Exploring Machine Learning Algorithms for Cyber Attacks' Classification

NVA Pavan Kumar Inguva[1], Oludotun Oni[2], Jacob Bryant[3]

Research Scholar, School of Information Technology, University of the Cumberlands, Kentucky, USA [1]

Professor,School of Information Technology, University of the Cumberlands, Kentucky, USA [2]

Adjunct Professor, PhD Leadership, University of the Cumberlands, Kentucky, USA [3]

Abstract*: Cyber security is like a race between defensive and offensive capabilities. Day by day the attacks are increasing consequently the preventive mechanisms are also raising. The technological evolution must address the cyber security problem effectively. Cyber security is always the cutting-edge technology to which Machine learning added potentiality. Machine learning plays a crucial role cyber-attacks in various dimensions. The recent advancements in usage of Machine learning towards cyber security preventive and detective measures clearly indicates that the Cyber security certainly accelerates. But at the same time the threat framework also takes the advent of innovative machine learning models. In this paper we are intended to explore various machine learning algorithms to classify cyber-attacks, which are very useful in designing efficient threat defensive models*

Keywords: Cyber Security, Machine Learning, cyber-attacks classification

I. INTRODUCTION

The current Network traffic is terrific and the future growth rate will be still enormous. Daily the transactions are growing at high pace. Proportionately the data required for analysis for the cyber criminals is increasing. Too much data for any single team of security professionals to analyse is a intricate task. Machine learning can be used to learn the underlying trends of the data which allows for future predictions, to classify threats and to differentiate malicious and normal network traffic.

Machine learning is the process of building a model, feeding sets of data with useful features so as to train the model and make it learn the underlying concepts. Consequently, the model gives the predictions for the future data and events. In the context of cybercrimes, it may be used to generate sophisticated and targeted phishing emails. Security analysts and organisations are capitalizing the technology in preventing cybercrime. With the ability of machine learning algorithms, the cyber attacks could be classified due to which appropriate cyber threat and attack classification could be done and finally strong cyber defense models could be built. In this section some machine learning concepts are discussed and in the succeeding section various machine learning models implemented to address various issues have been discussed. Finally, the process involved in cyber attack classification is discussed and thereafter the final section concludes our proposed procedures.

Machine learning is categorized into different types among which Supervised, Semi supervised and Unsupervised learning are of the broad classification.

The initial step in supervised learning, a task-driven method, is to label and feed the model data. From the standpoint of cyber security, samples of executable files are provided with information on whether or not the file is malware. The model is trained and then able to make judgements with respect to fresh data based on this labelled data. The limitation of the labelled data is a drawback.

The goal of ensemble learning is to find a solution by combining many basic models. It builds on top of supervised learning and uses a variety of approaches, even when merging very basic models.

In situations when labelled data is unavailable, unsupervised learning may be used to enable the model to self-learn using features. Given the impossibility of labelling all data, this data-driven learning approach is generally seen to be more powerful and designed to detect data abnormalities.

DOI: 10.48175/IJARSCT-19438

When some data has been tagged, a method called semi-supervised learning may take use of it, combining the best features of supervised and unsupervised learning.

When the behaviour has to respond to changes in the environment, one Environment Driven technique that may be used is reinforcement learning. It seems that the learning environment is based on trial and error.

Data optimisation, data categorisation, dimensionality reduction, and other operations all make use of Machine Learning techniques. Our main emphasis is on categorisation, whereby attack data is sorted into different groups using machine learning methods. As an example, consider an email system that employs a spam filter to isolate unwanted communications.

Logistic Regression (LR), K-Nearest Neighbours (K-NN), Support Vector Machine (SVM), Kernel SVM, Naïve Bayes, Decision Tree Classification, and Random Forest Classification are some of the Machine Learning approaches used for classification. Since their effectiveness is data-dependent, there is no universal algorithm that can be used universally.

II. LITERATURE STUDY

For data classification, the authors of [1] suggested a model that made use of the Decision Forest algorithm. Based on the accuracy and detection rate, the suggested ML method processed four types of attack data. Effective and accurate normal/abnormal data categorisation is the goal of the suggested strategy. Also, with little training and testing time, the invasions may be found in big datasets. For attack categorisation, we suggest an Azure ML-based model. This study used an ensemble approach and a multicast decision forest, both of which outperformed the benchmark in terms of accuracy. Additional optimisations might be made to the model to accommodate unbalanced datasets from other sources and domains. It could also be adjusted for use on the Hadoop Map Reduce platform.

In order to conduct network intrusion detection, the authors of [2] used feature selection and machine learning methods on four different datasets: ISCX-URL-2016, NSL-KDD, CICIDS-2017, and NSL-KDD. Following a baseline phase, the machine learning algorithms were then linked with feature selection techniques. Afterwards, the four top algorithms were compared with each other in terms of processing time and accuracy. The result is a variety of suggestions for network intrusion detection algorithms that use feature selection in different ways. The study led to the creation of other combinations, including Decision Tree and ExtraTree Classifier, Decision Tree and SelectKBest, Decision Tree and Variance Threshold, and Decision Tree and Select Percentile. While the overall processing time was drastically cut, the accuracy standards were maintained by the combinations. We also discovered that the algorithms are quite reliable. huge data sets, lengthy processing times, a huge number of features, data manipulation, and class imbalances are just a few of the difficulties that arise when dealing with algorithms and data. Additionally, the dataset's complexity and lack of intuitiveness is the main limitation encountered while dealing with cyber security data. The elimination of strongly correlated characteristics may not be optimised by a human approach, thus automated feature selection is the emphasis instead. This is because of the intricacy involved. This is due to the fact that the data's fundamental structure and meaning are murky and complicated. Using hyper-parameter tweaking and cross-validation to get the first baseline machine learning statistics might expand this paper's study. To further optimise the detection and classification in terms of processing speed and accuracy, further sophisticated machine learning (neural network) algorithms and other methods might be used.

In [3], the approach is contrasted with a solution for injection attack detection that is well-known in the literature. In response to the dismal performance of existing signature-based solutions for SQL injection attacks, we present an algorithm that merges the best features of ADS with signature-based methods; this allows us to achieve detection effectiveness that is significantly better than signature-based methods.

Apache SNORT, ICD, and SCALP are used for comparisons. An Apache server access log file analyser is Apache SCALP. The suggested method can identify and categorise several forms of web application-targeted assaults. According to the findings, SCALP and Snort are not very effective. The solutions have the benefit of being simply able to feed fresh signatures. Additionally, the current criteria are designed to identify attacks that often target specific weaknesses in web-based applications.

In their work on identifying assaults on IoT networks, Alsemiri et al. [4] focused on machine learning. The unique properties of the Bot IoT data set, including frequent updates, a variety of network protocols, and a broad variety of attacks, led them to adopt it. Using CICFlowMeter, the flow-based characteristics were retrieved from the raw traffic traces. The 84 network traffic characteristics defined by CICFlowMeter are what make up the network flow. We employed the Random Forest Regressor method to determine the feature weights, which were then used in the machine learning approaches. In the first approach, weights were determined for each assault type separately; in the second, group computations were carried out with all of the attacks combined into one. The next step was to identify the shared characteristics that were critical to every assault. They employed seven popular but distinct tools in their investigation. The F-measures for the selected algorithms—Naive Bayes, QDA, Random Forest, ID3, AdaBoost MLP, and K Nearest Neighbours—were 0.77, 0.86, 0.97, 0.97, 0.83, and 0.99, correspondingly. This might serve as a springboard for building a multi-layered model that incorporates several machine learning methods for enhanced performance.

The cyber security battle is becoming more difficult due to factors such as cloud computing, increasing Internet use, changing network infrastructures, mobile operating systems, and ever-evolving network technologies. These are the new problems that have recently emerged, and in order to fix them, network security systems, protection plans, and sensors will need to advance significantly. Such difficulties were discussed in [5]. They zeroed emphasis on new forms of application layer cyber assaults because of the apparent severity of these threats. Patterns expressed as Perl Compatible Regular Expressions (PCRE) make up the model. A combination of dynamic programming and a graph-based segmentation method yields these. With a false positive rate of less than 4.5 percent, the suggested method achieved a performance level of 94.46%.

Software known as an Intrusion Detection System (IDS) keeps tabs on computers, either individually or in a network, to see whether somebody is trying to steal data or break the protocols of the network. Modern intrusion detection systems (IDS) aren't up to the task since cyberattacks are more sophisticated and ever-changing. Consequently, machine learning approaches are more suited to these types of systems. In addition to reduced false alarm rates, these methods also have tolerable transmission and computation costs. The authors conducted an in-depth analysis and performance comparison of many similar methods in [6]. They sorted all the plans into two groups: those that relied on traditional AI techniques and those that relied on computational intelligence. They have also detailed the ways in which different CI method features may be used to create effective IDS. Another benefit is that this kind of system can easily adjust to new forms of harmful behaviour.

Analysis of the models studied:

A wide variety of models which addressed the cloud technology attacks, attacks targeting web applications, IoT based attacks, targeted Intrusion Detection system and other ones were explored which are promising in detection and classifying the cyber attacks. They were modelled on various cyber data sets. The machine learning techniques applied in the models gave promising solutions which are capable in classifying the data and predicted detections. Accuracy is the outcome of dividing the number of properly categorised examples by the total number of occurrences. Processing time refers to the duration required to process the data in order to achieve precise categorisation. All the models demonstrated superior performance when compared to each other. All the models followed the similar procedure which was given below.

1. Pre-process the dataset.
2. Divide the data into random groups of 70% training and 30% testing, or 80% training and 20% testing.
3. Figure out what categorical traits are and turn them into categorical features.
4. The fourth step is to use the Convert to Indicator Values tool to turn columns with category values into features that are easier to use.
5. Bring the information in or upload it.
6. Pick out the columns in the dataset that are important.
7. Train the model with a machine learning algorithm.
8. Give the model a score and rate it. The "Evaluate model" also shows how the results will look..

III. CONCLUSION

It is evident that machine learning is being used effectively in cyber security in a wide range of applications. Machine learning was used in cyber security to identify malware and malicious links. In cyber crime it is used to avoid 'captcha' checks, generate targeted phishing emails and elude filters. Cyber security appears to have much more consolidated uses for machine learning. The experiments that used various classification techniques are evaluated in terms of two metrics – accuracy and processing time. The models explored in this paper exhibited notable performance in terms of metrics and the used techniques for diversified cyber security problems.

REFERENCES

[1] Chourasiya, Rahul, V. Patel and Anurag Shrivastava. "CLASSIFICATION OF CYBER ATTACK USING MACHINE LEARNING TECHNIQUE AT MICROSOFT AZURE CLOUD." (2018).

[2] Alexander Powell, Darren Bates, Chad Van Wyk, and Adrian Darren de Abreu, "A cross-comparison of feature selection algorithms on multiple cyber security data-sets", FAIR2019

[3] Kozik R., Choraś M. (2014) Machine Learning Techniques for Cyber Attacks Detection. In: S. Choras R. (eds) Image Processing and Communications Challenges 5. Advances in Intelligent Systems and Computing, vol 233. Springer, Heidelberg. https://doi.org/10.1007/978-3-319-01622-1_44

[4] Alsemiri, Jadel &Alsubhi, Khalid. (2019). Internet of Things Cyber Attacks Detection using Machine Learning. International Journal of Advanced Computer Science and Applications. 10. 10.14569/IJACSA.2019.0101280.

[5] M. Choraś and R. Kozik, "Machine learning techniques applied to detect cyber attacks on web applications," in Logic Journal of the IGPL, vol. 23, no. 1, pp. 45-56, Feb. 2015, doi: 10.1093/jigpal/jzu038.

[6] Zamani, Mahdi. (2013). Machine Learning Techniques for Intrusion Detection.

[7] D. Kong, J. Gong, S. Zhu, P. Liu and H. Xi. SAS: semantics aware signature generation for polymorphic worm detection. International Journal of Information Security, 50, 1–19, 2011.

[8] M. Sharma and D. Toshniwal. Pre-clustering algorithm for anomaly detection and clustering that uses variable size buckets. RecentAdvances in Information Technology, 515–519, 2012.

[9] M. Zmyslony, B. Krawczyk and M. Wozniak. Combined classifiers with neural fuser for spam detection.In:HerreroA.etal.(eds.),AdvancesinIntelligentSystemsandComputing,Vol.189, 245–252, Springer, 2012.

[10] R. Vijayasarathy, S. V. Raghavan and B. Ravindran. A system approach to network modeling for DDoS detection using a Naive Bayesian classifier, Communication Systems and Networks (COMSNETS), 2011 Third International Conference on, pp. 1–10, 4–8 Jan. 2011.

[11] P. Barthakur, M. Dahal and M. K. Ghose. A Framework for P2P Botnet Detection Using SVM. 2012 International Conference, Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) pp.195–200, 10–12 October 2012.

[12] Stefano Zanero and Sergio M. Savaresi. Unsupervised learning techniques for an intrusion detection system. In Proceedings of the 2004 ACM symposium on Applied computing, SAC '04, pages 412–419, New York, NY, USA, 2004.

[13] Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. Review: Intrusion detection by machine learning: A review. Expert Syst. Appl., 36(10):11994– 12000, December 2009.

[14] Srinivas Mukkamala, Guadalupe Janoski, and Andrew Sung. Intrusion detection using neural networks and support vector machines. In Proceedings of the 2002 International Joint Conference on Neural Network (IJCNN), volume 2, pages 1702–1707, 2002.

DOI: 10.48175/IJARSCT-19438