute variations of an attack [8].

An important part about ensemble/hybrid techniques is that they rely on independent decisions made by a combination of intrusion detection methods or systems, and not just one intrusion detection system. Hybrid systems can thus detect intrusions that might have been missed by a signature-based method or system while also bolstering the ability of anomaly-based detection systems in their ability to detect anomalous activity. However, there is not a guarantee that a hybrid system will necessarily be better than a non-hybrid system, as use cases are always important in machine learning techniques used in intrusion detection systems [2].

Now to talk about Artificial neural networks or ANNs, as they've been mentioned before. Artificial neural networks are a learning algorithm or system of algorithms capable of learning and detecting potential attacks even if the data has

been badly damaged in some way or heavily distorted. This is useful in particular in network intrusion detection systems, as an ANN provides a faster response time and can process nonlinear data much better than other methods. The success of an ANN relies upon the learning of the weights of various sets of data and adjusting for it to determine the data's importance in the detection of an intrusion. An ANN can be combined and incorporated within a rule-based system, where the neural network acts as a filter and making sense of erroneous data before giving it to the rule-based system. Thus, ANNs can also be used in an unsupervised or supervised manner, or in conjunction with other techniques [4]. Reference [2] however notes that SVMs can typically outperform ANNs at intrusion detection due to difficulty of implementation with other methods.

Random forests are used semi-frequently as well in IDS systems. Random forests are a type of ensemble learning used for regression and classification, but also other tasks. It works by creating a "forest" of decision trees, and the mean result of these trees is the classification for the data it is processing. This helps diminish the overfitting problem in decision trees. They have been applied very broadly in many ways, both in supervised learning and unsupervised learning methods, to great effect [2].

Reference [9] mentions in their report the usage in the healthcare field of at least one IDS using "stacked autoencoders", that being autoencoders combined with other methods such as fuzzy logic, clustering, and association rules in order to improve intrusion detection. This was mentioned with other techniques that were used in conjunction to one another to improve detection.

IV. Impact of Intrusion Detection Systems

The impact of intrusion detection systems on overall system and network security is quite noticeable. In [9] Bari et al. have found that within the healthcare field, patient data is much more efficiently handled through the use of an intrusion detection system, in particular the effectiveness of clustering algorithms in the healthcare field. However, in the same report, it is noted that there are challenges faced by such systems, namely on limitations of machine learning. Machine learning-based intrusion detection can have issues with false positives, or ordinary actions by human users that are interpreted by the intrusion detection system as an intrusion or breach.

The automation of cybersecurity systems is often considered a continuing and future trend within cybersecurity, and as such, the ability to streamline and refine the detection of breaches and intrusions is incredibly important to the well-being of corporate, medical, and government systems alike. With an IDS that is able to look at data with context and analyze the finer minutia that a human observer may miss, it makes and entire world of difference to the professional behind the screen to make safety decisions optimally and efficiently.

V. Conclusion

In this paper, an overview of intrusion detection systems is provided. Types of algorithms are described according to the type of teaching and training used for them to detect intrusions. They are grouped into three separate categories, supervised, unsupervised and ensemble, and then individually explained within the context of an intrusion detection system. The impact of these systems on the overall security landscape is illustrated, noting that while there are limitations to machine learning, intrusion detection is overall more efficient when handled by an intrusion detection system.

Intrusion detection systems are an important utility moving forward in cybersecurity, as automation and automated systems like them will continue to grow in popularity and use. The future is sure to yield more exciting new methods to implement in intrusion detection systems, given the palpable potential of machine learning in theory and practice. Assuredly the rate of detection will also improve as technology advances.

References

[1] N-able, "Intrusion detection system (IDS): Signature vs. anomaly-based - N-able," *N*, 05-May-2021. [Online]. Available: https://www.n-able.com/blog/intrusion-detection-system. [Accessed: 16-Nov-2022].

[2] S. Dua and X. Du, *Data Mining and machine learning in Cybersecurity*. Boca Raton: CRC Press, 2011.

[3] D. Selvamani and V. Selvi, "Association rule mining for Intrusion Detection System: A survey," *Asian Journal of Engineering and Applied Technology*, vol. 8, no. 1, pp. 20–24, 2019.

[4] S. S. Roy, A. Mallik, R. Gulati, M. S. Obaidat, and P. V. Krishna, "A deep learning based artificial neural network approach for intrusion detection," *Communications in Computer and Information Science*, pp. 44–53, 2017.

[5] U.-M. O'Reilly, "Genetic Programming: A Tutorial Introduction," in *Proceedings of the 15th annual conference companion on Genetic and evolutionary computation*, pp. 247–264.

[6] "Clustering in machine learning," *GeeksforGeeks*, 23-Aug-2022. [Online]. Available: https://www.geeksforgeeks.org/clustering-in-machine-learning/. [Accessed: 16-Nov-2022].

[7] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the Classification Effectiveness of Intrusion Detection by Using Improved Conditional Variational AutoEncoder and Deep Neural Network," *Sensors*, vol. 19, no. 11, 2019.

[8] E. M. Maseno, Z. Wang, and H. Xing, "A systematic review on Hybrid Intrusion Detection System," *Security and Communication Networks*, vol. 2022, pp. 1–23, 2022.

[9] T. Bari and M. Abualkibash, "The Impact of Intrusion Detection Systems upon Healthcare Environments: A Research Review," in *Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management Singapore, March 7-11, 2021*.

[10] M. N. Mohammed and N. Sulaiman, "Intrusion detection system based on SVM for WLAN," *Procedia Technology*, vol. 1, pp. 313–317, 2012.

[11] "Clustering in machine learning," *GeeksforGeeks*, 23-Aug-2022. [Online]. Available: https://www.geeksforgeeks.org/clustering-in-machine-learning/. [Accessed: 16-Nov-2022].