Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Improving Network Security by Implementing a Security Assessment as a Service Model Using Machine Learning Algorithms

Anupoju Venkata Malleswara Rao[1], Sheheda Akthar[2]

[1]Research Scholar, Dept. of Computer Science and Engineering, Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, Andhra Pradesh, India & Additional Director, Software Technology Parks of India, MeitY, Govt. of India.
[2]Lecturer in Computer Science, Government College for Women (A), Guntur & Research Director, Dept. of Computer Science and Engineering & Executive Council Member of ANU Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.

Internet or network security is a severe concern of information technology, and different institutions in various domains look for security mechanisms to safeguard their datasets. Many AI and machine learning models are proposed to safeguard the information and network. There is a need to address this issue architecturally and support these prediction models with libraries and prediction modules containing information about the network's attacks and security threats. Thus, by utilizing the data obtained from the libraries by the machine learning models, which classify and analyze the reliability of the traffic, the proposed model can detect the issues faced in the system. Thus, the proposed model provides the necessary security and safeguards the networks from external attacks. This paper uses a Security Assessment As a Service (SeAAS) model to identify malicious traffic, and a classification algorithm is used to classify the obtained data from the traffic. Machine learning algorithms like J48, Random Forest (RF), Multi-Layer Perceptron (MLP), and Naive Bayes (NB) are compared for prediction. Thus, it predicts the normal and abnormal connections in the network and authenticates the connections to the network. In the comparison, the MLP algorithm performed consistently with 99.8% accuracy in the prediction process.

Keywords: Security Assessment as Service, Machine Learning, J48, Multi-Layer Perceptron, Naive Bayes, Random Forest.

1. Introduction

In recent years, the Internet has become a more critical tool for sharing information among people, industries, and organizations. Internet-based systems connect millions of people through webpages, computers, applications, the Internet of Things, and online portals.

Through this system, users can transfer data like video, audio, text, files, photos, and mail with other users. So, the Internet is a communication unit to send and receive information through various networking mediums like Wide Area Network (WAN), Local Area Network (LAN), Metropolitan Area Network (MAN), and others. The ICANN corporation manages all individual devices data accessing processes and IP addresses [3]. The IP address is a device identification number provided by internet service providers (ISPs) to precisely connect the devices to the Internet. Every device has its unique IP address to handle the internet connection efficiently [7]. Most communication industries and sectors are moved to internet-based service systems like education units, hospitals, e-businesses, banks, social media, and private and public companies.

The internet-based server has to manage vast amounts of data worldwide to connect people, organizations, or devices. It leads to cyber-attack, data breaching, and other security issues. Especially Cyber-attack [2] is one of the significant security issues the unauthorized user performs. It can be performed by an individual or a group of people. The hacker's primary goal is to breach the details of the users or to control the devices without the authorized user's knowledge. Generally, cybercriminals have utilized various techniques and methods to launch malicious data into the systems. The most common types of cyberattacks are DoS, Trojan horses, Ransomware, Spyware, Worms, SQL injection, DNS spoofing, Supply chain attack, and Scareware [14].

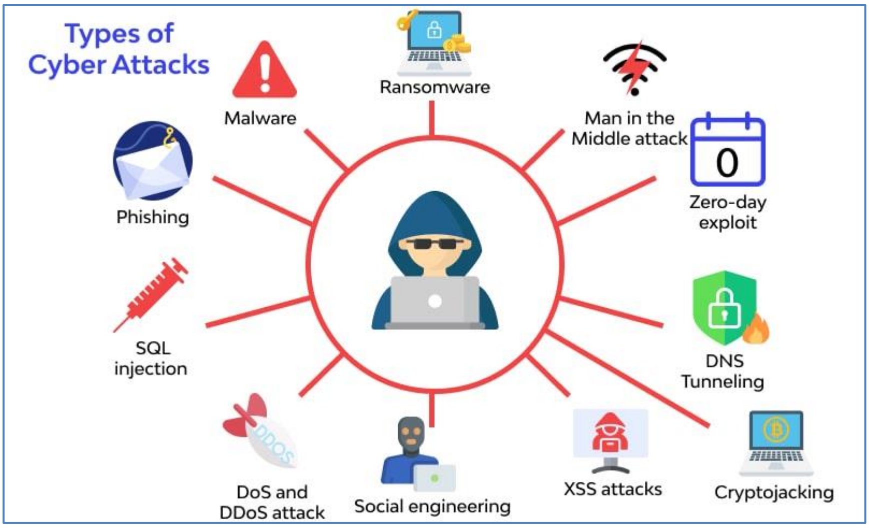


Figure-1. Types of Cyber Attacks

Security enhancement techniques and features are required to protect the Internet from cyberattacks [2]. In that sense, various cybersecurity is developed by many researchers. The main goal of this cyber security [2] system is to safeguard the hardware and software components or data from cyber threats. A sound cyber security system works against malicious links are data created to breach, damage, delete, or extort the more sensitive information of the users or organizations. It also minimizes or eliminates the continuous growth of malicious activities on the Internet [14]. As cyber security becomes highly popular, various cybersecurity solutions are developed. Mainly it is classified into seven disciplines: network security, endpoint security, cloud security, mobile security, application security, IoT security, and zero trust method [14].

Traditionally various techniques are used to prevent the systems from cyber-attacks, like regularly updating the OS and system software, installing anti-virus software, managing the device and applications using strong security passwords, ignoring unknown attachments, files, mail, and messages, and avoiding accessing the unknown WiFi network. Though these steps prevent the devices from malware attacks, they require additional features or techniques to enhance the cyber security of the Internet further. So, in this paper, a machine learning-based security model is implemented to improve the efficiency of the security system [14].

Machine learning is the sub-set of an AI-based model, which can perform regression and classification processes [8], [13]. ML-based security systems are used in many real-time applications, such as schools, industries, IT sectors, and hospitals. The most common type of ML-based applications in cyber security systems is: identifying cyber threats, managing the system with highly secured AI-based anti-virus software, predicting the device based on the user behavior, standing against threats, and automatically monitoring and verifying mail regularly. These features increase the usage of the ML-based model in cyber-security systems. ML algorithms are classified into three phases: supervised, unsupervised, and reinforcement [7], [8]. Thus, in this paper, various machine learning model is implemented, and accuracy is evaluated using various performance metrics and the performance of the ML-based security is illustrated by reviewing various literature works, the functionality of the proposed models, and the result produced by the proposed approach [14].

This paper proposes a new ML-based cyberattack detection model to overcome the issues in the traditional approaches. The main aim of the proposed model is to create an automatic attack detection technique without human interaction. The proposed model is performed based on the following steps:

❖ Initially, the data that travels in the network layer are analyzed and fetched.

❖ Then the captured sequence of input data is split into several elements.

❖ Vulnerabilities of the classified elements are verified using the security assessment service (SeAAS).

❖ Again, the vulnerabilities verified elements are classified using an ML-based controller to get a more robust training result.

❖ The classified input data detects the standard and abnormal files in the network.

2. Literature Survey

In this section, various literature works are discussed to emphasize the performance of the proposed model. Most recent researchers have utilized ML-based algorithms to detect cyber attacks compared to traditional research. H. Alqahtani et al. (2020) utilized several well-known machine learning classification algorithms for intrusions method to detect cyber-security. The algorithms employed include Bayesian Network, NB classifier, DT, Decision Table, and ANN. They have evaluated these algorithms' efficiency by investigating cyber-security datasets encompassing different cyber-attack sections. Finally, they assessed various performance metrics to determine the effectiveness of the detection methods. J. Perez-Diaz et al. (2020) introduce a new method known as a modular architecture designed to identify and mitigate LR-DDoS attacks in SDN (Software-Defined Networking) environments. The architecture incorporates an IDS trained with six ML methods. To assess the performance of these models, we utilize the CIC DoS dataset provided by the Canadian Institute of Cybersecurity. The evaluation results showcase that our approach achieves a remarkable detection rate of 95%, even when dealing with the challenges associated with detecting LR-DoS attacks.

T.A. Tuan et al. (2020) conducted an empirical analysis to examine the effectiveness of various ML models in detecting Botnet DDoS attacks. The assessment is performed on two well-known public datasets, UNBS-NB 15 and KDD99, which are widely used for the above-said method of DDoS attack detection. The evaluation metrics employed in the analysis include Accuracy, Sensitivity, and Specificity. The results demonstrate that the performance of the KDD99 dataset surpasses that of the UNBS-NB 15 dataset. These findings hold significance not only in the realm of computer security but also in other related fields. R. Ch et al. (2020) introduced an adaptable computational tool that utilizes machine learning methods to assess the rate of cybercrimes on a state level within a country. The tool aids in the categorization of various cybercrimes by employing security analytics and data analytics techniques to analyze integrated data from India. This data may consist of both structured and unstructured formats. The significant advantage of this study lies in its comprehensive testing analysis reports, which achieve an impressive 99 percent accuracy in accurately classifying offenses. R. Santos et al. (2020) have utilized four ML methods to classify attacks of DDoS in a simulated SDN environment. A scary tool simulates a DDoS attack, and IPs are valid. The findings reveal that the RF algorithm improves the highest efficiency, while the Decision Tree algorithm exhibits the fastest processing time. Finally, it identifies the most significant features for classifying DDoS attacks and discusses limitations in implementing a classifier to detect three specific DDoS attacks.

A. Aljuhani (2021) examined recent research on detecting DDoS attacks in modern networking platforms, focusing on using single and hybrid machine learning (ML) approaches. Furthermore, this work explores various ML-based DDoS defense systems implemented in virtualized environments. They have investigated Machine Learning methods as security measures against DDoS attacks. They have suggested several potential avenues for future research. Y. Miao et al. (2021) highlighted the latest developments in a new form of attack called ML-based stealing attacks and the associated countermeasures. By summarizing the latest publications, the survey establishes a comprehensive understanding of the attack methodology, identifies its limitations, and suggests future research directions. Additionally, the survey puts forward countermeasures that aim to enhance protection against ML-based stealing attacks, covering aspects of detection, disruption, and isolation. R.J Alzahrani and A. Alzahrani (2021) focused on utilizing various ML methods within the WEKA tool to assess the performance of detecting attacks on recently available DDoS CICDDoS2019 datasets. Among the ML models tested, CICDDoS2019 demonstrated the most promising outcomes. The study employed six different algorithms. The evaluation revealed that both DT and RF achieved exceptional accuracy rates of 99%. However, the Decision Tree algorithm outperformed Random Forest due to its shorter computation time of 4.53 seconds compared to 84.2 seconds for RF.

Furthermore, the research highlights areas that require further investigation in future studies.M. Aamir and Zaidi (2021) suggested a clustering-based approach for differentiating network traffic flows, including normal and DDoS traffic. The study focuses on identifying features at the victim end to detect attacks, utilizing three specific features that can be checked on the particular machine. Through parameter optimization within predefined value sets, the experimental results reveal accuracy scores of 95% for k-NN, 92% for SVM, and 96.66% for RF. F. Hussain et al. (2021) created a comprehensive dataset by integrating various scanning and DDoS attack sections. To improve the training of the ML method, they have integrated samples from publicly-available datasets. Our proposed approach involved a two-fold ML method to identify whether botnet attacks were prevented. The two-fold method exhibited impressive results, with high accuracy, precision, recall, and f1-score in preventing and detecting IoT botnet attacks. Based on the experimental results, we conclusively established that our proposed two-fold approach outperforms other trained models in efficiently preventing and detecting botnet attacks. R. Amrish et al. (2022) utilized a machine learning algorithm to differentiate between normal network traffic and DDoS attack traffic. Four various machine learning classification techniques are employed to detect DDoS attacks. The CICDDoS2019 dataset, collected by the Canadian Institute of Cyber Security, is used for training and testing the ML methods. V. Gaur and R. Kumar (2022) suggested a hybrid approach to select relevant characteristics by applying feature selection approaches to ML classifiers. Random Forest, Decision Tree, k-Nearest Neighbors, and XGBoost are four different classifiers. The CICDDoS2019 dataset, which includes a comprehensive range of DDoS attacks, is utilized to train and evaluate the new approach within a cloud-based platform. Compared with the other methods, the hybrid methodology outperforms well. This approach is beneficial for detecting DDoS attacks on IoT devices early.

M. Ahsan et al. (2022) examined the ML method to enhance the security of cybersecurity systems by analyzing relevant data. It discusses the utilization of machine learning methods to counter existing cyber security threats and addresses the limitations of current models. Additionally, the survey explores the evolution of attack patterns over the past decade. They have evaluated the effectiveness of these ML techniques in combating the escalating threat of malware that impacts our online community. A. Mishra (2022) introduced several ensemble classification techniques that leverage the strengths of multiple algorithms to enhance performance. These techniques are evaluated against existing ML methods to determine their efficacy in identifying various DDoS attacks. Evaluation metrics such as accuracy, F1 scores, and ROC curves are utilized to compare and assess their performance. The results demonstrate significant accuracy and overall solid performance. K.M Sudar and P.Deepalakshmi (2022) using ML method they suggested a new method called flow-based identification and also detect LR-DDoS attacks utilizing ML methods. The proposed approach involves extracting key features from traffic flow samples to identify LR-DDoS attacks. In the mitigation phase, the framework handles the attack flow data and implements mitigation rules to prevent LR-DDoS attacks originating from the same level. They have concluded that Naïve Bayes techniques obtained improved accuracy.

Limitations and Motivation

With the increased network traffic, various security models are proposed to safeguard the network from external attacks. The network traffic is analyzed, and its functions are monitored to define a network as a security model. Network security can be classified into three types: network, information, and cyber security [8]. Though various protocols are proposed to limit the conversation between the nodes, it is difficult for the system to analyze the functions of an address. The various works discussed in the literature show the performance of machine learning models in detecting cyber attacks. There is a necessity for a network to identify the route of the data and evaluate their trustability of them. Through various services are available to improve the accuracy of the model, there is always the issue of device level and network-level security, and for that, a machine learning model needs to be used to optimize the classification of the network traffic and also be capable of predicting the cyber security attacks. The network layer must be optimized to find the route and protect the network. Thus, a machine learning model and a suited architecture favor the functioning of machine learning [8].

Intrusion Detection System

The usage of computer networks is drastically increasing with an increasing number of applications performing on top of it. Thus, network security is increasing because all applications and systems suffer from vulnerabilities that increase various attacks (Figure-2) that negatively impact the economy. Thus identifying and detecting vulnerabilities in the network system becomes more important and should be accurate in real-time applications. This paper develops a service model and trains a machine learning algorithm to differentiate if there is a malicious attack [2], [14].

Figure-2. Virtual Machine Security

Intrusion Detection systems are developed to monitor the network and its application behavior by analyzing the traffic for malicious activity and alerting it to discover such activities. IDS is a software module that scans any environment and data for malicious activity or penetrating policy. In case of malicious detection is reported to the central server, administrator, or any security in charge with the help of Security Information and an Event Management System

(SIEM). It aggregates the output from different IDS sources and makes an alarm based on the malicious action [2].

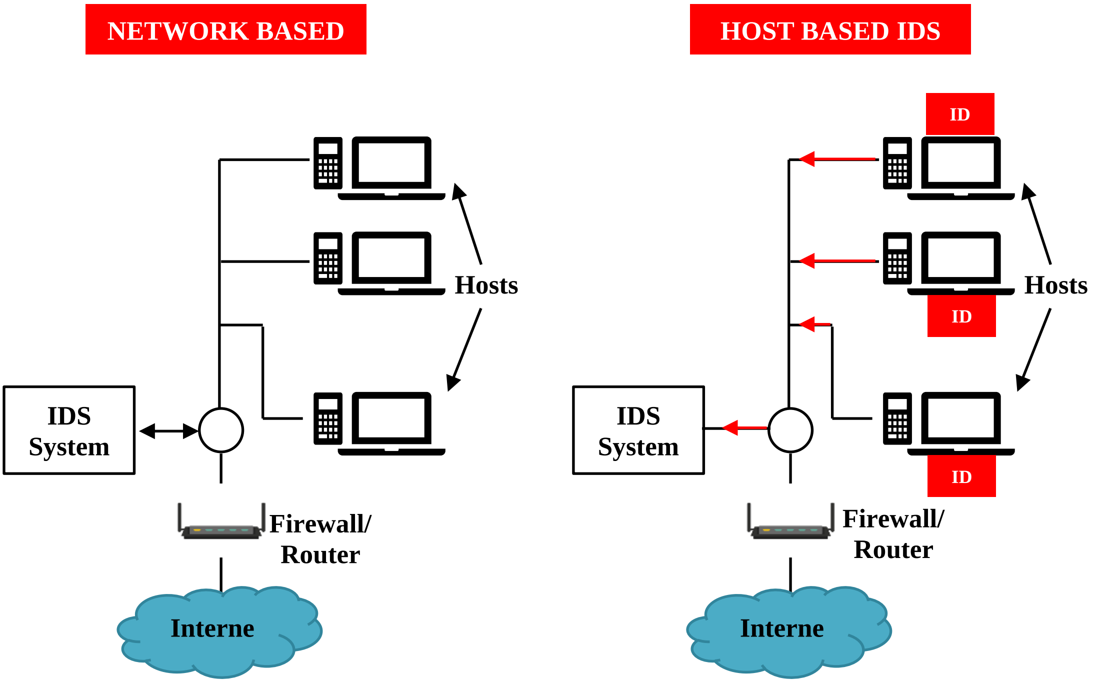


Figure-3. Various Intrusion Detection Systems

Host and Network IDS are different IDS used in various network applications to provide security solutions (Figure-3). Host-IDS is installed in any one specific endpoint, which can protect the system from various threats [2]. HIDS can monitor the entire network system regarding traffic and execution processes and investigate the log information [7]. The visibility of HIDS is available only to the installed machine, not all the host computers. NIDS is a solution for network security designed to monitor the entire network traffic, data packets, and metadata about the contents [2], [7]. NIDS can identify and detect prevalent threats acting in the network. Different approaches like Signature-based IDS and Anomaly-based IDS were proposed to identify and detect malicious activities and threats [11], [14]. The signature-based IDS [2] verifies the attacks using some patterns, whereas the Anomaly-based IDS [2], [11] creates malicious activities to compare and detect unknown malware attacks. New malicious activities are created using machine learning algorithms. Thus this paper has aimed to select a better machine-learning model for malicious activity detection in networks.

3. Proposed model

This section elaborately discussed the architecture and functionality of the proposed approach and components, respectively. The overall architecture of the proposed model is illustrated in Figure-4. Based on the two-use case function, the overall functionality of the proposed model is performed, that is, prediction and detection use case.

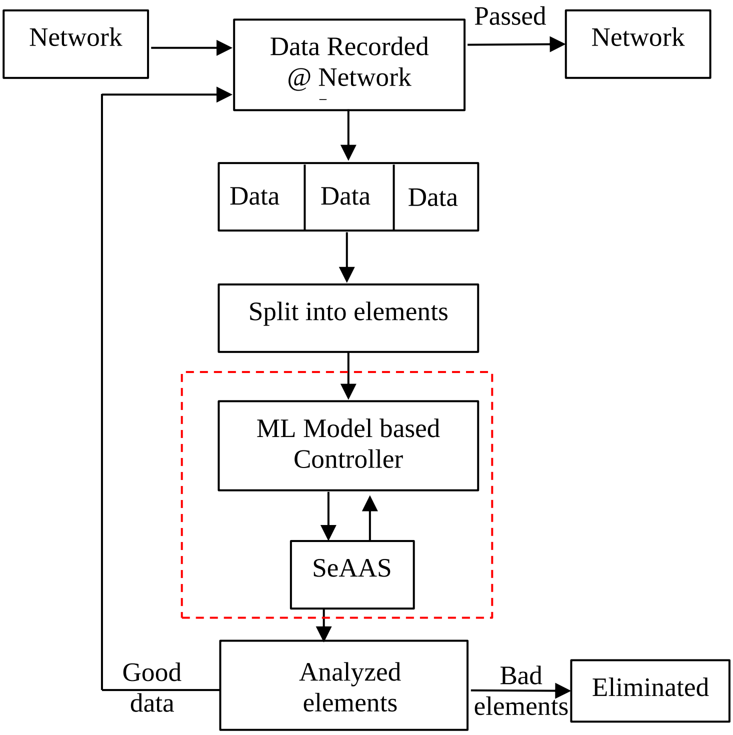


Figure-4. Overall Architecture of the Proposed Model

Machine Learning Algorithm For Cyber-Attack Detection

As mentioned in the earlier sections, ML is the subset of the AI algorithm. It can perform both regression and classification processes. The main goal of implementing the ML-based algorithm is to improve the efficiency and accuracy of the proposed and minimize the error rate. The ML-based detection system can quickly identify the cybercriminal, attacks, and other malicious activities in the network [8], [14]. This system continuously monitors the labeled and unlabelled data to predict the final result accurately. The ML classifier produces the final classification result based on the resultant value of the training and testing data. Generally, ML algorithm is classified into supervised and unsupervised models. Supervised learning models are highly used for attack detection. In that sense, the following section discussed some of the supervised ML classifiers such as Random Forest (RF) [10], [13], [14], [15], J48, Naïve Bayes (NB) [2], [14], [15], and Multi-layer perceptron (MLP).

Multilayer-Perceptron (MLP)

It is a feed-forward neural network containing input, hidden, and output layers. The structure of the MLP [6] classifier is depicted in Figure-5. Each node in the MLP model uses a non-linear activation function to perform the classification task, except for the nodes in the input layer.

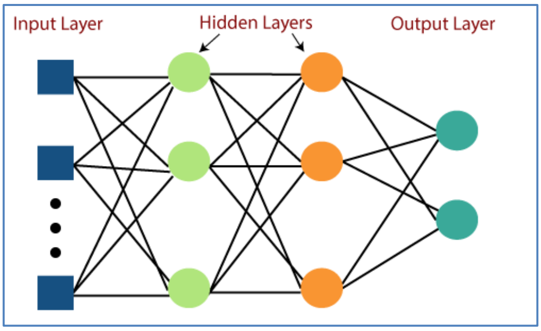


Figure-5. Multi-Layer Perceptron

In MLP, the input data are trained using the feedback-supervised learning model. To predict the desired output, it utilized the non-linear system, which is expressed as:

$$f(x) = \sum_{i=1}^{m} (wi * xi) + b \qquad (1)$$

Here, m represents the number of neurons in the existing layer, w, b represents the node's weight and bias value, and x represents the input value.

Random Forest algorithm (RF)

It is a widely used ML classifier for anomaly detection. The RF algorithm comprises the DT algorithm operators to perform the classification process (see Figure-6). This feature makes the RF model more popular in detecting vulnerability, intrusion, malware activities, and cyber criminals [10], [13], [14], [15]. The new branches in the tree are produced by comparing the current branch with the previous branch. One of the RF algorithm's major advantages over the others is that it does not consume more data or time to process the abnormal data in the datasets. The following mathematical expression is used to predict the classification result:

$$h(x, k), K = 1,2, \dots, i. \qquad (2)$$

Where, $\mathbf{h}, \mathbf{x}, \mathbf{k}, \mathbf{and}\ \mathbf{K}$ represent the classifier, tree class, and random vector, respectively.

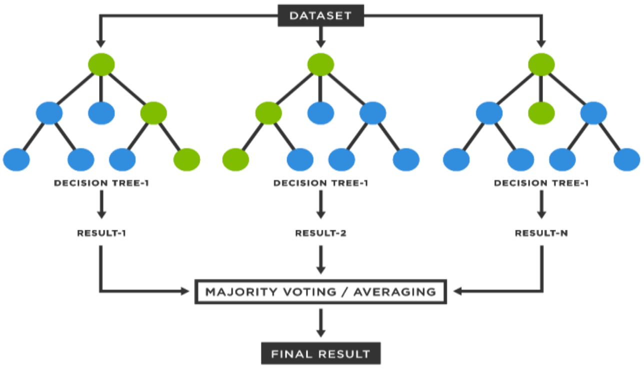


Figure-6. Structure of Random Forest

J48 Algorithm

One of the most popular machine learning algorithm used for classification is J48 [3]. It utilized the decision tree concept to classify the input data based on its features and parameters due to its simplicity, ability to handle the numerical attributes, and interpretability, widely used in many real-time applications. The nodes in the tree structure define the samples observed from the input data, and the leaves define the estimates. The structure of the J48 algorithm is shown in Figure-7.

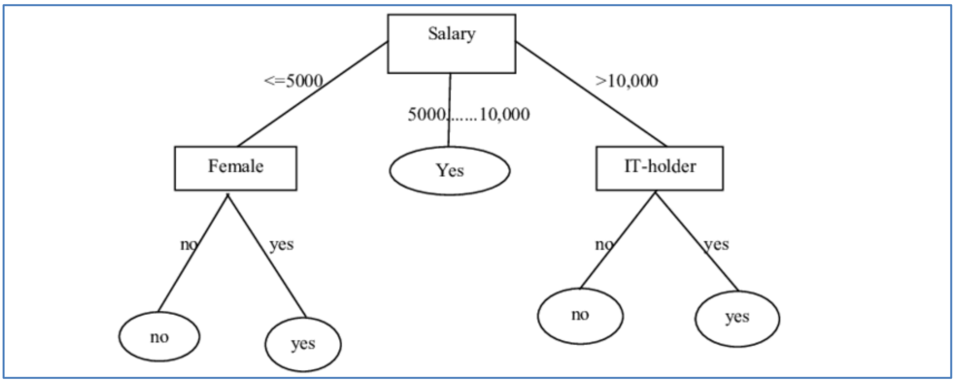


Figure-7. Structure of the J48 Algorithm

Naïve Bayes Algorithm (NB)- This algorithm is proposed based on the Bayes theorem (see Figure-8). It is mainly developed to perform the classification process. To produce the classification result, it evaluates each parameter in the model independently [2], [13], [14], [15]. When compared to others, it is more simple and fast computing algorithm. Most researchers have preferred this model for cyber attack detection because it takes less time to process the input data and produce the appropriate result. NB algorithm reduces the classification problem and performs better than the others. It is expressed using the following equation.

$$\mathbf{P(c|x)} = \frac{\mathbf{P(x|c) * P(c)}}{\mathbf{P(x)}} \tag{3}$$

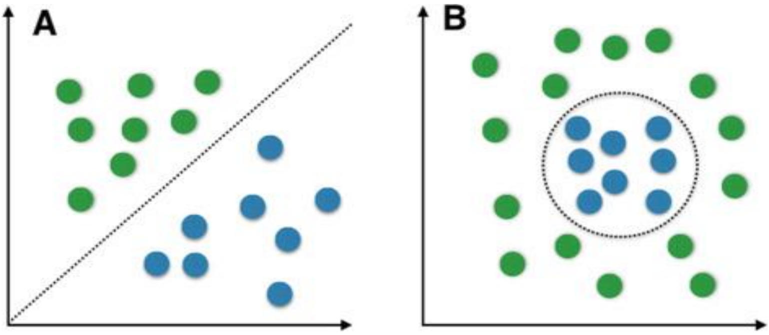


Figure-8. Naïve bayes classifier

Fetching Input Data

The input data sequence is gathered from the network layer to perform the prediction function in this proposed framework. Then based on the size and features, the input data are split into several elements to perform further verification, classification, and prediction. The segmented input data are now passed into the proposed network control model to predict the final classification result. The proposed model comprises ML based controller and Security Assessment Service (SeAAS) to analyze and verify the vulnerability of each element in the network, respectively.

Security Assessment as Service (SeAAS)

The proposed SeAAS system is specially developed to manipulate the internal functions of the network automatically. Therefore, as mentioned above, the SeAAS component is implemented to verify the vulnerability of each element in the current network. After verifying the robustness of the model, the report is transferred to the ML-based controller. The ML controller uses This verification report to classify the input elements appropriately. In addition, the proposed network controller continuously monitors the network flow of each element to produce the final classification result.

ML-based controller

The ML-based controller is the major component in the proposed approach to monitoring the network elements continuously. The proposed ML-based controller utilized a neural network to accurately detect the input elements' cyber-attacks. The ML model is trained using the verification result produced by the SeAAS. An activation function is applied to minimize the proposed approach's loss value. This network model activation function increases the proposed framework's training and testing accuracy. The primary role of the ML-based controller is to classify the good and bad elements in the model. It is performed based on the report sent by the SeAAS. As mentioned above, the proposed security detection system verifies the element's vulnerability and transfers the verification result to the ML controller. Good elements can transfer the data with the neighboring networks based on the result and the harmful elements are eliminated from the network. The internal function of this classification process is performed using two primary use cases are explained in the below sections. The overall process of ML models is carried out in two different phases, Training and Testing/Evaluation, as shown in Figure-9. The training phase learns and extracts hidden information called features from the input data (training data) and classifies them. Based on the classification, the testing phase predicts the test data's class.

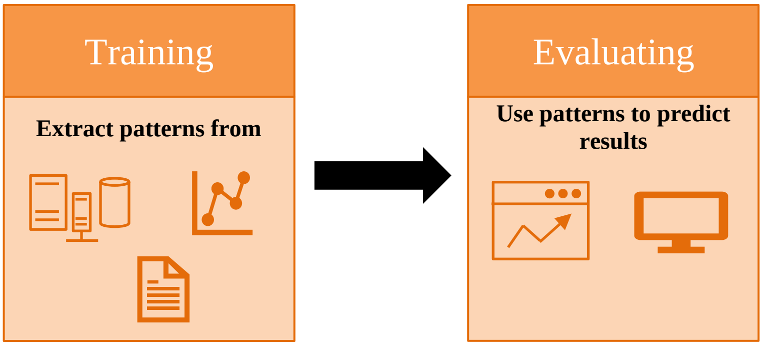


Figure-9. Training and Testing Process

Fundamental Use Cases

The overall workflow of the proposed cyber attack detection process is performed based on the two basic use cases. The first use case defines the element identification and prediction process. And the second use case defines the cyberattack detection process. These two-use cases are more useful to define the robustness and prediction accuracy of the model.

Identification and prevention use case

In this use case, the vulnerability of each element is identified, and a protection measure is established to protect the system. The vulnerability of the element is identified using the Security Assessment System (SeAAS). This security system is performed based on the element received from the ML controller. The vulnerability of the element is detected based on the IP address, location, and device name. This SeAAS system generated the verification result and sent it again to the ML controller. This generated report contains a detailed list of the vulnerability level of each element and the assessment score. The assessment score and the elements' features are extracted using the CVSS V3.0 score value.

Prediction use case

In this use case, the ML-based controller performs the overall function. After getting the report from the SeAAS component, the ML controller verifies the element flow again to predict the final classification result. The ML-controller is trained using the SeAAS report values to produce the final prediction result and then tested. The training and testing result classify the elements into good and bad. If any element is classified as bad, it is eliminated from the network. The good elements are again fed into the network layer with permission to transfer the data to the neighboring network. It is depicted in the figure-10.

Datasets

For evaluating the performance of the proposed approach, the input data are collected from the CIC-IDS2018 dataset [1]. The input datasets contain both normal and malicious files, which include seven different types of cyber-attacked files. The input data are organized into 5 departments. It is organized based on the IP address, duration, device location, tool, and victim. Based on these factors, the proposed detects the normal and malicious elements from the inputs [1].

4. Experimental Result

This section discusses the efficiency of the machine learning algorithm in detecting cyber attacks and normal files in the input datasets. The efficiency of the proposed model is evaluated using various performance metric values. The performance metrics function is based on the total number of true positive, true negative, false positive, and false negative values. The following formulas predict the final accuracy result based on the positive and negative prediction values [2], [8], [13].

$$\mathbf{Precision} = \frac{\mathbf{TP}}{\mathbf{TP + FP}} \qquad (4)$$

$$\mathbf{Recall} = \frac{\mathbf{TP}}{\mathbf{TP + FN}} \qquad (5)$$

$$\mathbf{FScore} = \frac{\mathbf{2 * Precision * Recall}}{\mathbf{Precision + Recall}} \qquad (6)$$

$$\mathbf{Accuracy} = \frac{\mathbf{TP + TN}}{\mathbf{TP + TN + FP + FN}} \qquad (7)$$

5. Discussion

The results obtained from this type of graphical representation is more beneficial to current and future researchers to get a clear idea of ML-based cyber-attack detection techniques. As mentioned above, to evaluate the performance of the proposed model, the input data are taken from the CICIDS2018 dataset [1]. In the experiment, the ratio of protocols used in the network, based on the number of normal and malicious activities obtained in the training process, is shown in Figure-10. It shows that 47% of attacks are classified in the training process. Compared to all the protocols, most network models used 82% TCP protocol, 12% UDP, and 7% ICMP.

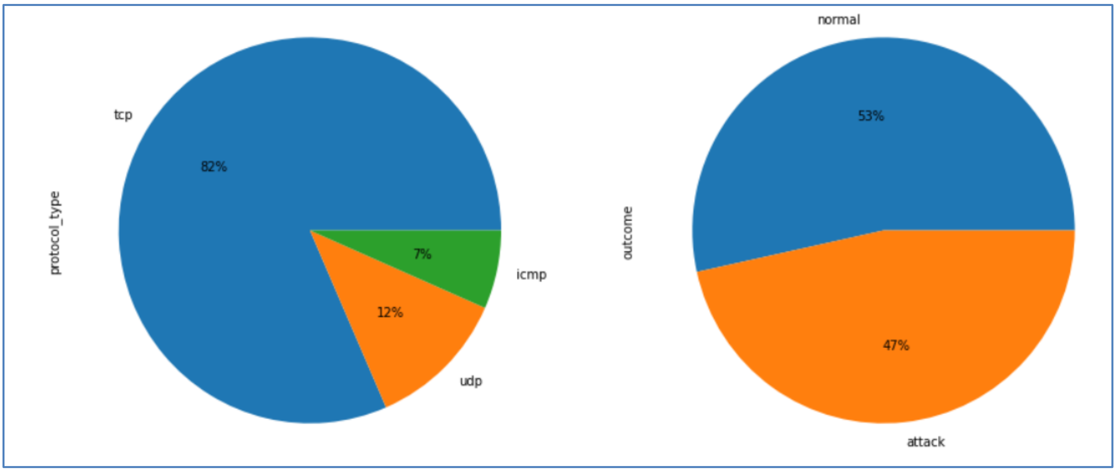


Figure-10. Protocols Used, Normal Versus Attacks

The performance of attack detection and classification concerning the normal and abnormal data using the ML controller is verified using the loss value calculation. The loss value of the machine learning algorithms experimented with for classifying the cyber-attacked files is shown in Figure-11. From the comparison, the MLP obtained more loss value than the other models [1]. It also depicts the data loss value of the proposed approach. The experimental result shows that when the number of epochs increases, the loss value of the proposed model decreases. Compared to the existing approach, the proposed model classifies the normal and abnormal elements with loss rates.

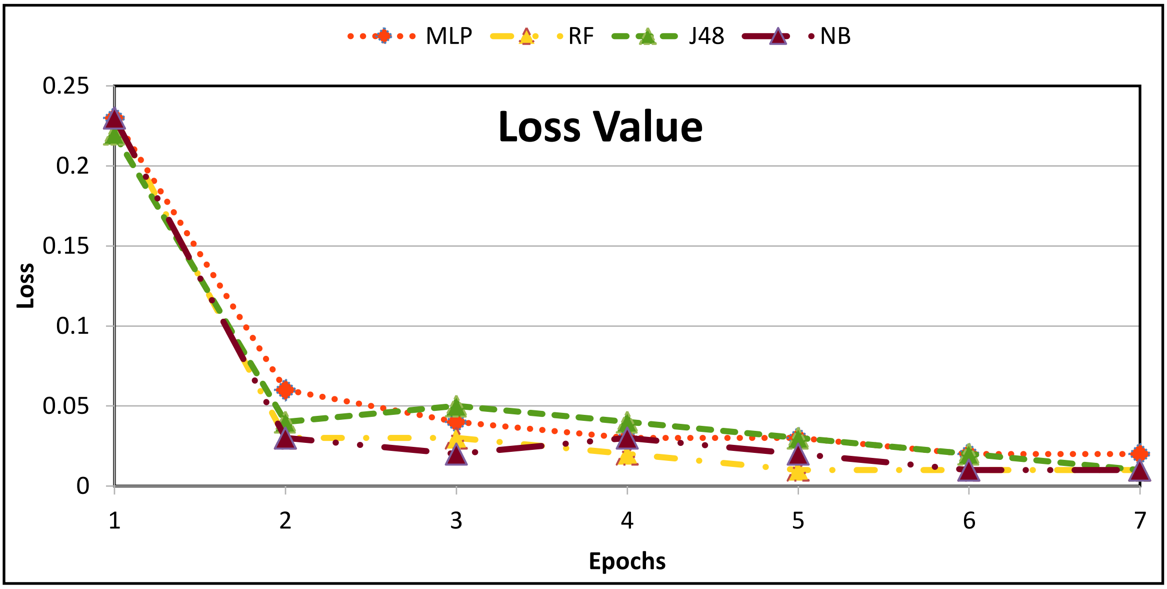


Figure-11. Loss Value of the Proposed and Existing Model [1]

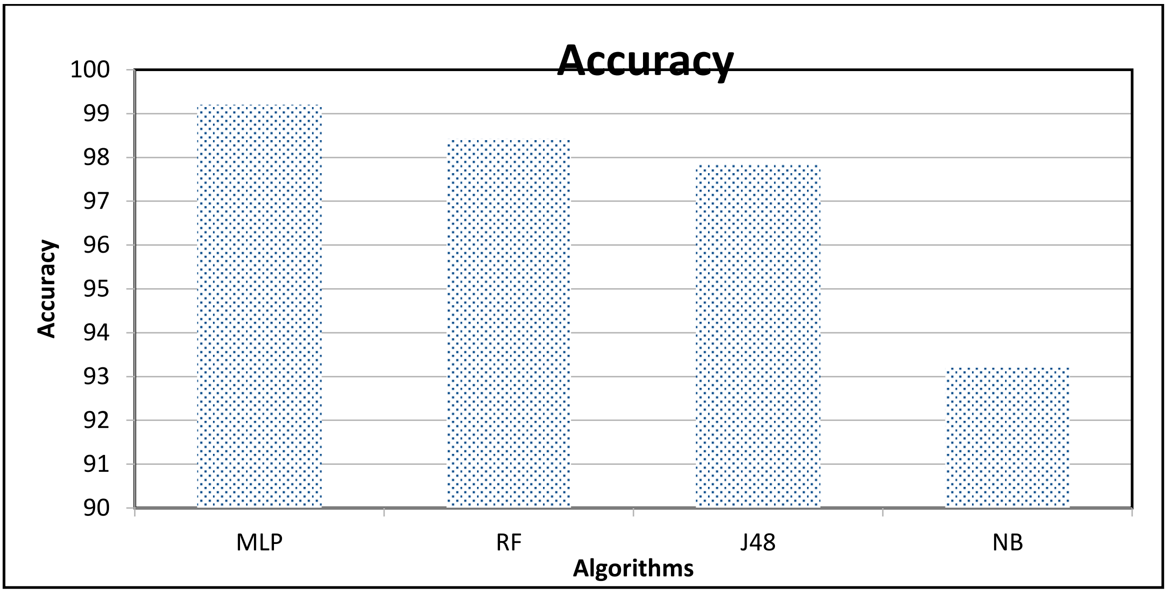


Figure-12. Accuracy Result of the Proposed and Existing Model [1]

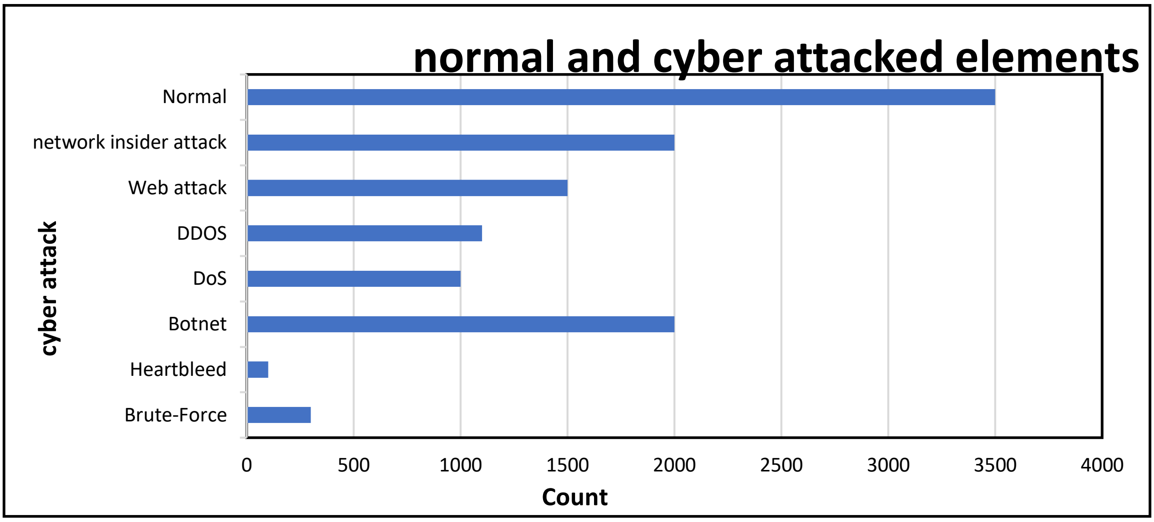


Figure-13. Cyber Attacks

Similarly, Figure-12 depicts the accuracy result of the proposed and existing models. The result produced by the proposed approach shows that when the number of epochs increases, the accuracy value of the proposed ML-based model also increases. While compared with the proposed approach, the existing model is classified with less accuracy. The analysis results indicate that the proposed model classifies each cyberattacked data accurately. The proposed model accurately classifies the input dataset's seven cyber-attacked and standard elements [8]. It is shown in Figure-13, which clearly defines the model's efficiency.

Table-1. Performance comparison of the machine learning algorithm.

Algorithms	Parameters	Probe Attack	User Root Attack	Remote to Local Attack
MLP	Precision	0.98	0.99	0.997
	ROC	0.97	0.95	0.992
	F1-Score	0.98	0.95	0.992
	Recall	0.98	0.96	0.97
	Accuracy	0.99	0.99	0.97
Naïve Bayes	Precision	0.96	0.99	1
	ROC	0.97	0.95	0.99
	F1-Score	0.98	0.95	0.99
	Recall	0.98	0.96	0.97
	Accuracy	0.98	0.99	0.97
Random Forest	Precision	0.97	0.95	1
	ROC	0.98	0.95	1
	F1-Score	0.98	0.96	0.97
	Recall	0.98	0.99	0.97
	Accuracy	0.97	1	1
J48	Precision	0.98	0.96	1
	ROC	0.99	0.96	1
	F1-Score	0.99	0.97	0.98
	Recall	0.99	1	0.98
	Accuracy	0.97	1	1

It can be seen from the comparison table that; the machine learning algorithms are compared in terms of performance metrics. Each ML-based algorithm based algorithms have produced better performance metrics value on performing the classification tasks.

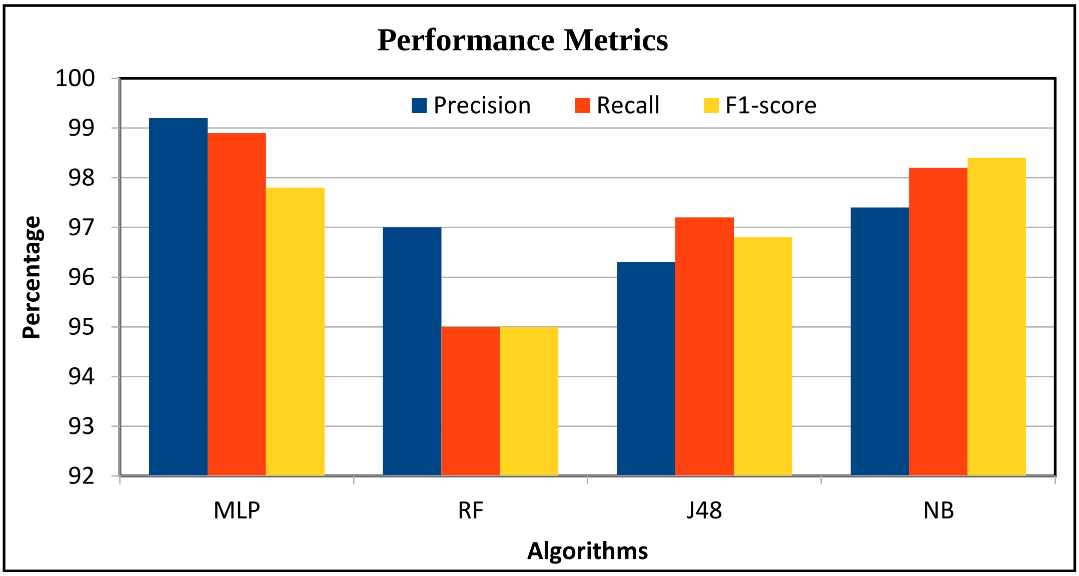
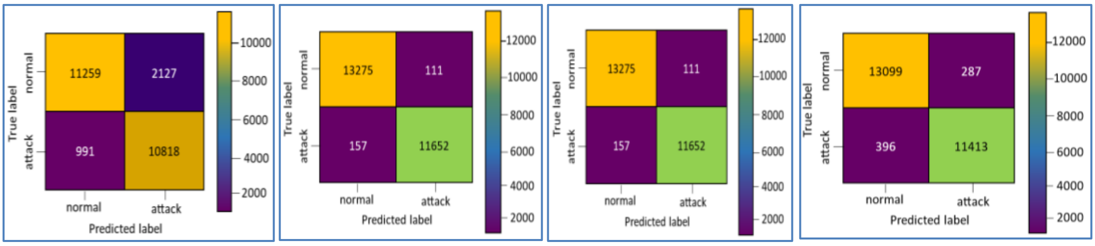


Figure-14. Performance Metrics of the Proposed and Existing Model [1]

Figure-14 depicts the performance metrics comparison result of the proposed and existing models. Compared to the existing model, the proposed machine learning-based detection model achieved 97%, 95%, 95%, and 98.43% precision, recall, F1-score, and accuracy value, respectively. The confusion matrix obtained for all the machine learning models involved in this paper is shown in Figure-15.



MLP Random Forest Naive Bayes J48

Figure-15. Comparison of Confusion Matrix

6. Conclusion

Thus, the proposed model comprises a security architecture that provides the necessary security for the network. It uses a machine learning model to provide the necessary security for the network. The proposed model provides a secured architecture and route for the data packets, from fetching the data to processing and detecting malicious attacks. The machine learning model proposed gets the split and formatted data and efficiently predicts the cyber attacks. The classification algorithm used in the network classifies the network traffic and allocates the available resources accordingly. After classification, the abnormal traffic from the dataset is identified and compared with similar models, and the performance of the proposed model is evaluated. Different machine learning algorithms like MLP, J48, Naive Bayes, and Random Forest algorithms are considered for the comparison. Traffic evaluation is carried out through the SeAAS module, providing better classification accuracy. The ML model is used as a controller to make the network function efficiently and authenticate the network connections. Among the various machine learning algorithms considered, the MLP algorithm provides better results with 99.8% accuracy.

References

1. https://paperswithcode.com/dataset/cicids2018
2. Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1 (pp. 121-131). Springer Singapore.
3. Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. IEEE Access, 8, 155859-155872.
4. Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., Priyadarshini, I., & Son, N. T. K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. Evolutionary Intelligence, 13, 283-294.
5. Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify cyber crime offenses using machine learning. Sustainability, 12(10), 4087.
6. Santos, R., Souza, D., Santo, W., Ribeiro, A., & Moreno, E. (2020). Machine learning algorithms

to detect DDoS attacks in SDN. Concurrency and Computation: Practice and Experience, 32(16), e5402.

7. Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. IEEE Access, 9, 42236-42264.
8. Miao, Y., Chen, C., Pan, L., Han, Q. L., Zhang, J., & Xiang, Y. (2021). Machine learning–based cyber attacks targeting on controlled information: A survey. ACM Computing Surveys (CSUR), 54(7), 1-36.
9. Alzahrani, R. J., & Alzahrani, A. (2021). Security analysis of ddos attacks using machine learning algorithms in networks traffic. Electronics, 10(23), 2919.
10. Aamir, M., & Zaidi, S. M. A. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. Journal of King Saud University-Computer and Information Sciences, 33(4), 436-446.
11. Hussain, F., Abbas, S. G., Pires, I. M., Tanveer, S., Fayyaz, U. U., Garcia, N. M., ... & Shahzad, F. (2021). A two-fold machine learning approach to prevent and detect IoT botnet attacks. Ieee Access, 9, 163412-163430.
12. Amrish, R., Bavapriyan, K., Gopinaath, V., Jawahar, A., & Kumar, C. V. (2022). DDoS detection using machine learning techniques. Journal of IoT in Social, Mobile, Analytics, and Cloud, 4(1), 24-32.
13. Gaur, V., & Kumar, R. (2022). Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arabian Journal for Science and Engineering, 47(2), 1353-1374.
14. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527-555.
15. Mishra, A. (2022). Prediction Approach against DDoS Attack based on Machine Learning Multiclassfier. arXiv preprint arXiv:2204.12855.
16. Sudar, K. M., & Deepalakshmi, P. (2022). Flow-based detection and mitigation of low-rate ddos attack in sdn environment using machine learning techniques. In IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021 (pp. 193-205). Springer Singapore.
17. Manal Loukili, Faycal Messaoudi, Raouya & El Youbi, “Implementation of Machine Learning Algorithms for Customer Churn Prediction”, Journal of Information Systems and Telecommunication, Vol.11, No.3, July-September 2023, pp. 196-208.
18. Mohammad Akhondi Darzikolaei, Ata Ebrahimzade & Elahe Gholami, “The separation of Radar clutters using Multi-Layer Perceptron”, Journal of Information Systems and Telecommunication, Issue 17, Vol. 5, No. 1, January-March (Winter) 2017, pp. 41-49.
19. Karen Scarfone, Paul Hoffman, “Guidelines on Firewalls and Firewall Policy”, Recommendations of the National Institute of Standards and Technology, U.S. Dept. of Commerce, NIST Special Publication 800-41 Revision 1.
20. Raghav Arora, Rana Rahul Sathyaprakash, Saurabh Rauthan, Shrey Jakhetia, “Internet Security and Privacy” International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 2, Issue 3, pp: (467-475), Month: July - September 2014, www.researchpublish.com
21. R. Bhuvana Indumathi & R. Bhuvaneswari, “Network Security”, International Journal of Current Research and Modern Education, Special Issue, January, Page Number 50-52, 2017.
22. Alhasan, S., Abdul-Salaam, G., Bayor, L., & Oliver, K. (2021, December). Intrusion detection system based on artificial immune system: a review. In 2021 International Conference on Cyber Security and Internet of Things (ICSIoT) (pp. 7-14). IEEE.
23. Alzahrani, A. O., & Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Future Internet, 13(5), 111.
24. Jin, D., Lu, Y., Qin, J., Cheng, Z., & Mao, Z. (2020). SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism. Computers & Security,

97, 101984.

25. Narendra Kumar Chahar, “Computer Network Security”, International Journal of Innovative Science and Research Technology, ISSN No:-2456-2165.
26. Ohta, T.; Chikaraishi, T., "Network security model," Networks, 1993. International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Proceedings of IEEE Singapore International Conference on, vol.2, no., pp.507-511 vol.2, 6-11 Sep 1993.
27. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008.
28. Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access," Proceedings of the IEEE, [1]
29. vol.85, no.12, pp.2034-2051, Dec 1997.
30. Ohta, T.; Chikaraishi, T., "Network security model," Networks, 1993. International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Proceedings of IEEE Singapore International Conference on , vol.2, no., pp.507-511 vol.2, 6-11 Sep 1993.