Improving Cyber Security using Artificial Intelligence

J Ramyashree[1] and Hemavathy R[2]

[1,2]*Department of Computer Science and Engineering, Rashtreeya Vidyalaya College of Engineering, Bangalore, Karnataka, India.*

Abstract — In a world where there is an increasing number of cyber security threats, there is a need for faster and more cost-effective way of detecting and responding to threats. This paper deals with how we can use artificial intelligence to improve cyber security. The methodology used is to use Splunk to get the fields which we are interested in and feed that data to K-means algorithm which forms clusters of subsets of the attacks. Then those clusters are fed into individual ANNs from which the aggregated results are fed into SVM which outputs whether the attack is malicious, non-malicious or benign.

Keywords — Artificial Intelligence, Cyber Security, Machine Learning, Supervised Learning.

I. INTRODUCTION

With the rise of Machine Learning, there is also a rise in cyber-criminality. Due to this we need a faster way of detecting threats and responding properly. Using ML makes the task faster. What takes a Cyber Security operation team two days to figure out, ML can figure it out in a day and since ML continuously learns based on experience and results, it will take lesser and lesser time to understand and figure out what's happening. Machine learning is technique wherein the machine, given the necessary data will be trained and thereon will start learning on its own. Its accuracy of prediction increases with more data and time. Three main techniques for machine learning are supervised, semi-supervised and unsupervised. Supervised learning refers to a technique of training on the data which is already labeled and predicting output from the given labeled input. Unsupervised learning refers to a technique where the algorithm tries to find patterns in the data and gives output. Semi-Supervised technique is where the algorithm trains on a labelled and unlabeled but mainly on unlabeled data. K- Means clustering is an unsupervised technique. It is a technique where we initialize k points randomly, each point is categorized to its closest mean, and this step is repeated till we get our clusters. ANN is artificial neural network where the neural nets are trained by giving weights to yield various results. SVM is a supervised technique wherein there is a line called hyperplane which classifies the plotted data points into the different clusters.

There are many kinds of cyber threats such as ransomware, botnet, trojan, Advanced persistent threat, DDOS, Man in the middle attack, phishing, spyware, wiper attacks, malware, etc. An Intrusion detection system (IDS) is a process wherein the whole intrusion detection process is automated. An Intrusion prevention system (IPS) is a process wherein it can not only detect attacks but also prevent the possible attacks. Given the increasing number of cyber-crimes today, we need a system which can detect and prevent attacks.

The attack which occurs could be accidental,intentional or unintentional and cause various issues like loss of data, data access, data modification, etc.

The whole purpose of computer security is to detect and prevent use of the system without any authorization. Destruction or any kind of modification to data is prevented.

Fire-walls, anti-viruses, suites are some of the examples of computer-security. There are different kinds of Threats and classified such as-

A. Physical Threats

Physical threats when there is physical damage to the hardware and infrastructure caused by fire, earthquake, landslide, etc

B. Non-physical Threats

These are the kind of attacks which could lead loss or corruption of sensitive data, monitoring of computer systems illegally, breaches in cyber security, etc. Some of the examples of these kind of threats are key loggers, virus, worms, adware, phishing, DDOS, spyware, DOS, etc.

II. LITERATURE REVIEW

A brief literature survey was carried out to gain understanding about various concepts like cyber security threats and machine learning algorithms. Excerpts from a few of the papers/ journal referred are as follow:

Noor Ahmed et. al. gives an overall description about the various kinds of IDS and how different algorithms are used to detect IDS and their performance. [1].

Jack W Stokes et. al speaks about how static malware analysis is not so efficient due to the fact that malware is usually in the encrypted format and how attackers can make small changes to the input and avoid the malware being detected. The technique used in this paper is adversarial attack strategies against a dynamic malware analysis classification system. [2].

Cristian Pascariu et. al speak about applying machine learning for analysing the dynamic malware process. This is applied for Windows operating System. This technique focuses on the process hierarchy in a way that that will capture information about the created process and its parent process. The output will have a higher score if its malicious and a lower score if it's safe activity. [3].

Rahul Vigneswaran K et. al explains how to exploit the randomness of the incoming attacks which is not visible to the human eye but can be made better by using Artificial intelligence. Hence, by training the algorithm with existing cyber attacks, prediction will be done whether the attack is malicious or not. Due to this, the time and cost to detect becomes increasing less.[4].

S. Ponmaniraj et. al takes the TCP/IP parameters as input and analysing the network security. The intrusion detection system deals with huge networks congestion highly irregular based data pattern. The difference between regular and irregular or anomaly pattern data sets are, regular pattern has certain static derived input and expected output sets whereas irregular all kind of data are processing as input and dynamically they are getting change in its behaviours. Regular data set cannot change over a time whereas irregular pattern will get change and therefore classification and prediction model must be changed accordingly. In networks intrusion detection can be classified into misuse and anomaly detection. Detection of misuse found by trained data set and well known attacking methods with predicted output results. Anomaly detection dealing with unknown data sets which shows variations in usual set of normal behaviours or patterns unknown to the system to detect. [5].

III. METHODS

A. *Experimental Setup*

The various tools and programming languages used while carrying out the experiment is as follows:

- Splunk Enterprise version
- Jupyter Editor
- Splunk Programming Language
- Python

B. *Design Modules*

The modules that make up the entire system is depicted in Figure 1.

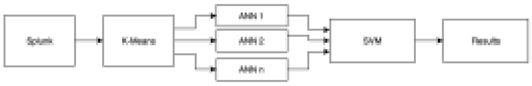

Figure 1. Design Modules

Splunk is a software that captures real time data and indexes,correlates and presents the data in a way which can be searched and visualized easily which can be widely and esily applied for cyber security.

K-means is an algorithm which is unsupervised learning technique which is used to find patterns in the data and find clusters. Data points based on the similarity of data points are clustered. The number of clusters are pre-determined and that is known as K.

Artificial neural networks are statistical models which try to model the human brain. There are nodes in the ANN which conveys the data to the next neuron and so on till it is fed to the output nodes. After this, labels can be given to the output.

SVM is an algorithm which is used primarily for classification and it is a type of supervised type of algorithm. There is a hyper plane which is a line which classifies the labelled data points into different classes.

C. *Implementation*

The data is fed from the NSL-KDD dataset into the Splunk Indexer which is used for parsing and indexing the data, the resulting data is fed into Splunk Forwarder which is used for data forwarding. The reason Splunk is chosen for choosing the relevant features instead of PCA is because the types of malicious activities is fixed and hence the features will be constant and the efficiency will be more.

Based on the features selected, the data is split into 7:3 ratio of training and testing respectively. The training data is fed into the K-Means algorithm and clusters of data are formed.

This clusters of data are fed into the individual ANN and the various results are obtained.

The aggregated results are fed into the SVM which gives the results of whether the attack is malicious, non malicious or benign.

IV. RESULTS AND ANALYSIS

The data that are analyzed using these algorithms. All the algorithms were trained with a total of 400 samples with 280 training samples and tested with test data set containing 120 samples. All the four different types of algorithms were compared and the accuracies obtained were:

Method	Accuracy	Precision	Recall	F1 Score
K Means and SVM	0.7843	0.81	0.83	0.79
PCA, K Means and SVM	0.8540	0.86	0.84	0.82
Splunk, K-Means and SVM	0.8756	0.84	0.86	0.87
Splunk, K-Means, ANN and SVM	0.9256	0.94	0.93	0.94

Table I : Comparison of different models

By this we can observe that by far, using the combination of algorithms initially it could be time consuming but as training progresses, this is by far the most efficient method.

V. CONCLUSION

It is impossible to prevent cyber-crimes completely, by using the current technologies in security. In this paper, an efficient method intrusion detection system is proposed to detect whether the attack is malicious, non-malicious or benign. Taking the help of Splunk to get the important features after which the data is fed to K Means to get a cluster of subsets.After obtaining the clusters, training will be given to the individual artificial neural networks separately and after which the aggregated results is fed into the SVM which classifies the attacks as malicious, non-malicious or benign. The dataset considered here is the NSL-KDD dataset. The evaluation metrics here is accuracy, precision, recall and F-square. The results show that the approached method is efficient.

REFERENCES

[1] Noor Ahmed Biswas and Wasima Matin Tammi " FP-ANK: An Improvised Intrusion Detection System with Hybridization of Neural Network and K-Means Clustering over Feature Selection by PCA " in 18th Internation Conference on Computer and Information Technology (ICCIT),2015.

[2] Jack W Stokes and Md Amran Siddiqui "Detecting Cyber Attacks with explanations and Expert Feedback", in: ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)

[3] Cristian Pascariu and Ionut-Daniel Barbu "Dynamic analysis of malware using artificial neural networks" in ECAI 2017 - International Conference – 9th Edition,2018,pp.67-71.

[4] Rahul Vigneswaran K, Vinayakumar R " Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security" in 9th ICCCNT 2018,pp.26-29.

[5] K. Ibrahimi and M. Ouaddane, "Management of intrusion detection systems based-kdd99: Analysis with lda and pca," in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017, pp. 1–6.

[6] N. Moustafa and J. Slay, "The significant features of the unsw-nb15 and the kdd99 data sets for network

intrusion detection systems," in Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2015 4th International Workshop on. IEEE, 2015, pp. 25–31.

[7] L. Sun, T. Anthony, H. Z. Xia, J. Chen, X. Huang, and Y. Zhang, "Detection and classification of malicious patterns in network traffic using benford's law," in Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864–872.

[8] S. M. Almansob and S. S. Lomte, "Addressing challenges for intrusion detection system using naive bayes and pca algorithm," in Convergence in Technology (I2CT), 2017 2nd International Conference for. IEEE, 2017, pp. 565–568.

[9] M. C. Raja and M. M. A. Rabbani, "Combined analysis of support vector machine and principle component analysis for ids," in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5.

[10] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," Journal of Computational Science, vol. 25, pp. 152–160, 2018.

[11] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.

[12] R. Christopher, "Port scanning techniques and the defense against them," SANS Institute, 2001.

[13] S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.

[14] E. Gerhards-padilla and F. Fkie, "Intrusion Detection in Tactical Multi-Hop Networks," 2009.

[15] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1. IEEE, 2003, pp. 130–138.