Cyber Attack Prediction Using Machine Learning

Pulkit Dwivedi
Department of Computer Science & Engineering
Apex Institute of Technology
Chandigarh University
Mohali, India
pdwivedi1990@gmail.com

Amit Kumar
Department of Computer Science & Engineering
Apex Institute of Technology
Chandigarh University
Mohali, India
amitkumarprasad55@gmail.com

***Abstract*—Due to the increasingly complex and devastating nature of cyber attacks, cyber security is a crucial problem in today's digital environment. In order to improve proactive security methods and lessen the impact of cyber threats, this research study examines the use of machine learning approaches for cyber attack prediction. The main goal is to create a methodical strategy that uses previous attack data, machine learning algorithms, and anomaly detection techniques to effectively forecast and neutralize assaults. By providing a methodical approach to cyber attack prediction using machine learning, this research offers important insights into the field of cyber security. The conclusions offer a road map for professionals and decision-makers to strengthen their defensive plans and better safeguard digital assets in a threat environment that is always changing.**

***Index Terms*—Cyber Threats, Machine Learning, Cyber Security, Predictions, Algorithms, Python, Anaconda.**

I. Introduction

The security of digital lines and information is pivotal in a time when digital technology has a far and wide effect. A huge and complex cyberspace has been produced by the rapid-fire growth of networked technologies, pall computing, and the Internet of Effects (IoT), furnishing preliminarily inconceivable benefits while also exposing us to new and developing pitfalls. Among these troubles, cyberattacks have become a top precedence due to their implicit transgression of sensitive data, vitiate vital structure, and serious fiscal and reputational detriment. Cyber pitfalls are continually changing, as substantiated by decreasingly complex attack styles and frequent cases. Although necessary, traditional security styles constantly fall behind these arising troubles. As a result, visionary and adaptive cybersecurity ways that can prevision and stop intrusions before they beget damage are urgently demanded. Artificial intelligence's subset of machine literacy has become a potent armament in the cybersecurity toolbox. Machine literacy has the implicit to ameliorate our capability to fete and respond to cyber pitfalls by assaying large datasets, spotting trends, and making prognostications. In order to increase our precautionary defense mechanisms, this exploration composition investigates the use of machine literacy approaches for cyber attack vaticination. This study has two pretensions in mind. We first want to look at the implicit effectiveness of machine literacy algorithms for cyberattack vaticination. In particular, we'll look at a number of algorithms, including supervised literacy bones like Random Identify applicable backing agency here. However, cancel this, If none. timber and Support Vector Machines, unsupervised literacy bones like K- Means and DBSCAN, deep literacy bones like Convolutional Neural Networks(CNNs) and Long Short- Term Memory(LSTM) Networks, and ensemble styles like mounding and advancing classifiers. We strive to capture a broad range of attack actions and ameliorate the cast delicacy of our models by exercising a diversified collection of algorithms. Alternatively, we want to give cybersecurity professionals and policymakers perceptivity and useful advice for using these styles in their protective sweats. As a result of this exploration, the wisdom of cyber attack vaticination will develop, and individuals and associations will be given the tools and information necessary to strengthen their defenses in a troubled terrain that is always changing. Our study also strives to help the larger cybersecurity community by offering useful approaches and perceptivity. We are apprehensive that the success of cyber attack vaticination depends not only on algorithms but also on the coordinated sweats of specialists, groups, and decision- makers. As a result, we will also examine the function of cooperation, information exchange, and visionary measures that go beyond the horizon of algorithms. With this comprehensive strategy, we want to develop not only the field of cyber attack vaticination proposition but also the factual use of strong cybersecurity measures. The structure of this essay is as follows We go into the issue of cyberattacks in the following corridor, assaying the being trouble geography and its possible impacts.

We look at the current cyber attack vaticination studies and technology, pressing their benefits and downsides. also, we go over our fashion, which consists of data gathering, preprocessing, choosing features, and training models. We examine the measures used for model evaluation and assess the efficacity of a variety of machine-learning algorithms for prognosticating cyberattacks. The cyber trouble geography has fleetly changed in recent times as a result of the complication of adversaries and the complexity of assaults. Cybercriminals constantly modify their strategies, styles, and practices to get beyond standard security preventives, making it harder than ever to read cyberattacks. In addition, the growth of mobile, pall, and Internet of Effects (IoT) technologies has increased the attack face, giving bad actors new ways to exploit excrescencies. As a

Identify applicable funding agency here. If none, delete this.

result, there's a critical need for creative and visionary methods of relating and anticipating cyber pitfalls. Through the use of machine literacy and prophetic analytics, this exploration aims to break these changing difficulties and contribute to the ongoing fight against cyber pitfalls. also, this study studies the significance of anomaly discovery in spotting peculiar patterns that point to cyber-attacks and considers the viability of real-time monitoring for prompt trouble identification. Practical case studies show how our machine learning fashion may be used in colorful cybersecurity settings, and we compare it to presently available cybersecurity results. By furnishing a regular approach to cyber attack vaticination using machine literacy and exhibitioning the eventuality of colorful machine literacy algorithms to ameliorate cast delicacy and adaptability, this exploration aims to contribute to the area of cybersecurity. By doing this, we stopgap to equip businesses and people with the coffers and information they need to fortify their defenses and cover their digital means in the face of a constantly changing trouble terrain.

II. RELATED WORK

According to the constantly changing threat landscape, the issue of anticipating and mitigating cyberattacks has attracted a lot of attention in the field of cybersecurity. With an emphasis on the use of machine learning algorithms and associated approaches, this review of the literature offers a thorough overview of the state-of-the-art research and advancements in the subject of cyber attack prediction. Anomaly detection, deep learning, ensemble approaches, machine learning algorithms, intrusion detection datasets, and real-time monitoring are just a few of the major issues that the review is organized around. here is a literature survey that covers various aspects of cyber attack prediction, intrusion detection, and related topics. This survey summarizes key research papers and works in the field, highlighting their contributions and relevance:

Wu. et al. [1] proposed an android malware using API call tracking and manifest data. As a result of their strategy, the recall rate was higher than that of tools like Androguard, which was released at Blackhat in 2011. And also proposed DroidMat, which was a program that analyzed malware for Android devices. In this, the K-mean clustering technique is used, and the SVD (Singular Value Decomposition) method is used to determine the number of clusters. Their study found that DroidMat was 2 times more time-efficient than Androguard.

Lim et al. [2] highlights the botnet-based threat prediction methodology. They mainly employed Botsniffer and BotMiner in their prediction model to find botnets. They also developed the prediction model for the estimate of dangers. Finally, they keep an eye on zombies, botnets, and contact with the CC server while assessing any potential dangers to the domain.

Axelsson, S. [3] presented a cognitive bias that arises when the prior probability of a rare event is underestimated. This fallacy carries profound implications for intrusion detection, where the prevalence of actual cyberattacks is typically low compared to the vast volume of benign network traffic.

Amarasinghe et al. [4] used to explain the work on artificial intelligence (AI)-based detection, prevention, and prediction systems for cyber threats and vulnerabilities. Their work has been separated into three stages, including detection, prevention, and prediction. They assess the findings using a robust database, and logistic regression is then used to make the final forecast.

Morris et al. [5] Introduce the ontology-based framework featuring a dynamic knowledge repository. The outcomes encompass an agile capacity for overseeing cyber missions and delivering real-time cyber intelligence to experts, policy-makers, and analysts as needed. Farooq et al. [6] Addresses the challenge of forecasting cyber threats by employing the most effective machine learning algorithms. Through a combination of predictive, classification, and forecasting algorithms, they introduced machine learning techniques that proved to be optimal, as determined through both analytical and empirical assessments. These encompassed Decision Trees, Ensemble Learning, Deep Learning, as well as Classification and Regression, among others.

Dalton et al. [7] greatly enhanced the information foraging that can increase the precision of forecasting systems with an emphasis on the cybersphere. They presented a framework for Information Foraging for Algorithm Discovery (IFAD) in this study. The findings show that cognitive enhancement and information foraging are helpful in the creation of tools to foresee cyber dangers.

Some other works focused on predicting attacks related to social networks [8], [9]. Amir Javed et al. [8] used tweet metadata to construct a machine learning model able to predict if a malicious URL is malicious for Twitter's social network. The proposed model is composed of three components, namely: feature extraction, persistent storage, and machine learning. In the feature extraction phase, the analyzed URL is passed to a sandbox environment to create snapshots of machine activity at regular intervals. These snapshots containing machine activity and metadata of the tweet of the analyzed URL are saved in a database by the persistent storage component. Finally, during the machine learning phase, the predictive model was trained using four ML algorithms: Decision tree, Naive Bayes, Bayes Net, and Neural Network. The predictive accuracy was compared using the Weka toolkit. The honeypot's exclusion list is regularly updated once every 14 days to include new methods used by cybercriminals for executing a drive-by-download attack. The performance evaluation of the proposed method shows an F-measure of 0.833 when using an unseen test set and reaching 0.99 when using 10-fold cross-validation

Al-Qurishi et al. [9] proposed a prediction method for Sybil attack targeting social networks using a deep-regression model. The proposed system is also composed of three modules, which are: data harvesting, feature extracting, and a deep-regression model. During feature extraction, the system considers features based on profile, content, and graphs. The experimental results show a prediction accuracy of 86 percent using noisy and unclean data.

Based on threat intelligence, Zhang [10] proposed a network

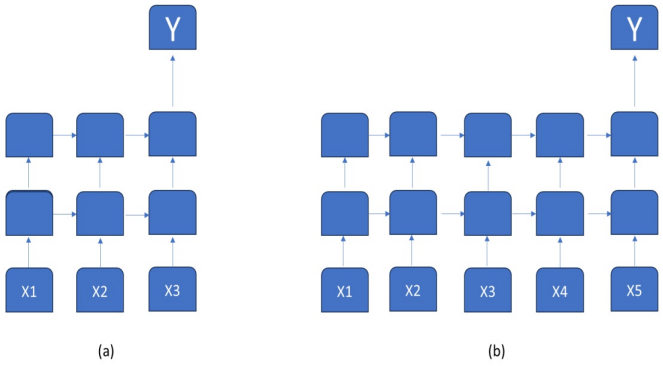


Fig. 1. Unlike DNN, where the neural network topology is set based on the number of inputs, the dual LSTM structure is variable with respect to the number of inputs. (a) LSTM structure in the case of three inputs; (b) LSTM structure in the case of five inputs.

attack prediction system aiming to predict intruder behavior in response to APT (Advanced Persistent Threat). However, the proposed method only focuses on APT, and therefore cannot predict other types of attacks.

III. Proposed Methodology

In this section, the deep learning model utilized in the proposed Cyber Attack Prediction System is thoroughly studied, followed by an introduction to the purpose of constructing the proposed Cyber Attack Prediction System and the findings of preliminary experiments. Before going any further, let's put all definitions and abbreviations in Table 1 for easier comprehension.

An LSTM has an advantage over existing deep neural networks (DNNs) and convolutional neural networks (CNNs) in that it can produce outputs with the same form even in cases where the input shapes differ in size [6] [10]. This is because, as **Figure 1** illustrates, an LSTM expands the architecture of the present recurrent neural network (RNN), which produces outputs of the same dimension for inputs of different sizes. Because of this LSTM feature, Cyber Attack Prediction System may split each packet into segments according to a predetermined size, which can then be entered into each LSTM cell. This allows for the use of all packet sizes as input for the classifier.

A dual LSTM structure is depicted in Figure 1a, where three identical-sized data points are input into each cell of the LSTM first layer, the output of each cell is input into each cell of the LSTM second layer, and the final cell's output serves as the classification result for all of the input data points combined. This classifier has the freedom to change the number of inputs, thus even if Figure 1b's data input count rises to five, the classification can still be completed with the same structure intact. The complete packet data can be utilized to classify an LSTM; however, the relationship between classification performance and packet data size has not been examined in any research. Thus, it is imperative to conduct a verification experiment to verify that utilizing the complete packet data as an input improves the detection accuracy. This study examines the classification performance in relation to the packet length employed by CAPS. Furthermore, an investigation is conducted into the categorization performance based on the quantity of packets utilized in CAPS inside the session's packets.

A. Proposed system

Based on prior experimental findings, the suggested algorithm can be created in the following way: First, the classifier's input should contain all of the received packet's packet data, not just a portion of it. In addition, the classifier's input should contain as many packets as feasible throughout a session. To do this, LSTM is applied. One packet must, however, be split into equal pieces and fed to LSTM (i.e., packet classifier) as LSTM demands the same shape as the input of each cell. Next, a packet classifier is used to transform each received packet into a feature for each packet.

Regardless of the quantity of packets received, the packet classifier uses a double LSTM classifier to process all of the packets in a session. This results in the conversion of every packet into a packet feature of the same size. The packet features that have been translated in this way are sent into the session classifier one after the other. One LSTM classifier was used for session classification, much like for packet classification. In this manner, the session classifier may use the packet characteristics created from the packets to categorize the session, regardless of the number of packets in the session.

Figure 2 shows the entire classification process for the proposed classification model. According to the figure, packet features are created by the packet classifier, and these packet features are integrated into one session feature by the session classifier, and then the final classifier uses it to detect network intrusion. The packet and session classifiers will now be described in detail.

B. Dual LSTM-Based Packet Classifier

Every packet that is received throughout the session is first split into 100-byte units as shown in Figure 1(b). A piece of each packet that is less than 100 bytes is then zero-padded and fed into each cell of the packet classifier. The last packet classifier cell's output serves as the session classifier's input feature. To provide higher-quality packet characteristics, the packet classifier is set up twice.

IV. Experimental Results

A. Dataset Description:

The NSL-KDD dataset [23], which has 41 attributes total and one class attribute, was used to test the suggested technique. The NSL-KDD dataset is smaller than KDD99, which has more duplicate records. Because there are no duplicate records in the NSL-KDD training set, the difficulty level is lowered [16]. The NSL-KDD data collection has a number of benefits over the original KDD dataset, which are covered by [16]. KDDTrain data, which comprises 22 different attack types, is used for training, while KDDTest data, which contains

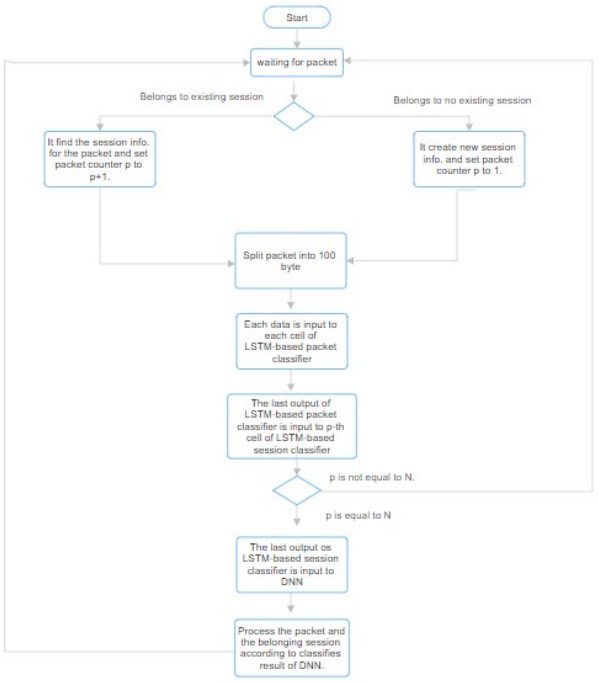


Fig. 2. The overall classification process for the proposed classification model, where N denotes the total number of cells in the LSTM-based session classifier.

17 more attack types, is used for testing. Table I presents common qualities among the four types of assaults that may be classified for training and testing purposes.

There are four types of attacks:

- A hostile attempt to stop system or network resources and services is known as a denial of service (DoS) attack.
- Probe: This attack gathers data on the target system's possible weaknesses so that assaults against such systems may be launched later.
- Remote to Local (R2L) - Unauthorized access to a remote system via network dumps of data packets, allowing the user or root to perform unauthorized actions.
- User to Root (U2R): In this scenario, an attacker logs in as a regular user and exploits security flaws to get administrative rights.

TABLE I
ATTACK CATEGORIZATION FOR TRAINING AND TESTING DATASETS

DOS	**Probe**	**R2L**	**U2R**
apache2	IP sweep	Spy warez-client	buffer overflow
back land	mscan	ftpwrite	oadmodule perl
mailbomb	portsweep	httptunnel	ps rootkit
processtable	saint	imap multihop	snmpguess
upstorm	satan	snoop	xterm
neptune		guesspasswd	
teardrop			
worm			

Table II displays the attacks in the NSL-KDD train and test sets. Italicized terms in the table indicate that they are only available in the training data set, while bold words in the table indicate that they are new assaults introduced in the test set. The assault classes and the quantity of pattern fall for each class are shown in Table III. The training set of the NSL-KDD dataset has 125973 patterns, whereas the testing set contains 22544 patterns. In order to make the proposed model more realistic, it also checks for these 17 unidentified assaults on the testing set.

TABLE II
NUMBER OF PATTERNS FALLS PER CLASS

Training dataset		**Testing dataset**	
Class	**Pattern**	**Class**	**Pattern**
Normal	67343	Normal	9711
DOS	45927	DOS	7458
Probe	11656	Probe	2421
R2L	995	R2L	2754
U2R	52	U2R	200
Total	**125973**	**Total**	**22544**

B. Evaluation Metric

To evaluate the performance of our hyperparameter-optimized CNN-based and LSTM-based cyber attack prediction model, we used a metric combination of precision, recall, F1-score, and accuracy. These four metrics provide a comprehensive picture of the effectiveness of our model in correctly identifying cyber attacks with a low rate of false positives and negatives. Precision: Ratio of correctly predicted positive observations to the total number of predicted positive observations. A high precision is associated with a low false-positive rate. We can represent precision as

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

Recall (Sensitivity): The ratio of correctly predicted positive observations to all observations in an actual class. A high recall is associated with a low false-negative rate. The formula for recall is as follows:

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

F1-Score: The harmonic mean of precision and recall. It attempts to achieve a balance between precision and recall. An F1 score is considered perfect when it is 1, whereas the model is considered a failure when it is 0. The formula for the F1-score is

$$F1Score = 2 * \frac{(Recall * Precision)}{(Recall + Precision)} \tag{3}$$

Accuracy: The most intuitive performance measure. This is simply the ratio of correctly predicted observations to the total number of observations. The formula for accuracy is as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}. \tag{4}$$

Fig. 3. Confusion Matrix for a Classification Model

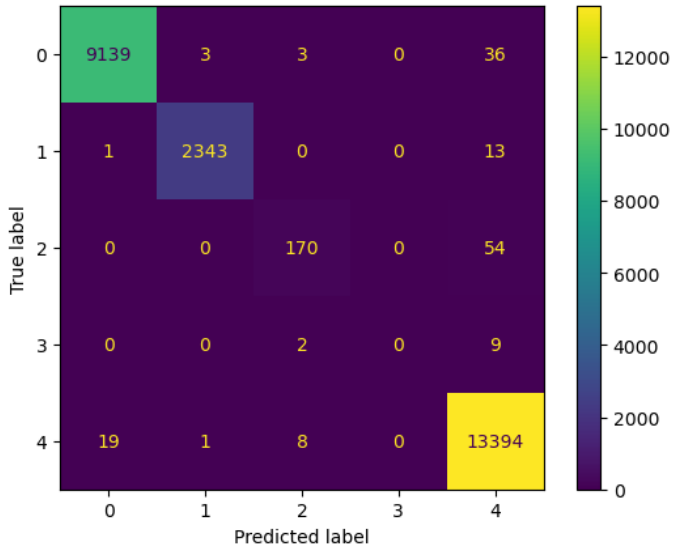
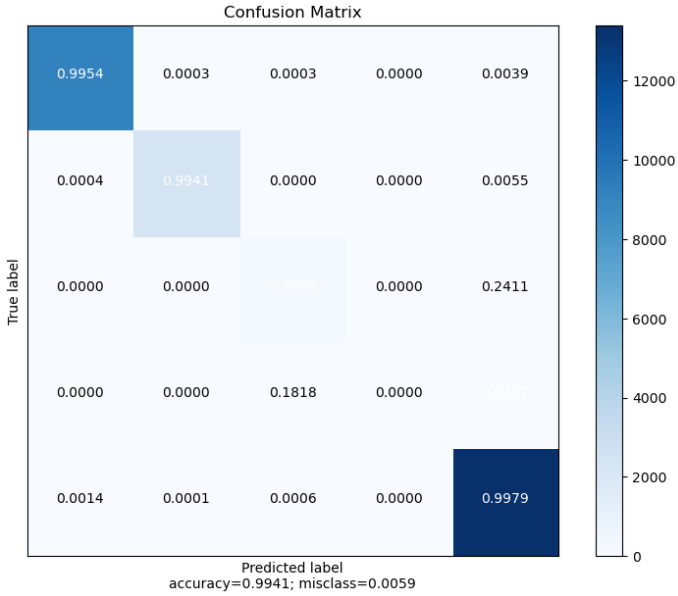


Fig. 4. Accuracy of different attack for test dataset



Where TP, TN, FP, and FN denote true positive, true negative, false positive, and false negative, respectively.

Collectively, these metrics provide a comprehensive measure of the model's performance. While accuracy shows the overall correctness of the model, precision and recall provide insights into the model's capability to minimize false positives and negatives. The F1-score provides a balance between precision and recall. These metrics are crucial for network intrusion detection. A high precision indicates that our model correctly identifies actual intrusions, thereby reducing the risk of false alarms (false positives). A high recall ensures that the system detects most intrusions, thereby reducing the risk of missed threats (false negatives). The F1-Score is the metric that balances these factors.

In Fig. 3 and Fig. 4, we plotted a confusion matrix that shows the accuracy of the cyber attack prediction model. In Fig. 3 Each cell represents the count of instances where the actual class (row) and the predicted class (column) intersect. This matrix provides a detailed view of the model's performance across different classes, aiding in the analysis of classification accuracy and potential misclassifications."

C. Comparative Analysis

During the experimentation, we took the system outcome in two forms: one with a feature selection step and one without. Precision, Recall, F1 Score, Cross Validation, Train Score, and Test Score.

The experiment was done using a Laptop where the operating system was Windows 10Enterprise 64-bit, the Processor was Intel(R) Core(TM) i3 CPU and Python programming language was used

The results of the training and testing on the 5 algorithms using an NSL-KDD dataset are presented in Table IV, below. The table give the training times (s) and training accuracies(%) as well as the testing times (s) and testing accuracies(%) achieved.

TABLE III
RESULT FOR TRAINING AND TESTING ALGORITHMS

Machine Learning Algorithms	Training Times(s)	Testing Time(s)	Training Accuracy	Testing Accuracy
Decision Tree	0.2	0.016	95.9%	95.86%
Linear SVM	1.4	0.016	96.98%	97.13%
Convolutional Neural Network	234.92	0.83	97.83%	97.62%
Artificial Neural Network	192.79	0.74	98.69%	98.5%
Recurrent Neural Network	571.16	2.35	99.17%	98.95%

V. Conclusion

Because technology is changing so quickly, maintaining system security is a challenging task. Cyberattack detection is a difficult challenge these days. We have introduced the comparative machine learning method for predicting and identifying cyberattacks. Four dataset classes—Normal DOS, Probe, R2L, and U2R—are employed for the experimental analysis. With the dataset, several machine learning methods are used. We have implemented the suggested model in two different ways: one with feature selection and the other without.

We can conclude from the analysis of the data that the system improved its F1 Score, Accuracy, Precision, and Recall with SVM for 97.62%, CNN for 98.5% on the other side using LSTM for more accuracy with 98.95%.

The technology is used for the observation of network security. In subsequent studies, we will examine the system

performance using a multiclass data set. Attempt to deal with sophisticated cyberattacks as well.

REFERENCES

[1] D. -J. Wu, C. -H. Mao, T. -E. Wei, H. -M. Lee and K. -P. Wu, "DroidMat: Android Malware Detection through Manifest and API Calls Tracing," 2012 Seventh Asia Joint Conference on Information Security, Tokyo, Japan, 2012, pp. 62-69, doi: 10.1109/AsiaJCIS.2012.18.

[2] S. -H. Lim, S. Yun, J. -H. Kim and B. -g. Lee, "Prediction model for botnet-based cyber threats," 2012 International Conference on ICT Convergence (ICTC), Jeju, Korea (South), 2012, pp. 340-341, doi: 10.1109/ICTC.2012.6386855.

[3] Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. ACM Transactions on Information and System Security, 3(3), 186–205. https://doi.org/10.1145/357830.357849

[4] A. M. S. N. Amarasinghe, W. A. C. H. Wijesinghe, D. L. A. Nirmana, A. Jayakody and A. M. S. Priyankara, "AI-Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System," 2019 International Conference on Advancements in Computing (ICAC), Malabe, Sri Lanka, 2019, pp. 363-368, doi: 10.1109/ICAC49085.2019.9103372.

[5] T. I. Morris, L. M. Mayron, W. B. Smith, M. M. Knepper, R. Ita and K. L. Fox, "A perceptually-relevant model-based cyber threat prediction method for enterprise mission assurance," 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), Miami Beach, FL, USA, 2011, pp. 60-65, doi: 10.1109/COGSIMA.2011.5753755.

[6] H. M. Farooq and N. M. Otaibi, "Optimal Machine Learning Algorithms for Cyber Threat Detection," 2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim), Cambridge, UK, 2018, pp. 32-37, doi: 10.1109/UKSim.2018.00018.

[7] A. Dalton, B. Dorr, L. Liang, and K. Hollingshead, "Improving cyber-attack predictions through information foraging," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 2017, pp. 4642-4647, doi: 10.1109/BigData.2017.8258509.

[8] Amir Javed, Pete Burnap, Omer Rana, "Prediction of drive-by download attacks on Twitter, Information Processing & Management", Volume 56, Issue 3, 2019, Pages 1133-1145, ISSN 0306-4573, https://doi.org/10.1016/j.ipm.2018.02.003.

[9] Muhammad Al-Qurishi, Majed Alrubaian, Sk Md Mizanur Rahman, Atif Alamri, Mohammad Mehedi Hassan, "A prediction system of Sybil attack in social network using deep regression model"Volume 87,2018, Pages 743-753, ISSN 0167739X, https://doi.org/10.1016/j.future.2017.08.030.

[10] Zhang, H., Yi, Y., Wang, J. et al. Network attack prediction method based on threat intelligence for IoT. Multimed Tools Appl 78, 30257–30270 (2019). https://doi.org/10.1007/s11042-018-7005-2

[11] Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Alduailij, and Fazila Malik," Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method", Cloud Computing and Symmetry: Latest Advances and Prospects,1-15, DOI https://doi.org/10.3390/sym14061095,2022

[12] Alzubaidi, L., Zhang, J., Humaidi, A.J. et al. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. J Big Data 8, 53 (2021). https://doi.org/10.1186/s40537-021-00444-8

[13] R. E. Uhrig, "Introduction to artificial neural networks," Proceedings of IECON '95 - 21st Annual Conference on IEEE Industrial Electronics, Orlando, FL, USA, 1995, pp. 33-37 vol.1, doi: 10.1109/IECON.1995.483329.

[14] M. Mishra and M. Srivastava, "A view of Artificial Neural Network," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India, 2014, pp. 1-3, doi: 10.1109/ICAETR.2014.7012785.

[15] Ibor, A. E., Oladeji, F. A., Okunoye, O. B., & Ekabua, O. O. (2020). Conceptualisation of Cyberattack prediction with deep learning. Cybersecurity, 3(1), 1-14. https://doi.org/10.1186/s42400-020-00053-7

[16] Ghulam Mohi-ud-din, December 29, 2018, "NSL-KDD", IEEE Dataport, doi: https://dx.doi.org/10.21227/425a-3e55.

[17] Sarker, Iqbal H., Yoosef B. Abushark, Fawaz Alsolami, and Asif Irshad Khan. 2020. "IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model" Symmetry 12, no. 5: 754. https://doi.org/10.3390/sym12050754

[18] Hiba Asri, Hajar Mousannif, Hassan Al Moatassime, Thomas Noel,Using Machine Learning Algorithms for Breast Cancer Risk Prediction and Diagnosis,Procedia Computer Science,Volume 83,2016,Pages 1064-1069,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2016.04.224.

[19] M. A. Jabbar, Rajanikanth Aluvalu and S. Sai Satyanarayana Reddy, "Intrusion Detection System Using Bayesian Network and Feature Subset Selection", 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 14-16 December 2017, Coimbatore, India, pp. 1-5, DOI: 10.1109/ICCIC.2017.8524381.

[20] Michal Kedziora, Paulina Gawin, Michal Szczepanik and Ireneusz Jozwiak, "Malware Detection Using Machine Learning Algorithms and Reverse Engineering of Android Java Code", International Journal of Network Security & Its Applications (IJNSA), Vol. 11, No. 1, January 2019, pp. 1–14, DOI: 10.5121/ijnsa.2019.11101

[21] Kinam Park, Youngrok Song and Yun-Gyung Cheong, "Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm", 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService), 26-29 March 2018, Bamberg, Germany, pp. 282-286, DOI: 10.1109/BigDataService.2018.00050.

[22] Kilichev, Dusmurod, and Wooseong Kim. 2023. "Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO" Mathematics 11, no. 17: 3724. https://doi.org/10.3390/math11173724

[23] NSL-KDD — Datasets — Research — Canadian Institute for Cybersecurity — UNB. (n.d.). https://www.unb.ca/cic/datasets/nsl.html