e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

Review of Cyber Intruder Detection System Using Supervised Learning

[1]Gogbe Tia Raoul, [2]Dr Manjunath C R

[1]PG Student, Department of CSE, JAIN(Deemed-to-be-University), Bengaluru, India

[2] Professor, Department of CSE, JAIN(Deemed-to-be-University), Bengaluru, India

ABSTRACT: With the rise of technology, particularly the internet, there has been a corresponding increase in various types of network attacks. One of the most challenging security threats of our time is the DOS attack, which can cause significant damage. The DDoS attack is of particular concern due to its potentially severe impact. These attacks are difficult to detect and counter, as they can happen suddenly and without warning, quickly depleting the communication resources of the victim. As these attacks become more advanced and numerous, detecting and countering them becomes increasingly difficult. We have successfully detected DDoS flooding attacks using a variety of Machine Learning techniques, such as KNN, SGD, Multi-layer Perceptron, Naive Bayes, SVM, Decision Tree, and deep learning techniques like DNN, to combat this. To evaluate the effectiveness of these algorithms, we performed a detailed comparative analysis based on accuracy metrics. Wireshark was used to detect the upsurge of packets during a DDoS attack, while the various ML algorithms were used to detect the attack itself. By comparing the results of each algorithm, we can determine which is the most effective for detecting and countering DDoS attacks. Network attacks become increasingly advanced, it is essential to utilize all available tools and techniques to detect and counter them effectively. Machine Learning algorithms have proven to be an effective tool in detecting DDoS attacks, and by performing a comparative analysis of these algorithms, we can continue to improve our ability to detect and prevent such attacks.

KEYWORDS: *Machine Learning, Ddos , Cyber Intruder*, Supervised learning, Unsupervised learning

I. INTRODUCTION

Intruder detection system is designed to detect unauthorized entry or intrusion into a protected area or premises. In order to protect assets from theft or damage, intruder detection systems are commonly used in commercial, industrial, and residential buildings. These systems consist of sensors placed at key locations throughout the building, such as doors and windows, which can detect movement, changes in temperature, or other signs of an intruder. Once an intrusion is detected, the system can trigger an alarm, alert security personnel, or activate other security measures like locking doors or turning on cameras.

Today, many critical sectors, including healthcare, finance, power corporations, water, telecommunications, transportation [1], defense, education, and research and development, rely heavily on the internet. However, this reliance also makes them vulnerable to cyber-attacks, which can have long-lasting negative effects on their operations. To safeguard valuable information from such attacks, cyber defense mechanisms are necessary, but accurately predicting the timing of the next attack is challenging.

Soft computing techniques, such as intrusion detection systems, artificial neural networks, and artificial intelligence, have been developed to help predict future cyber-attacks by analyzing past data collected from the system's environment. The most effective intrusion detection systems now rely on machine learning mechanisms like support vector machines, neural networks, and decision trees, which can improve their classification performance and speed up processes without explicit customization [2].

Several factors influence the development of effective intrusion detection systems. One is the increasing complexity of networked systems, which creates more opportunities for errors that can be exploited by intruders. Another factor is the significant security vulnerabilities present in current network systems, which make them attractive targets for attackers, and although efforts are being made to address these deficiencies, it is not possible to completely eliminate all security gaps.

Although some intrusion prevention systems exist, they cannot provide absolute protection. Therefore, IDSs have emerged as an effective means of detecting and identifying intrusions, which can then be used to update prevention mechanisms.

Most protection measures aim to defend against external attacks, but identifying and preventing attacks from authorized employees within a company can pose a significant challenge and can cause more damage. Moreover, it's important to note that new attack techniques are constantly emerging to bypass existing defense and detection systems.

Therefore, security systems need to be regularly updated through continuous learning or update procedures to adapt to these evolving threats.

Overall, IDSs consist of three primary components, including a data collection mechanism to trace network flows, feature identification to create a feature vector, and a classification engine to identify whether the traced flow is normal or an intrusion based on previous knowledge [6].

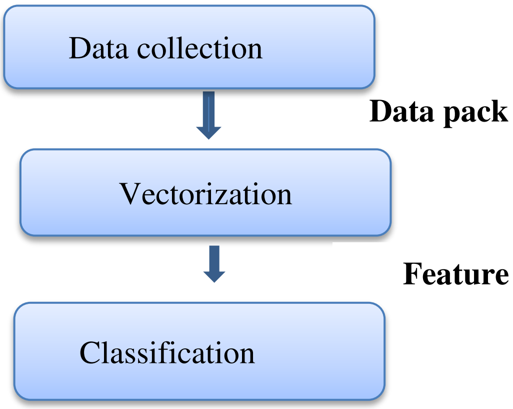

Fig. 1. Data process

The DDos attacks that adversarial hackers now regularly use to flood the victim's server will be the main topic of our paper. IDS come in a variety of forms. We will discuss machine learning techniques and different algorithms to use along with a little more information on the current approaches or strategies.

According to Tanishq Kothari and Atharav Hedage [5], The study presents an experimental evaluation of various machine learning models for intrusion detection in IoT networks. The authors test six different models: Random Forest, Decision Tree, SVM, KNN… etc.,. The paper "Cyber Attacks on Intrusion Detection System" by Priyanka Sharma and Rakesh Singh Kunwar[1] provides an overview of the many types of cyberattacks that may be launched against intrusion detection systems (IDSs) and the various defense mechanisms that may be employed to mitigate them.

The paper begins by defining an IDS and its importance in detecting and preventing cyber-attacks. It then goes on to describe various types of attacks that can be launched against an IDS, including denial-of-service (DoS) attacks.

II. Related work

A crucial step in detecting a ddos (distributed denial of service) attack is to monitor network traffic for abnormal spikes in incoming traffic. since ddos attacks rely on overwhelming a target server or network with a flood of requests or traffic, a sudden increase in incoming traffic is often an indicator of an attack. previous research has also yielded several techniques for detecting a ddos attack. in our research we have discovered several techniques used for the detection of dddos attacks. in this article we will give you the summary of some authors.

the study conducted by santhosh kumar et al[8] in 2022 presents a supervised machine learning-based approach to detect cyber-attacks against computer systems. the authors proposed a model that can identify and classify different types of cyber-attacks, including denial of DOS, DDOS, probe, r2l (remote to local), and u2r (user to root).the proposed model consists of two main phases: the first phase involves feature selection and extraction, where relevant features are selected from the network traffic data using principal component analysis (pca) and mutual information (mi) techniques. the second phase involves the application of variety supervised ml algorithms, such as decision tree, random forest , naïve bayes and svm, to classify the network traffic.

other way syam akhil r. and venkata ratnam k[4],proposes an IDS that uses artificial intelligence and ML algorithms to detect and prevent malicious activities in computer networks.

the authors begin by discussing the increasing importance of intrusion detection systems in protecting computer networks from various types of attacks, such as denial-of-service attacks, malware infections, and unauthorized access. they highlight the limitations of traditional intrusion detection systems, such as their reliance on predefined rules and signatures.

A Machine Learning for Intrusion Detection" by Shilpa Shree, Lingareddy, Nayana, and Sunil Kumar[2] presents an approach for using decision trees as a machine learning technique for intrusion detection.

The paper begins by discussing the need for intrusion detection systems (IDSs) and the challenges in accurately detecting and preventing attacks. It then provides an overview of decision trees as a machine learning technique and their advantages, such as being easily interpretable and computationally efficient. Gozde Karatas, Onder Demir, and Ozgur Koray Sahingoz,[6] published in 2018, explores the use of deep learning techniques for intrusion detection systems (IDSs). The authors begin by providing background information on IDSs and the challenges of detecting unknown attacks using traditional IDSs. They then discuss the potential of convolutional neural networks , such as DL techniques and recurrent neural networks , for improving the accuracy of .The study presents an experimental evaluation of various deep learning models for intrusion detection. The authors use a publicly available dataset, NSL-KDD, to train and test their models. They compare the performance of deep learning models to that of traditional machine learning models, such as decision trees and, SVM. In this paper [18] the authors gave some details on IDS have played a crucial role in safeguarding networks and information systems. However, utilizing conventional IDS techniques in IoT proves challenging owing to its unique traits, such as limited-resource devices, distinctive protocol stacks, and standards. In paper [3] and [14] The authors then describe their approach for using machine learning to detect cyber-attacks, which includes collecting also preprocessing data, selecting relevant features, training ML models, and evaluating their performance.

TABLE I. ADVANTAGES AND DISADVANTAGES

REFERENCES	ADVANTAGES	DISAVANTAGES
Syam ., Venkata K..([4]	By utilizing a dataset of network traffic generated by an authentic computer network, the proposed system was tested, enabling its application in real-world scenarios.	The study's ML techniques were not adequately described in the publication, which makes it difficult to reproduce the results or comprehend the system's limitations.
Khraisat,., Gondal., Vamplew.& Kamruzzaman,[24]	Detailed analysis of the challenges: The article not only presents a list of difficulties that intrusion detection systems encounter but also offers an in-depth examination of each challenge along with potential remedies	Limited scope: While the paper covers a wide range of intrusion detection techniques, datasets, and challenges, it is not an exhaustive review.
Sarker, , Abushark., Alsolami,& Khan, [22]	Interpretability: The decision tree model used in the proposed method provides interpretability, which can help in identifying the specific features that contribute to the detection of intrusions.	Limited comparison: The authors only compare their proposed model with a few machines learning based intrusion detection models.
B. Dong and Wang [19]	Comparative study: The paper presents a comparative study of traditional methods and deep learning methods for network intrusion detection. This allows the readers to gain insights into the strengths and weaknesses of each approach.	Limited scope: The paper only considers a single dataset for evaluation. This limits the generalizability of the findings and conclusions presented in the paper.
Zarpelao, Miani, Kawakami, and Alvarenga [17]	Methodical approach: To identify and classify the various intrusion detection techniques for IoT, the authors used a systematic and methodical methodology. They have also examined each technique's efficiency and given a thorough description of it.	Lack of comparison: The paper does not provide a direct comparison of the various intrusion detection techniques for IoT, which makes it difficult for readers to assess the relative merits and demerits of each technique.

III. MACHINE LEARNING(ML) TECHNIQUES

With (ML) is a field of study that enables machines to learn patterns and make predictions based on:

A. Supervised learning

Supervised Learning: In this technique, the machine is trained on a labeled dataset, which means that the output
data, without being explicitly programmed. There are several techniques that are commonly used in machine learning, including:
or outcome is already known. The aim is to find a function that maps input variables to output variables. Examples include classification and regression.

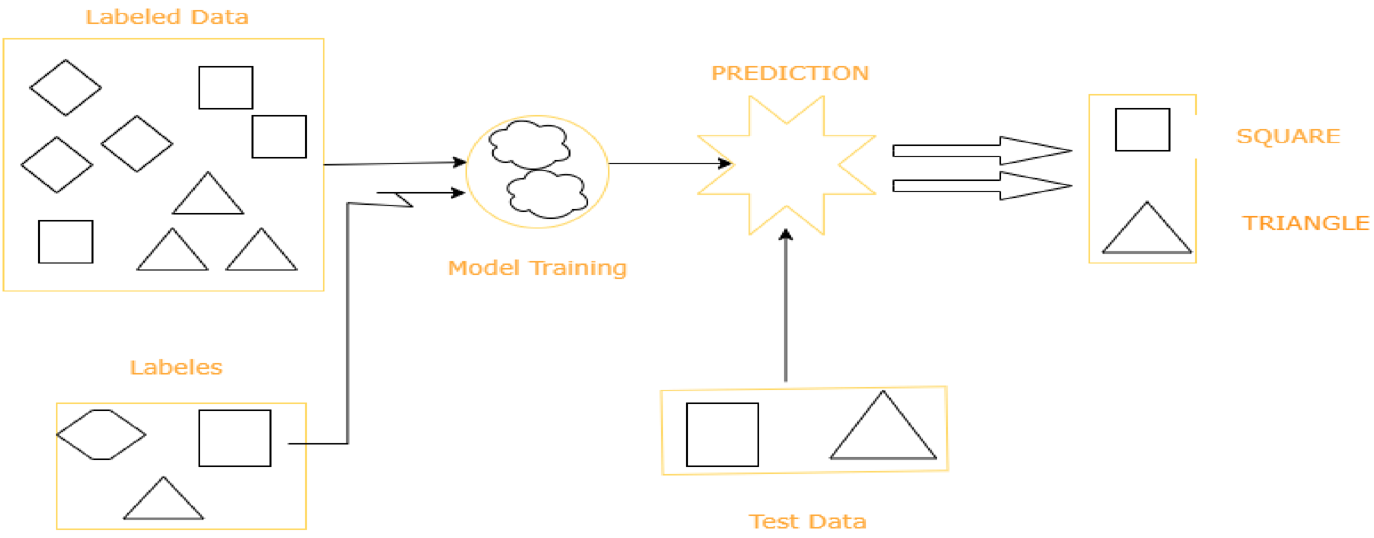

Fig. 2. Supervised learning

B. Unsupervised learning

Here, the machine is trained on an unlabeled dataset, which means that the outcome is unknown. The aim is to find patterns or groupings in the data. Examples for that technique include clustering and dimensionality reduction.

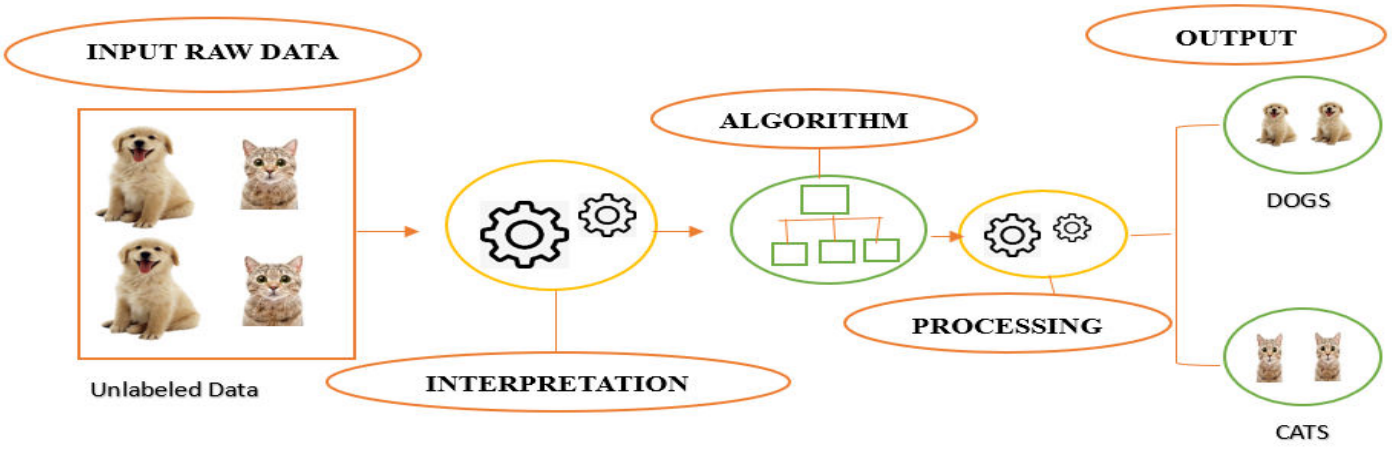

Fig. 3. unsupervised learning

C. Transfer learning

This technique allows the machine to transfer knowledge learned from one task to another. For example, a machine that has been trained to recognize images of dogs can transfer some of that knowledge to recognize other animals.

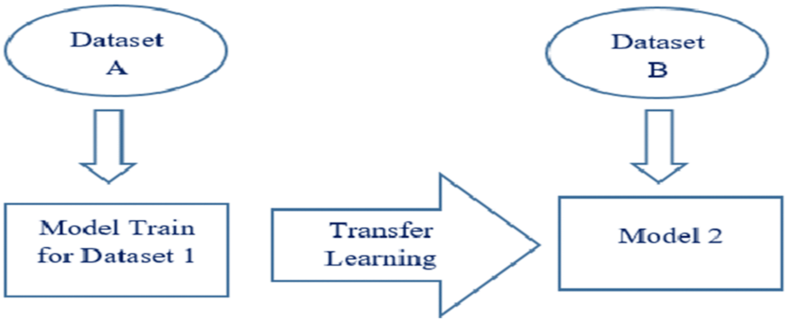

Fig. 4. Transfer learning

D. Semi-supervised learning

Explanation with diagram

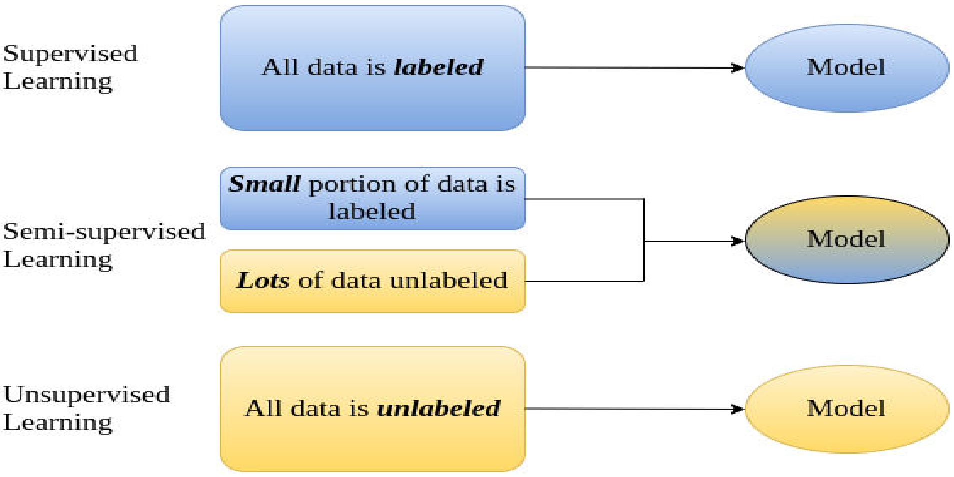

Fig. 5. Semi-supervised learning

In order to work with an unlabeled dataset, Semi-supervised learning relies on a few assumptions to accomplish this, such as the continuity assumption, which suggests that objects that are close to one another are likely to share the same label or group. Low-density borders' smoothness presumption is added to these decision boundaries in semi-supervised learning, though.

The cluster assumption, which includes grouping data into distinct clusters where points within the same cluster share the same properties, is another premise utilized in semi-supervised learning label. Lastly, the manifold assumption relies on the use of distances and densities, where the data lies on a lower-dimensional manifold than the input space. This assumption is useful for data that has a higher degree of complexity, making it difficult to model directly.

These are just a few examples of the many techniques used in machine learning. The choice of strategy depends on the problem at hand and the nature of the data.

IV. MACHINE LEARNING ALGORITHM USED

There are several ML algorithms that can be used depending on the specific task and data you are working with. Let’s talk about a few examples of the many machine learning algorithms that are used in practice. The choice of algorithm depends on the problem at hand, the size and complexity of the data, and the desired outcome.

✓ Naïve Bayes Classifier

Naïve In order to forecast values for the new class, the Bayes classifier uses discriminative learning to determine the probabilitie for each in a dataset. It is applied on the Bayes theorem; under the assumption that the features are independent, we may determine the likelihood that A (the hypothesis) will occur given that B (the evidence) has happened. The existence of one predictor or trait has no bearing on the other, making it naive.

✓ Support Vector Machine

One of the most popular machine learning (ML) algorithms for numerous applications, including pattern recognition, spam filtering, and intrusion detection, is SVM. For regression, classification, and distribution estimation, there are various SVM formulations. It comes from the best classification hyperplane that is linearly separable. Due to the fact that detecting DDoS attacks is equivalent to solving a binary classification.

.

✓ Random Forest

The Random Forest classifier uses the ensemble learning technique and is composed of many decision trees. Each tree included in the random forest offers a class prediction. The class with the most votes becomes the final forecast made by the entire model. The main goal of the classifier is to outperform any of its component models individually by using a large number of trees working together as a whole. Low correlation between the models is crucial. Uncorrelated models can result in models that are more accurate than any one forecast. The main explanation is that the trees protect one another from minor errors. If many other trees are right, even though some may be mistaken.

V. DATASET

Choosing an appropriate dataset is the main challenge in evaluating the effectiveness of intrusion detection systems. Monitoring network activity is usually required to gather the information for the dataset, which can be an expensive task. As a result, developers often prefer to utilize existing datasets to control their network or systems. This section highlights some of the most frequently employed datasets for attack detection systems.

A. *NSL-KDD dataset*

The NSL-KDD dataset used by [3] consists of network traffic data generated in a simulated environment using a variety of tools and techniques. The dataset includes both normal traffic and different types of attacks, such as DOS, inquire to local, and user-to-root attacks. The dataset contains a total of 41 features. The dataset is divided into training and testing sets, and each instance in the dataset is labeled as either normal or one of the four attack categories. The NSL-KDD dataset has become a widely used benchmark dataset for evaluating IDS and ML models for cyber-attack detection. However, it should be noted that due to the synthetic nature of the dataset, the results obtained using it may not always reflect real-world scenarios accurately.

B. KDD Cup 1999 dataset

The demand for a sufficient dataset to evaluate intrusion detection systems led to the development of KDD Cup99[6]. This simulation dataset, which was created in 1998, is frequently used in the domains of data mining and ML. Approximately 4 million data points make up the KDD Cup99 standard dataset, with 80% of those being assault data.

The dataset includes both training and test data, and features 41 categories that can be classified as basic, traffic, and content features. The data can be classified into five main categories, with four being attacks and one being normal. The attack types include DOS, Probe (Probing attacks), (Root to Local), and (User to Root), with 21 subtypes that fall into these categories. The KDD Cup99 dataset includes both numeric and text information about request categories, with an additional feature at the end indicating whether the data represents an intrusion or not.

C. CIC IDS 2017 dataset

CIC IDS 2017 The Canadian Institute for Cybersecurity (CIC) produced this dataset. Common attacks are included in the CIC IDS 2017 dataset, which is representative of real-world data. The conference on Big Data, Deep Learning, and Countering Cyber-crime is also included. The outcomes of the CICFlowMeter network traffic analysis in Ankara, Turkey, on the 3–4th of December, including source and destination IP addresses, ports, and attack methods. Furthermore, everybody should have access to the dataset. To create a trustworthy benchmark dataset, CIC has defined eleven requirements [11]. These standards include: fully configured network, fully trafficked, labelled dataset, fully interacted with, fully captured.

D. CSE-CIC-IDS2018

The Canadian Institute for Cybersecurity[21] and Communications Security Establishment have created a comprehensive dataset that provides detailed information on various types of attacks. Here the dataset includes more than 6 differents attack scenarios, including Bruteforce, DoS, Web, Infiltration, Botnet, DDoS…etc.

To collect data on Bruteforce attacks, the CIC used FTP Patator and SSH Patator tools. For DoS attacks, they used Hulk, GoldenEye, Slowloris, and Slowhttptest tools. The CIC collected data on Web attacks using Damn Vulnerable Web App and In-house Selenium framework tools. Infiltration attacks were recorded using Nmap and portscan tools, while screenshots and keylogging were used to collect data on Botnet attacks. The CIC used Low Orbit Ion Canon (LOIC) to collect data on DDoS attacks involving UDP, TCP, or HTTP requests. Heartleech, a type of DoS attack, was also included in the dataset.
The CIC team recorded the raw data on a daily basis, including network traffic and event logs. They used the CICFlowMeter-V3 to extract over 80 network traffic features during the feature extraction process from the raw data. Finally, the extracted features were saved as a CSV file per machine.

VI. DATASET COMPARISON

Datasets utilized for Intrusion Detection and Mitigation are constantly evolving due to the ongoing and dynamic changes in cybersecurity threats, with new attacks emerging every day. While the KDD Cup 99 dataset is a traditional option for this purpose, it has been found to contain numerous anomalies. To address some of these issues, the NSL-KDD dataset has been suggested. This dataset eliminates redundant records in the KDD 99 training set and ensures that there are no duplicate records in the proposed test sets. The NSL-KDD dataset includes 22 attack types in the KDD training set and an additional 17 attack types in the KDDTest data. With 41 attributes and one class attribute, respectively, it provides a more comprehensive option for intrusion detection and coping purposes.

VII. RESULTS

The evaluation metrics for ML models applied on four open DDoS datasets are presented in Table in below. The aim of the evaluation was to assess the performance of the datasets in detecting intrusion via DDoS attacks. The results indicate that the CSE-CIC-IDS2018 dataset [25] achieved the highest accuracy rate of 99% across all models and an F-measure of 99%. This suggests that a model trained using this dataset performs very well in predicting threats with high precision and recall rates across all models.

The random forest ensemble model outperformed the other machine learning models overall, reaching 100% accuracy for the NDSec-1 dataset and 99% accuracy for the other datasets. Additionally, for the NDSec-1 dataset[26] and 99% for the others, it attained 100% precision and recall. The accuracy of the naive Bayes method was the lowest, at 45%.
The 1 dataset with the fewest records (5,83) used the least amount of calculation time
volume of records (1,046,84 rows). In contrast, the NDSec-

CSE-CIC-IDS2018 dataset had the longest training time of 148 seconds, while the random forest algorithm got the big training time across all dataset
with the CICDDoS2019 dataset[27], and the SVM model produced the second-lowest result with an accuracy of 68% for the NDSec-1 dataset. The remaining models had consistent results.

***Table 2**: Performance metrics*

		K-NN	SVM	NAÏVE BAYES	DECISION TREE	RANDOM FOREST	LOGISTIC REGRESSION
CICDDOS2019	Accuracy	0.98	0.86	0.45	0.99	0.99	0.99
	Precision	0.99	0.86	0.66	0.99	0.99	0.99
	Recall	0.99	0.87	0.54	0.99	0.99	0.99
	F-measure	0.99	0.85	0.38	0.99	0.99	0.99
	Compilation Time	3.5 seconds	7.29 seconds	1.3 second	4.53 seconds	84.2 seconds	5.53 seconds
CSE-CICIDS2018	Accuracy	0.99	0.99	0.99	0.99	0.99	0.99
	Precision	0.99	0.99	0.99	1	0.99	0.99
	Recall	0.99	0.99	0.99	1	0.99	0.99
	F-measure	0.99	0.99	0.99	1	0.99	0.99
	Compilation Time	148.2 seconds	16.8 seconds	2.7 seconds	5.3 seconds	120.8 seconds	10.8 seconds
NDSEC-1	Accuracy	0.98	0.68	0.99	0.97	1	0.99
	Precision	0.99	0.81	1	0.99	1	0.99
	Recall	0.99	0.79	1	0.99	1	0.99
	F-measure	0.99	0.75	1	0.99	1	0.99
	Compilation Time	0.2 seconds	0.1 seconds	0.2 seconds	0.3 seconds	0.6 seconds	0.2 seconds
CICIDS2017	Accuracy	0.99	0.89	0.8	0.99	0.99	0.98
	Precision	0.99	0.93	0.88	0.99	0.99	0.98
	Recall	0.99	0.93	0.78	0.99	0.99	0.98
	F-measure	0.99	0.93	0.79	0.99	0.99	0.98
	Compilation Time	7.1 seconds	5.5 seconds	1.4 seconds	1.8 seconds	39.6 seconds	1.4 seconds

VIII. CONCLUSION

In conclusion, machine learning methods can be employed to assist in the detection and reduction of DDoS attacks. Anomalies and patterns connected to DDoS attacks can be found using ML algorithms, which can then be used to analyse network traffic patterns in real-time and launch automatic defences against the attack.

It's crucial to remember, though, that ML algorithms are not infallible and can still be exposed to hostile attacks. Adversaries can use techniques to manipulate the training data or exploit weaknesses in the algorithms to bypass detection.

Therefore, while machine learning can be a useful tool in combating DDoS attacks, Combining it with other security measures like firewalls, intrusion detection systems, and traffic filtering is recommended. Additionally, organizations should continuously update their machine learning models and algorithms to keep up with evolving attack techniques and to ensure optimal performance.

REFERENCES

[1] M. Priyanka, S. and Rakesh singh K. “Cyber Attacks On Intrusion Detection”, International Journal of information Sciences and Techniques (IJIST) vol. 6, 2016, No. 1/2.

[2] M. Shilpashree S,S,C. Lingareddy , Nayana G Bhat and Sunil Kumar G. “Decision Tree : A machine Learning for Intrusion Detection”, International Journal of innovative Technology and Exploring Engineering(IJITEE) vol. 8, 2019, pp. 2278-3075.

[3] M. G Uthej, K Mohammed H, Bala Suresh B., A Sai K. and Dr. C. Gulzar,” Detection of Cyber Attack In Network by Using Machine Learning”, Journal of Engineering Science (JES), vol 13, 2022, pp. 0377- 9254.--https://jespublication.com/upload/2022-V13I60151.pdf

[4] S. Akhil Repalle and Venkata Ratnam K., "Intrusion Detection System using AI and Machine Learning Algorithm" International Research journal of Engineering and technology (IRJET) vol.04, 2017, pp. 2395-0056.

[5] T. Kothari, A. Hedage , prof. Vaihali A. M and Prof Disha Sushant W. "Intelligent Intrusion Detection Systems with Machine Learning Models for Detecting Cyber Threats in IoT Network." International Research journal of Engineering and technology (IRJET) vol.10, 2021, pp. 2278-0181.

[6] Gozde K., Onder Demir, Ozgur Kray S., “Deep Learning in Intrusion Detection Systems” International Congress on Big data, Deep Learning and Fighting cyber terrorism, Ankara, Turkey, 3-4 dec, 2018.

[7] Yakub K. S., Aremu Idris A., Sanjay M., Monica K. H. and Ricardo Colomo-palacio “A Machine Learning Based Intrusion Detection for detecting internet of things network attacks” Alexandria Engineering Journal, Vol. 61, 2022, pp.9395-9409.

[8] Santhosh Kumar C., Sundharamurthy G., Vinoth Kumar S. and Vishnu Kumar K. “A supervised Machine Learning Based intrusion Detection Model For Detecting Cyber-Attacks Against Computer System,” International Journal of Communication Networks and Information Security, vol. 14, 2022, pp. 2076-0930.

[9] Abhijeet Prakash “Hack the world- Ethical Hacking”. Module 8, Denial of service-

[10] Ptacek H. T., and Newsham N. T. (1998) Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection. Secure Networks Inc.

[11] A. Alazab, M. Hobbs, J. Abawajy, and M. Alazab, Using Feature Selection for Intrusion Detection System, International Symposium on Communications and Information Technologies, 2012

[12] P. Ghosh, C. Debnath, D. Metia, and Dr. R. Dutta, An Efficient Hybrid Multilevel Intrusion Detection System in Cloud Environment, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. VII (Jul –Aug. 2014), PP 16-26.

[13] DipankarDasgupta. Immunity-based intrusion detection system: A general framework. In Proceedings of the 22nd Natio Information Systems Security Confer-ence (NISSC). Arlington, Virginia, USA, 1999..

[14] Peter Mell Karen Scarfone. Guide to intrusion detection and prevention systems (idps). National Institute of Standards and Technology, NIST SP - 800-94, 2007.

[15] Intrusion Detection Based On Artificial Intelligence Technique –International Journal of Computer Science Trends and Technology (IJCST)–Volume.2,Issue,4,,July-Aug,20

[16] Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014).

[17] B. B. Zarpelao, R. S. Miani, C. T. Kawakami, and S. C. de Alvarenga, "A survey of intrusion detection in the internet of things;' Journal of Network and Computer Applications, vol. 84, pp. 25-37, 2017.

[18] A.Vanamala Kumar, G. Lalitha Kumari, Y. Surekha “ANALYSIS OF MACHINE LEARNING BASED CYBER SECURITY” in Test Engineering and Management , Vol-83, ISSN-0193-4120 Apr-2020

[19] B. Dong and X. Wang, “Comparison deep learning method to traditional methods using for network intrusion detection,” in Proc. IEEE ICCSN, 2016, pp. 581–585.

[20] Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., and Li, K. (2020). A Survey of Intrusion Detection for In-Vehicle Networks. IEEE Transactions on Intelligent Transportation Systems, 21(3):919–933.

[21] Areej Alhasani1 , Faten Al omrani2 , Taghreed Alzahrani3 , Rehab alFahhad4, Mohamed Alotaibi5 “Role of Machine Learning in Intrusion Detection System”, IJCSNS International Journal of Computer Science and Network Security, VOL.22 No.3, March 2022

[22] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry, 12(5), 754.

[23] Delplace preprint arXiv:2001.06309, A., Hermoso, S., & Anandita, K. (2020). Cyber Attack Detection thanks to Machine Learning Algorithms. arXiv

[24] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1), 1-22.

[25] University of New Brunswick, “CSE-CIC-IDS2018 on AWS,” 2018.[Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html.

[26] F. Beer, T. Hofer, D. Karimi, and U. Bühler, “A new attack composition for network security,” in Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), 2017.

[27] University of New Brunswick, “DDoS Evaluation Dataset (CICDDoS2019),” unb.ca, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor
7.54

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com