Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 8, No. 4, December 2020, pp.2539-2546

Intrusion detection using machine learning-hardened domain generation algorithms

Mustafa Abdmajeed Shihab
Computer Science Department, Collage of computer Science and Mathematics, University of Tikrit

ABSTRACT

Machine learning has recently been applied in a variety of areas in information technology due to its superiority over the typical computer algorithms. The machine learning approaches are being integrated into cybersecurity detection approaches with the primary aim of supporting or providing an alternative to the first line of defense in networks. Although the automation of these detection and analysis systems is potent in today's changing technological environment, the usefulness of machine learning in cybersecurity requires evaluation. In this research, we present an analysis and address cybersecurity concerns of machine learning techniques used in the detection of intrusion, spam, and malware. The analysis will entail the evaluation of the current maturity of the machine learning solutions when identifying their primary limitations, which has prevented the immediate adoption of machine learning in cybersecurity.

Keywords: Machine Learning, Cybersecurity, Intrusion detection, Domain Generation Algorithm, Artificial Intelligence

Corresponding Author:

Mustafa Abdmajeed Shihab
Computer Science Department
Collage of computer Science and Mathematics
University of Tikrit
mustafa_shihab86@tu.edu.iq

1. Introduction

The pervasiveness and appeal of ML algorithms is increasing rapidly. The current approaches are being enhanced, and their potential to comprehend and solve real-life issues has continuously become desirable. These milestones have contributed to the adoption of ML algorithms in various technological areas such as medical analysis, computer vision, game social media marketing [1]. In a number of these applications, machine learning (ML) algorithms have been viewed as the best option over the original rule-based algorithms or human-based operators [2]. This changing mode is also impacting the cybersecurity field, with more systems being upgraded using the machine learning algorithms [3]. Although a lot has been done in terms of incorporating ML components into cybersecurity, designing a wholly automated cyber defense system is still a foresighted objective. The first layer experts in network and security operations centers have benefited considerably in the areas of detection and analysis elements that are reliant on machine learning. This paper addresses the application and maturity of current ML solutions in cybersecurity to identify the primary limitation and highlight the possibilities of enhancements. This study was completed through a comprehensive review of literature and novel experimentation on real, large Enterprise, and network traffic. Furthermore, the results were compared with other findings from academic papers, especially machine learning solutions for cybersecurity through consideration of various specific applications. Most researches have oriented their findings on artificial intelligence (AI) rather than cybersecurity [4]. In this evaluation, our analysis excluded commercial products that utilize machine language as most of these vendors rarely reveal the underlying algorithms and occasionally ignore the issues and limitations associated with the application of the ML [1]. In the review, we present the classification of machine learning in cybersecurity approaches. Secondly, we then relate these are algorithms to three specific cybersecurity problems in which machine learning has been used: malware analysis, spam, intrusion, and phishing detection. Ultimately, we analyze the shortcomings of these existing techniques.

The aim in this study, we highlight the advantages and limitations of the various machine learning approaches in cybersecurity, especially in terms of false-negative and false-positive alarms. This analysis is made primarily based on the complexity of managing machine learning architecture in cybersecurity and the absence of data for training, especially during fine-tuning of operations in applications that are characterized by continuous variation.

Problem

The recent increase in adversarial attacks on different technological systems has been made capable by the ease with which the attacks can evade the ML detectors. The drawbacks evidenced in this research will provide a pathway for future enhancement of ML components needed prior to full adoption into the cyber defense platform.

1.1. Literature Review

Machine learning (ML) entails an array of paradigms in continuous evolution, highlighting weak demarcation and cross relationships. Moreover, various applications and views may lead to variations in classification. Therefore, a single taxonomy is not enough to classify machine learning algorithms, but for the case of this research, we will utilize the original taxonomy presented in figure 1 [2]. This figure captures the difference in the myriad of techniques used in cyber detection. This taxonomy is also tailored for cybersecurity and avoids the ambiguity associated with the AI classification. In terms of cybersecurity, machine learning can be divided into shallow learning (SL) or the reason for the development of deep learning (DL) [5]. The shallow learning techniques require a domain expert who will be responsible for performing the critical task of identifying pertinent data features prior to executing the SL algorithms. In the case of deep learning, the system incorporates a multi-layered representation of input data performing autonomous processes in defined representation learning; thus, eliminating the need of a domain expert. Table 1 below illustrates the various uses of ML in cybersecurity [6].

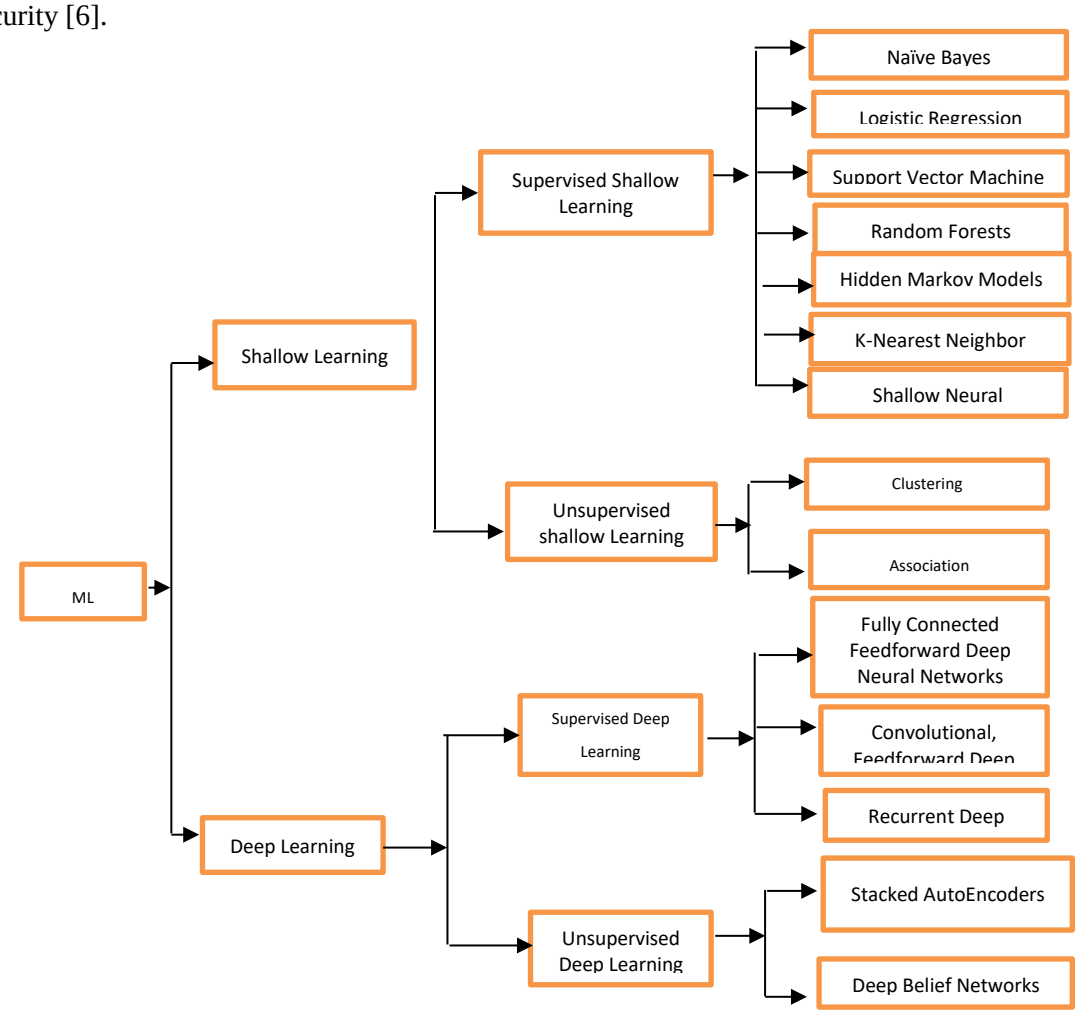

Figure 1. The taxonomy of machine learning based on cyber security applications [2]

The supervised ML algorithms require a training process that entails the use of a huge and representative set of data which may have been previously classified and prepared by experts via a variety of techniques [2]. Unsupervised ML algorithms do not need a pre-labeled training dataset.

2. Machine learning algorithms in cyber security

2.1. Malware analysis

This process is fundamental as existing malware can automatically produce novel variants of itself, i.e., mutate with similar malicious impacts but manifesting in entirely varied executable files [7]. The metamorphic and polymorphic characteristic of this modern malware defeat the typical rule-based malware identification techniques [8]. The machine learning approaches can be applied in the analysis of malware forms and successfully classifying them to the respective malware family.

2.2. Intrusion detection

Intrusion detection is a cyber-security technique aimed at detecting illegal activities within a computer or enterprise network using intrusion detection systems (IDS) [1]. IDS have been broadly implemented in modern, computer, and enterprise networks [9]. Originally, these systems traditionally relied on the structures of familiar attacks, but the modern IDS are deployed to evaluate the methods for threat detection, anomaly detection, and classification through ML [10]. In this study, we will evaluate two detection problems, i.e., botnets and domain generation algorithms (DGAs). In cybersecurity, a botnet is a collection of infected devices under the control of an attacker who uses these devices to conduct multiple illicit activities [11]. The identification of botnets is to detect the communication between the infected devices within the network under monitoring, as well as the external command-and-control server. The DGA is a system that automatically generates domain names, which are typically utilized by infected devices to correspond with the external server through the periodical generation of new hostnames [12]. The DGA presents a real peril for organizations as via them it is easy for attackers to evade defenses that are based on static blacklists of domain names.

2.3. Spamming and phishing detection

These approaches include a broad set of approaches that are aimed at decreasing the time wastage and potential hazards that can result from unsolicited emails [13]. Illicit emails, i.e., phishing, provides the first route for an attacker to establish a foothold in any computer or enterprise network. The phishing emails may contain malware or links to compromised websites that can be clicked by unsuspecting users [14]. Recently, phishing and spam detection have become difficult due to the advanced evasion methods implemented by attackers to bypass common filters [15]. The ML techniques can be used to enhance spam detection processes.

Table 1. The areas of application of machine learning in cyber security [3]

		Malware Analysis	Spam Detection	Intrusion Detection		
				Botnet	Network	DGA
Shallow Landing	Supervised	RF NB KNN SNN SVM LR HMM	RF NB SVM KNN LR SNN	RF NB SVM KNN LR SNN	RF NB KNN SNN SVM LR HMM	RF HMM
	Unsupervised	Association Clustering	Association Clustering	Clustering	Association Clustering	Clustering
Deep Learning	Supervised	FNN RNN CNN		RNN	RNN	
	Unsupervised	DBN SAE	DBN SAE		DBN SAE	

3. Methodology

In this section, we evaluate several cybersecurity issues to see the Machine learning algorithms can be applied in network security. The analysis is based on the assumption that no algorithm is regarded as entirely autonomous without any human supervision. The issues will be substantiated using experimental or results collected from the literature. For each case, the testing environment will be described as well as the metrics of consideration. These experiments will focus on network intrusion detection and DGA detection. The experiments will leverage the two most commonly used algorithms, i.e., Random Forest and Feedforward Fully Connected Deep Neural Network.

3.1. Analysis of intrusion detection

Three sets of real training data were used from benign and malicious network communication collected from large enterprise networks. These organizations had nearly 10000 hosts. These labels are generated by flagging malicious packets by raising alarms in the enterprise network IDS, which were reviewed by network experts. These training datasets are captured in table 2 below. Additional testing data of 50000 flows were collected from the Kaggle database. The primary areas of consideration for this data are captured in table 3 below. The datasets are employed in the testing and training of self-developed ML classifiers. The classifiers were developed from the Feedforward Fully-connected Deep Neural Network and Random Forests on different topologies. The FNN had neurons between 128 to 16384 on 2 to 16 layers while the RF is made of 100 decision trees based on the CART algorithms.

Table 2. The training data for the IDS [1]

Dataset	Benign Flows	Malicious Flows
1	100000	1000
2	250000	2500
3	500000	5000

Table 3. Feature included in the dataset [4]

Item	Features
1	Source/Destination IP Address
2	Incoming/Outgoing packets
3	Source/Destination port
4	Incoming/Outgoing bytes
5	TCP Flags
6	Protocols used
7	Duration of the flow
8	List of Alerts raised

The quality of every classifier is characterized using the following performance metrics: Recall, F1-score, and precision as expressed below

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1\ score = 2\ x \frac{Precision\ x\ Recall}{Precision + Recall}$$

Where
TP are the true positives
FP are the false positives
FN are the false negatives

For Completeness in this analysis, we take the true positives to be expected detection of malicious activities. Thus, the precision shows the extent to which a technique can provide correct results. The recall is a measure of the detection rate [1]. The F1-score is a combination of Recall and Precision to a single value. Accuracy is not used in this research as the number of legitimate events are greater than illegitimate events in an organization

thus the accuracy tends to be close to 1. These accuracy findings may prevent the full characterization of the classifiers. The results were used after a 10-fold cross validation to decrease the possibility of biased results.

DGA analysis

Two labeled datasets containing DGA and non-DGA domains were used for training. The first set contained DGA that was created using the commonly known technique while the second set contained DGA created with recent approaches. Non-DGA domains were collected from the Cisco Umbrella. Table 2 captures the training datasets in table 4 [1]. The test dataset was built from 10000 domains collected evenly from the training datasets. In addition, our research relied on unlabeled dataset containing 20000 domains from the large organizations. The features extracted from the data sets are captured in table 5.

Table 4. The training dataset for DGA detection

Dataset	DGA technique	Non-DGA count	DGA count
1	Common-known	20227	21355
2	Recent and well-known	8120	37673

Table 5. Extracted features

Item	Feature
1	n-gram normality score
2	Vowel-to-consonant ratio
3	Meaningful character ratio
4	Domain length
5	Number-to-character length

3.2. Comparison of shallow and deep learning

Traditionally, deep learning performance better than shallow learning in most network uses, especially in computer vision. In cybersecurity, the case may be different as some well managed-and-configured SL algorithms tend to be better than DL techniques. In this research, both SL and DL techniques were trained and tested [15]. To enhance the results, the training and test steps of these classifiers was repeated multiple times utilizing various topologies. The results for the best topology were computed using.

$$Accuracy = \frac{TP + FN}{TP + TN + FN + FP}$$

Where, TN are the true negatives

4. Results

For the FNN algorithm, the best topology consisted of 1024 neurons contained in four hidden layers. The RF classifier outperformed the FNN with an F1-score of 0.8 against 0.6 for FNN as illustrated in table 6 and figure 2.

Table 6. The comparison between SL and DL classifier

classifier	Precision	F1-Score	Recall
Full-connected Feedforward Deep Neural Network	0.7708	0.6085	0.5027
Random Forest	0.8727	0.7995	0.738

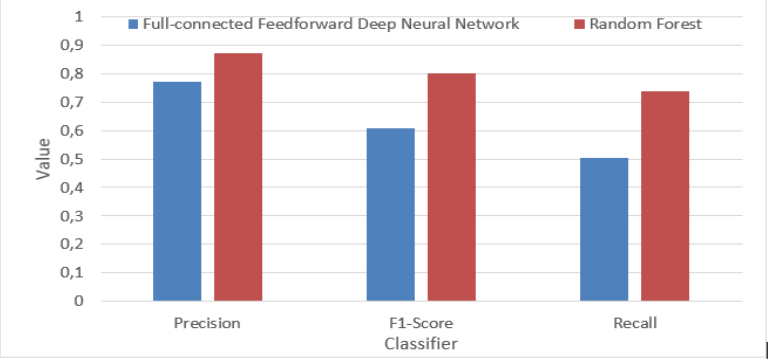

Figure 2. Comparison between SL and DL classifier

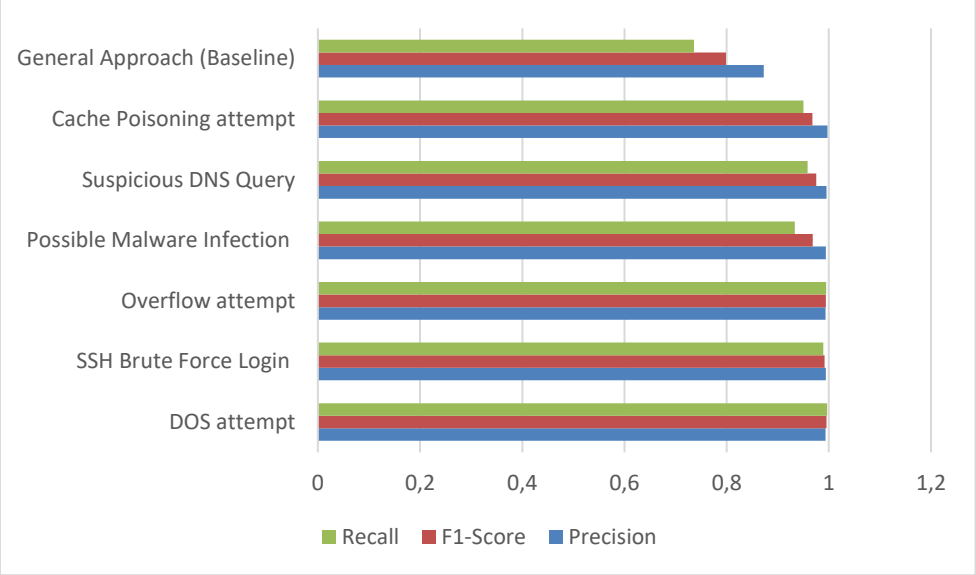

Figure 3. Comparison of general and specific detectors

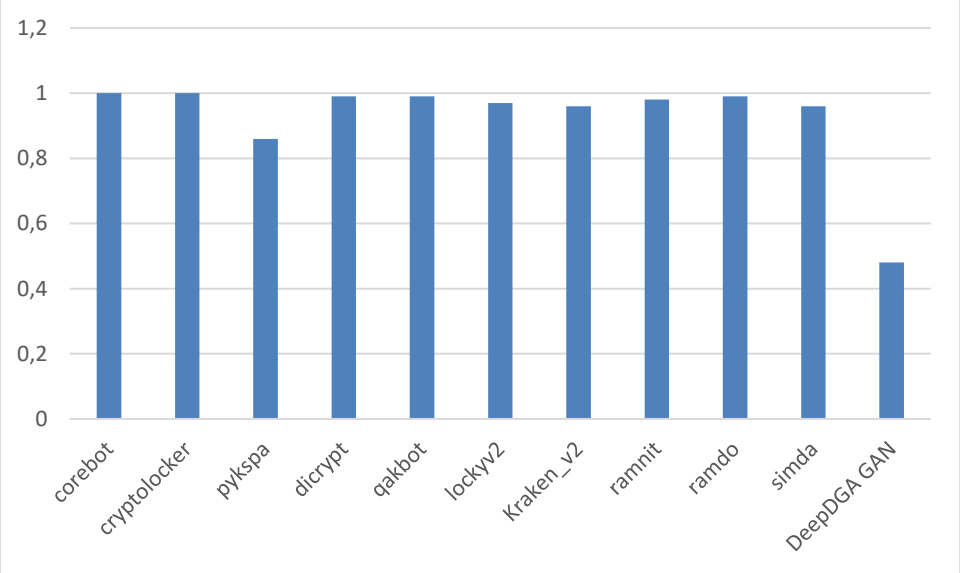

Figure 4. The DGA detection rate for the RF Classifier

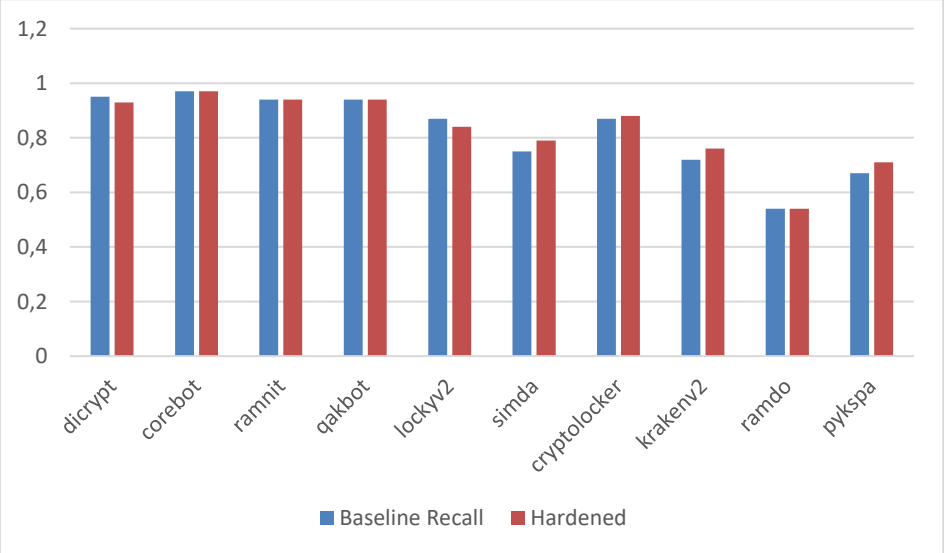

Figure 5. The performance of DGA before and After hardening

5. Discussion

The results in this analysis show that ML algorithms have superior performance in detecting cyber-attacks. The even perform better when they are finely tuned for a specific threat, such as illustrated in figure 3 rather than trying to detect an array of threats at once [16]. In this evaluation, we evaluated a number of intrusion detection systems that rely on the RF classifiers, each based on a particular type of attack. The classifiers had encouraging results on real network data with an F1-score of over 0.95. Similarly, the general classifiers were trained and tested; they performed poorly. This primary takes away for this analysis was that using ML detectors for a single identification process of malicious flows is rather than specific detection is unfeasible.

The modern-day attackers use new techniques to circumvent around detectors, even those based on ML algorithms [1]. The adversarial attacks might affect the integrity, privacy, and availability of the target system [16]. In terms of integrity violation, the attack will evade a clustering or classification algorithm by producing activities that appear legitimate. In the availability violation, the attack produces a vast number of legitimate events that can be considered as attacks; thus, increasing the number of alarms [17]. The privacy violation allows the attacker to obtain information from the target network through the exploitation of the defensive ML algorithm. The existing enhancement in deep learning has contributed to the creation of the generative adversarial networks (GAN), which are techniques based on DNN that automatically generates adversarial samples against a target ML system. The DeepGA was analyzed to determine the ability of GA evading the ML classifiers [1]. Figure 4 demonstrates the findings of the above experiment showing the first ten approaches and how they performed in detecting DGA [18]. The last column in figure 4 demonstrates the detection rate for DeepDGA GAN, and it is evident that the detection rate drops from between 0.85 and 0.96 to below 0.50.

In our novel proposal, we recommend adversarial learning, which utilized training dataset to harden the ML detector [19]. Figure 5 demonstrates that with hardening, the detection rate improved for 80% of the DGA families.

The unbiased comparison on the potency of the two ML algorithms demonstrated that the two techniques required training and testing. The testing and training were completed using the same datasets [1]. This is due to the severity of the implicit cost of misclassification in the cybersecurity domain. Therefore, the false positives may annoy the security experts and prevent remediation in case of actual infection [20]. Using the DREBIN datasets, a large family of malware was detected with an f1-score of 0.95 compared to the detection rate in earlier malware families with an F1-score of 0.89 [1]. In the case of a phishing email, our novel approach had an F1-score of 0.90, while initial systems had 0.89.

6. Conclusion

Machine learning techniques are increasingly becoming desirable in cybersecurity. Therefore, it is vital to evaluate the different categories of algorithms that can be used to attain adequate results. In this study, we analyzed the application of ML in cybersecurity through the following focus areas; malware analysis, intrusion detection, and spam detection. The analysis commenced with the classification of the ML algorithms relevant to cybersecurity. The results of this analysis demonstrate that the current ML algorithms are effective in cybersecurity but they are still affected by certain shortcomings that decrease their usefulness in cybersecurity. The results have shown that the ML techniques are still vulnerable to adversarial attacks. Our novel technique performed better than the existing methods by recording an F1-score of 0.95 in malware detection compared to 0.89 in the initial researches.

References

[1] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in 2018 10th International Conference on Cyber Conflict, Tallinn, Estonia, 2018.

[2] V. Ford and A. Siraj, "Applications of Machine Learning in Cyber Security," in 27th International Conference on Computer Applications in Industry and Engineering, New Orleans, Louisiana, 2014.

[3] R. Devakunchari, Sourabh and P. Malik, "A Study of Cyber Security using Machine Learning Techniques," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 7C2, pp. 183-186, 2019.

[4] D. S. Berman, A. L. Buczak, J. S. Chavis and C. L. Corbett, "A Survey of Deep Learning Methods for Cyber Security," Information, vol. 2019, no. 10, pp. 122-157, 2013.

[5] E. Proko, A. Hyso and D. Gjylapi, "Machine Learning Algorithms in Cyber Security," in 2018: The International Conference 'Recent Trends and Applications in Computer Science and Information Technology, Tirana, Albania, 2018.
[6] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications surveys & tutorials, vol. 18, no. 2, pp. 1153-1176, 2015.
[7] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," in 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 2017.
[8] A. D. Joseph, P. Laskov, F. Roli, D. J. Tygar and B. Nelson, "Machine Learning Methods for Computer Security," Dagstuhl Manifestos, vol. 3, no. 1, pp. 1-30, 2012.
[9] E. Sheyabni and G. Javidi, "Seminars in Proactive Artificial Intelligence for Cybersecurity (SPAIC): Consulting and Research," Systemics, Cybernetics and Informatics, vol. 17, no. 1, pp. 297-305, 2019.
[10] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 6, pp. 2818–2825, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13201.
[11] Y. Singh, P. K. Bhatia and O. Sangwan, "A Review of Studies on Machien Learning Techniques," International Journal of Computer Science and Security, vol. 1, no. 1, pp. 70-84, 2007.
[12] M. Sabhnani and G. Serpen, "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context," in Proceedings of the International Conference on Machine Learning; Models, Technologies and Applications, Las Vegas, Nevada, USA, 2003.
[13] Meenu and S. Godara, "Phishing Detection using Machine Learning Techniques," International Journal of Engineering and Advanced Technology, vol. 9, no. 2, pp. 3820-3829, 2019.
[14] S. Rawal, B. Rawal, A. Shaheen and S. Malik, "Phishing Detection in E-mails using Machine Learning," International Journal of Applied Information Systems, vol. 12, no. 7, pp. 12-24, 2017.
[15] M. Islam and N. Chowdhury, "Phishing websites detection using machine learning based classification techniques," in International Conference on Advanced Information and Communication Technology, Chittagong, Bangladesh, 2016.
[16] S. J. S. Daisy and R. A. Begum, "Hybrid Spam Filtration Method using Machine," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9, pp. 1818-1821, 2019.
[17] D. Mallampati and N. P. Hegde, "A Machine Learning Based Email Spam Classification Framework Model: Related Challenges and Issues," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 4, pp. 3137-3144, 2020.
[18] D. Gavriluț, M. Cimpoesu, D. Anton and L. Ciortuz, "Malware detection using machine learning," in Proceedings of the international Multiconference on Computer Science and Information Technology, Mrągowo, Poland, 2009.
[19] S. A. Shawkat, K. S. L. Al-Badri, and I. Al Barazanchi, "Three band absorber design and optimization by neural network algorithm," *J. Phys. Conf. Ser.*, vol. 1530, no. 1, 2020, doi: 10.1088/1742-6596/1530/1/012129.
[20] M. D. Khan, M. T. Shaikh, R. Ansari, M. Suriya and S. Suryawanshi, "Malware detection using Machine Learning Algorithms," International Journal of Advanced Research in Computer and Communication Engineering, vol. 6, no. 9, pp. 195-199, 2017.