Machine Learning Techniques for Detecting DDOS Attacks

Conference Paper · October 2023

DOI: 10.1109/eSmarTA59349.2023.10293366

CITATIONS
4

READS
461

9 authors, including:

Mamoon M. Saeed
University of Modern Sciences
35 PUBLICATIONS **263** CITATIONS
SEE PROFILE

Rashid Saeed
Taif University
321 PUBLICATIONS **3,578** CITATIONS
SEE PROFILE

Abdulguddoos S. A. Gaid
Taiz University (Faculty of Engineering & Information Technology)
37 PUBLICATIONS **190** CITATIONS
SEE PROFILE

Machine Learning Techniques for Detecting DDOS Attacks

Mamoon M. Saeed
Department of Communications and Electronics Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Yemen
Mamoon503@gmail.com

Rashid A. Saeed
Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
eng_rashid@hotmail.com

AbdulGuddoos S. A. Gaid
Dept. of Communication & Computer Engineering, Faculty of Engineering & Information Technology, Taiz University, Taiz, Yemen
quddoos.gaid@taiz.edu.ye

Husam Nedhal Rashad Mohammed
Department of Computer Network Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Yemen
hossamalmamari@gmail.com

Hossam Mohammed Ahmed Morei
Department of Computer Network Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Yemen
Hssm736558084@gmail.com

Ameen Sami Ameen Saif Al-Uosfi
Department of Computer Network Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Yemen
Ameen362000@gmail.com

Othman abdulkafi hazaea gazem
Department of Computer Network Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Yemen
athmanalafifi100@gmail.com

Aimen Ebdulkreem Thabet Eidah
Department of Computer Network Engineering, Faculty of Engineering, University of Modern Sciences (UMS) Yemen
aymoeida123@gmail.com

Mohamed Galal Qasem Al-madhagi
Department of Computer Network Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Yemen
mohamedgalal9677@gmail.com

***Abstract*— The development witnessed by the world of science and technology and the emergence of the Internet, where cybersecurity has become one of the most important areas that are growing rapidly every day, and one of its goals is to maintain access to users at any time. Where it is noted that the biggest enemy for the availability is Distributed Denial of Service (DDoS) attack, which works to prevent access to the service and slow down the service. Through this paper, machine learning will be used to discover the DDoS attack and know its type to be aware of it and take the necessary measures for that. Where the CICDDoS2019 dataset will be used. After it is studied, analyzed, cleaned and the best algorithm was selected. Five classification algorithms (Random Forest, Decision Tree, SVM, Naive Bayes, and xgboost) were used to train and test the data from the datasets, and it can be said that of the five, Random Forest algorithms had the highest level of accuracy (99.95426%).**

Keywords—DDOS attacks; machine learning; accuracy; algorithms.

I. INTRODUCTION

Design problems are made worse and security is increased by the power, processing, and memory constraints of network hardware and systems in general and the Internet of Things in particular. To be able to transmit data privately and securely across an infinite number of devices, new, inventive, and effective security protocols, procedures, and methods that can match the requirements and specifications of existing and new devices are required [1–5]. DDoS assaults provide a severe security risk to network systems, the Internet of Things, and cybersecurity in a variety of security attacks.

DDoS is regarded as one of the most hazardous cyberattacks that have ever occurred and continue to do so because, in 2020, more than 10 million DDoS attacks were identified in just one year, according to NetScout. And in only one month, fraudsters launched roughly 5.4 million DDoS attacks [6]. The first is for 2021 and represents an 11% rise over the corresponding time in 2020. Forecasts indicate that DDoS attacks will increase to 15.4 million by 2023 [7].

The threat of DDoS attacks and the consequent need for enhanced security can be seen in these numbers, along with the location and timing of the attack [8]. In a distributed denial of service (DDoS) assault, an excessive amount of Internet data is sent to a network or service to obstruct regular traffic. DDoS assaults are more effective because they can use a large number of computers connected to the Internet and other devices as a source of attack traffic [9]. Computers and other connected resources, such as Internet of Things (IoT) devices, are common targets for these attacks. When a DDoS attack occurs, the server's connectivity and bandwidth are severely compromised, which results in significant disruptions for all the different network services [10].

DDoS assaults' main objective is to disrupt the network and reduce the resources available to actual users. when a malicious assault causes the network to be overloaded above its bandwidth capacity, causing downtime and service disruption. Healthcare facilities, banks, and unnoticed public networks are all potential targets. Since legitimate and offensive traffic during a DDoS attack is so identical, it is impossible to distinguish between them [11]. They resemble normal network packets in many ways, but they are more concentrated on the target and are sent in larger numbers. A malicious assault is simpler to spot and defend against when only a small number of nodes are used. Given that a typical DDoS attack typically involves a large number of nodes, the

979-8-3503-0533-3/23/$31.00 ©2023 IEEE

overall behavior of these nodes significantly diminishes the likelihood of satisfying valid requests [12].

Machine learning algorithms that can assess the harm brought on by those packets are applied to counteract various DDoS attacks. Using machine learning techniques like decision trees, random forests, and KNN, DDoS detection has been demonstrated. A trained neural network has been found to produce less accurate results than deep learning, which combines machine learning and several abstraction layers [13]. Deep learning has enhanced the capabilities of devices, making them appropriate for a wide range of devices, including IoT devices [14]. One of the disciplines of artificial intelligence, machine learning, is used to find patterns in data. To develop a data-driven model, it employs algorithms [15]. Machine learning is a fantastic option due to its versatility in situations where data is always changing and task difficulty is continually changing [16,17].

This paper is organized as follows for the remainder: In Section II, the relevant works are displayed. Distributed denial of service (DDOS) attacks are described in Section III. The examples of the suggested system implemented using the used datasets are provided in Section IV, as the methodology, and several machine learning (ML) approaches in detail. In Section V, the findings and analyses are compiled. The final section, Section VI, contains the conclusion.

II. Related Work

ML has been used to detect DDoS attacks in numerous research. The CICDDoS2019 data set was used, and the DDOS attacks in this data set were compared, as the authors in [18] recommended A. Several algorithms were used to analyze the threat determination success rates, including Artificial Neural Networks (ANN), Support Vector Machines (SVM), Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regression, K-nearest Neighbor (KNN), Decision Tree (entropy-Gini), and Random Forest. The models that virtually always succeed—those created with K-nearest neighbor, Logistic Regression, Naive Bayes, and Multinomial-Bernoulli algorithms—have the highest success rates, it has been observed.

In contrast, the authors of [19] proposed a deep learning approach for identifying and thwarting flood attacks, also known as DoS-based Hello on the IoT healthcare network. They used the Deep Belief Network (DBN) model to confirm this kind of attack, which entailed sending plenty of Hello packets to slow down the network. The bypass-linked attacker update-based rider optimization algorithm (BAU-ROA) is a tool that the DBN approach has used to produce a variety of useful outcomes and function even better [20]. The development of the high-performing optimization technique known as BAU-ROA, a metaheuristic algorithm with a simple calculation methodology and fewer computing parameters, was done to enhance the execution of ROA. The BAU-ROA algorithm has been shown to perform better than other optimization algorithms when it comes to the DBN operational procedure in experiments [21].

According to IoT application and design, the authors of [22] provided a thorough analysis of recent and earlier studies in IoT traffic characterization. In the survey provided, the main focus on traffic characterization for security issues has been highlighted as the key attention of the articles in IoT. The accuracy, precision, recall, and F1 score of four ML algorithms i.e., DT, KNN, NB, and gradient-boosting (GRB) classifiers were compared in this study, along with the performance of each approach overall [23]. They made use of the BoT-IoT dataset. DT and GRB performed better in terms of accuracy, according to the performance evaluation findings of this study. The IoT networks' greater security will be aided by these impressive achievements.

To identify these attacks, a hybrid machine learning-based technique has been proposed, according to the authors of [24]. Blackhole optimization and the extreme learning machine (ELM) model are combined to implement the suggested method. To test the effectiveness of our suggested technique, several experiments have been carried out using four benchmark datasets: NSL KDD, ISCX IDS 2012, CICIDS 2017, and CICDDoS 2019. The accuracy is 99.23%, 92.19%, 99.50%, and 99.80% using NSL KDD, ISCX IDS 2012, CICIDS 2017, and CICDDoS 2019, respectively [25]. It is also done to compare the performance of the proposed method with existing methods based on ELM, backpropagation ANN, artificial neural network (ANN) trained with blackhole optimization, and other cutting-edge methods [26].

It was made obvious by the authors in [27] that adding a well-known DDoS dataset called CICDoS2019 would improve the accuracy of DDoS attack identification. The DDoS dataset has also undergone preprocessing utilizing two major methods to extract the most pertinent information. The DDoS dataset will be used with four distinct machine-learning models [28]. The Random Forest machine learning model, with an improvement over recently developed DDoS detection systems, provided the best detection accuracy with (99.9974%), according to the results of actual testing.

The three-level application layer architecture used by the creators of [29] for detecting DDoS attacks. The first level is in charge of choosing the samples' best attributes and categorizing the traffic as either benign or malicious; the second level is made up of a hard-voting classifier to determine if the DDoS source is UDP, TCP, or mixed-based. Last but not least, the DDoS type that best suits the attack is aligned at this level [30]. The accuracy score, precision, and time are employed as the model performance metrics in this approach's validation on the CIC-DDoS2019 dataset. The suggested architecture significantly outperforms the currently used machine learning (ML) methodologies in categorizing application-layer DDoS attacks both binary and multiclass [31].

III. Distributed Denial Of Service (DDos) Attack

A distributed denial-of-service (DDOS) assault is one kind of malicious operation that can obstruct the regular flow of traffic on a targeted server, service, or network. By using numerous compromised computer systems as attack traffic sources, this kind of attack overwhelms the target and the area's infrastructure with a massive amount of internet traffic [32]. Although the networking infrastructure is mostly secured, it is often vulnerable to DDOS attacks. The purpose of DDOS attacks may not necessarily be to steal information but to disrupt the network flow enough to cause significant losses for the targeted company.

According to [33], there are two major categories under which DDOS attacks can be divided. Reflexion-based DDOS assaults make up the first section. In this kind of assault, attack traffic, including HTTP calls, is transmitted to the target while the attacker's identity is concealed using

cyberspace devices. Targeting the IP addresses in the reflector servers (bots), these requests are delivered via the originating IP address. The victim receives notification of all of these conflicting demands as a result.

These attacks frequently use TCP, UDP, or a combination of the two to exploit application protocols. MSSQL or SSDP can be used in attacks that are TCP-based, while CharGen, NTP, or TFTP can be used in assaults that are UDP-based [34]. These protocols—DNS, LDAP, NetBIOS, SNMP, or PORTMAP—can be combined in attacks that have been proven to exist. Exploitation-based attacks, which also use TCP and UDP, are the second type of DDOS attack. Attacks based on UDP, such as UDP flood and UDP-Lag, are UDP-based, in contrast to attacks based on TCP, such as the SYN flood attack [35].

IV. METHODOLOGY

In the first step, a large dataset was taken to distinguish between DDOS and non-DDOS captured from CIC 2019 DDOS. The second step is Data pre-processing the form errors to make it suitable to be fed into the model. The third and fourth steps choose the best set of features to build the machine learning model under the features selection Then the process is to divide the data into training and test sets. Finally, the implementation of machine learning algorithms. Fig. 1 briefly represents our approach to identifying DDOS and non-DDOS in detail.

A. Data preprocessing

Without raw data processing, a good model cannot be built. Usually, the data flow can be divided into some steps as follows:

- Removing noise and missing values

First, remove the noisy and missing data. The raw data set may contain some noisy data and missing values. Noisy data is less valuable data. First, the noisy and missing data has been removed.

The following columns were found: Timestamp', 'Flow ID', ' Source IP', ' Destination IP' 'SimilarHTTP', 'Unnamed: 0 Since they were private in the Canadian Institute there are also some infinity values in our array. some errors were found. The following columns: FIN Flag Count, PSH Flag Count, ECE Flag Count, Bwd PSH Flags, Fwd URG Flags, Bwd URG Flags, Fwd Avg Bytes/Bulk, Fwd Avg Packets/Bulk, Fwd Avg Bulk Rate, Bwd Avg Bytes/Bulk, and Bwd Avg Bulk Rate Packets/Bulk', 'Bwd Avg Bulk Rate' was empty, so they are dropped

- Removing Duplicate values

In the raw data set, there were a few duplicate values. These redundant values have been removed from the dataset.

- Data Standardization

Data standardization means data modification. There are many methods available. Standardization was used for standardization. This means that a dataset has been drawn up.

B. Feature Selection

The 24 specific features that were used in the study were used [36] to evaluate the significance of specific features in the dataset, and DDoS Attacks RFR was utilized. The features that were employed in this are listed in Table 1 along with a brief description.

C. The Binary classification used in the implementation

It is a type of classification that divides data into only two main categories, usually a positive category and a negative category, or 1 and 0. The class 11 nomenclature used in the vulnerability implementation in this study is introduced, converting all attacks to 1 and non-attacks to 0 [37]. These attacks are anticipated in light of the twenty-four qualities listed in Table I above. With a brief description of exploit-based and reflection-based DDoS assaults, Table II gives the Class 11 terminology that is employed.

D. Training or Testing machine learning classifier

The training and testing of the learning classification machine were initiated after the feature selection process was completed. Thus, the training dataset and test data set were created from the data. Algorithms for machine learning classification were employed to train and test the dataset. The model is trained using the data [38]. creates a working model. Data testing is utilized to evaluate the device's performance as well as the model's capacity to identify fresh assaults and produce fresh outcomes. A total of 75% of the data was used for training and only 25% for testing.

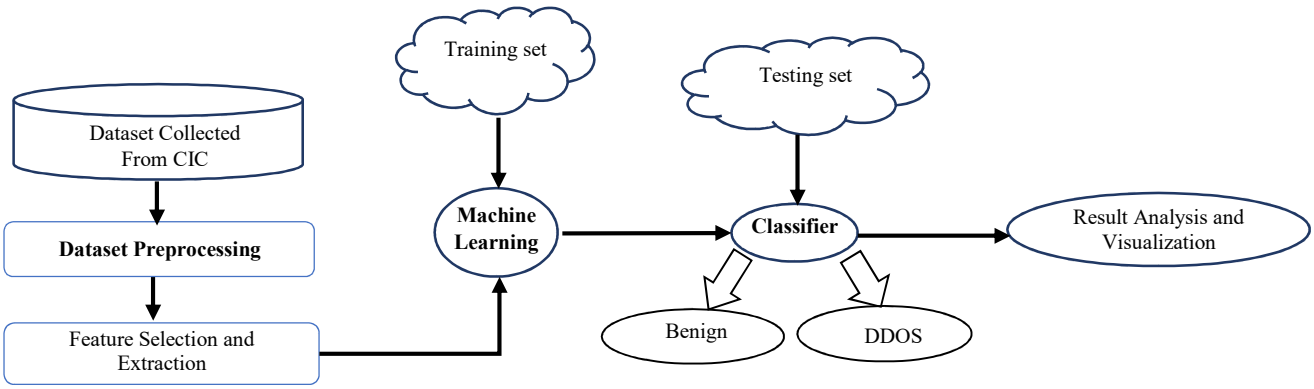

Fig. 1. The approach which identifies DDOS and non-DDOS.

TABLE I. THE FEATURE SET UTILIZED IN THE IDS

Feature	Description
Fwd iat mean	Between two packets on the forward route, in the interim
Fwd at max	The longest possible interval between any two packets traveling forward
Min Packet Length	A packet's bare minimum size
Max Packet Length	A packet's maximum size
Average packet size	standard size for a package
Fwd packets /s	Count of packets being forwarded per second
Fwd header length	A packet's forwarded packet header size
Fwd packet length std	A packet's forward-direction standard deviation
Flow lat min	The shortest amount of time that must elapse between two packets in a flow
Subflow fwd bytes	The average number of bytes in a sub-flow moving forward
Destination port	The address to accept the supplied TCP or UDP packets for data transfer
Protocol	The average packet variation
Packet length std	Duration of the flow
Flow duration	The duration of flows in us
Fwd header length 1	Aheader's forward-moving bytes in a header
Min_seg_size_forward	The smallest possible segment size moving forward
The total length of fwd packet	Size of the packets moving forward
Fwd iat total	The duration between each pair of packets on the forward route
Ack flag count	The number of ACK-containing packets
Init_win_bytes_forward	How many bytes are in the early window in the forward route?
Flow is mean	Flowing between two packets in the meantime
Flow at max	The most time between any two packets in the flow
Fwd Packet Length Max	Forward (outgoing) direction's maximum packet size
Fwd Packet Length Min	Most compact packet sizes on the forward route

TABLE II. THE CLASS 11 NOMENCLATURE.

	Type	Class	Description
Reflection based attack	UDP Attacks	NTP	In an expansion attack known as NTP [22], the attacker makes use of publicly accessible NTP servers to bombard the target with UDP traffic.
		TFTP	A TFTP attack takes advantage of a buffer overflow flaw in TFTP and its server [23].
	TCP Attacks	MSSQL	The MSSQL exploit enables the execution of malicious SQL declarations [14].
		SSDP	The SSDP attack depletes the victim's computational capabilities by using UPnP protocols to direct a ton of traffic their way [24].
	TCP/UDP Attacks	DNS	A DNS attack takes advantage of DNS protocol flaws [25].
		LDAP	An exploit known as LDAP injection affects web-based applications that create LDAP statements using user-supplied data [26].
		NETBIOS	A NetBIOS flaw enables data reading by an attacker [27].
		SNMP	An SNMP attack uses large amounts of traffic directed toward multiple victims in different networks [28].
Exploitation based attack	TCP Attacks	SYN Flood	In an SYN flood attack, the attacker floods a target system with a series of SYN requests, causing server resources to be depleted and rendering the system unable to handle legitimate traffic [29].
	UDP Attacks	UDP	UDP flooding attacks are a type of attack that is based on sending a high amount of UDP packets to the victim to download them in a way that makes them unable to respond, which leads to a heavy load on the firewall of the victim server [30].
		UDP-Lag	UDP-Lag is one of the types of attacks that disrupt the relationship between the client and the server, which leads to its inactivation [31].

V. RESULTS AND DISCUSSIONS

To work with any dataset, one needs to parse it properly to get a very good result. Several computational matrices such as ROC curve, accuracy score, confusion matrix, and classification report have been generated. Here, five machine learning classification algorithms have been applied for DDoS detection and Benign [39]. After pre-processing the analyzed data set.

Another performance metric that demonstrates the diagnostic capability of a binary classifier is the Receiver Operating Characteristic Curve [40]. By examining the ROC curve in Fig. 2, it can be seen that the Random Forest model is close to the True Positive Rate (TPR), and the AUC is 0.9988, whereas the Decision Tree model denotes a start deviation slightly above the True Positive Rate (TPR), and the AUC is 0.9081, denotes the XGBoost model is close to the True Positive Rate (TPR), and the AUC is 0.9824, the Naive Bayesian model denotes a start to work with any data set, it has to be analyzed properly to get a very good result [41-42].

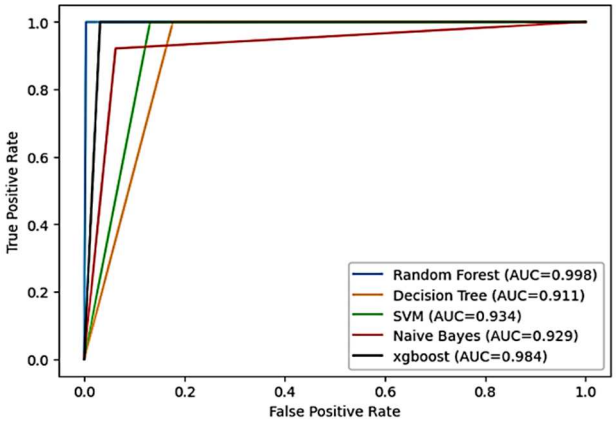

Fig.2. The Receiver Operating characteristic curve of different Algorithms.

Various computational matrices such as the ROC curve, accuracy score, confusion matrix, and classification report have been constructed. Table III displays the use of five machine-learning classification algorithms for benign and DDoS detection. After pre-processing the particular data set analyzed in this paper.

Fig. 3 shows the performance metrics of selected algorithms. Five classification algorithms (Random Forest, Decision Tree, SVM, Naive Bayes, and xgboost [40]) were used to train and test the data from the datasets, and it can be said that of the five, Random Forest algorithms had the highest level of accuracy (99.95426%). As a result, this technique can be used to recognize DDOS attacks. The result is the development and enhancement of defense solutions against this kind of attack, which is extremely dangerous for both big and small businesses as well as Internet users [43-44].

TABLE III. RESULTS OF DIFFERENT ALGORITHMS OVER THE DATASET

Metric	Random Forest	Decision Tree	SVM	Naive Bayes	xgboost
Accuracy Score	99.954260	99.858607	99.774889	92.135307	99.946915
Precision Score	99.998824	99.887308	99.926878	99.958176	99.978583
Recall Score	99.955154	99.991853	99.862943	92.125467	99.968003
F1 Score	99.976984	99.937049	99.884082	95.882121	99.973292
AUC Score	99.882027	90.819277	93.985528	92.930055	92.930055
Confusion Matrix	[7312 14] [534 1190216]	[5983 1343] [351 1190399]	[6456 870] [1827 1188923]	[6867 459] [93766 1096984]	[7071 255] [381 1190369]
Total misclassification	548	1694	2697	94225	636
Total correct classification	1197528	1196382	1195379	1103851	1197440

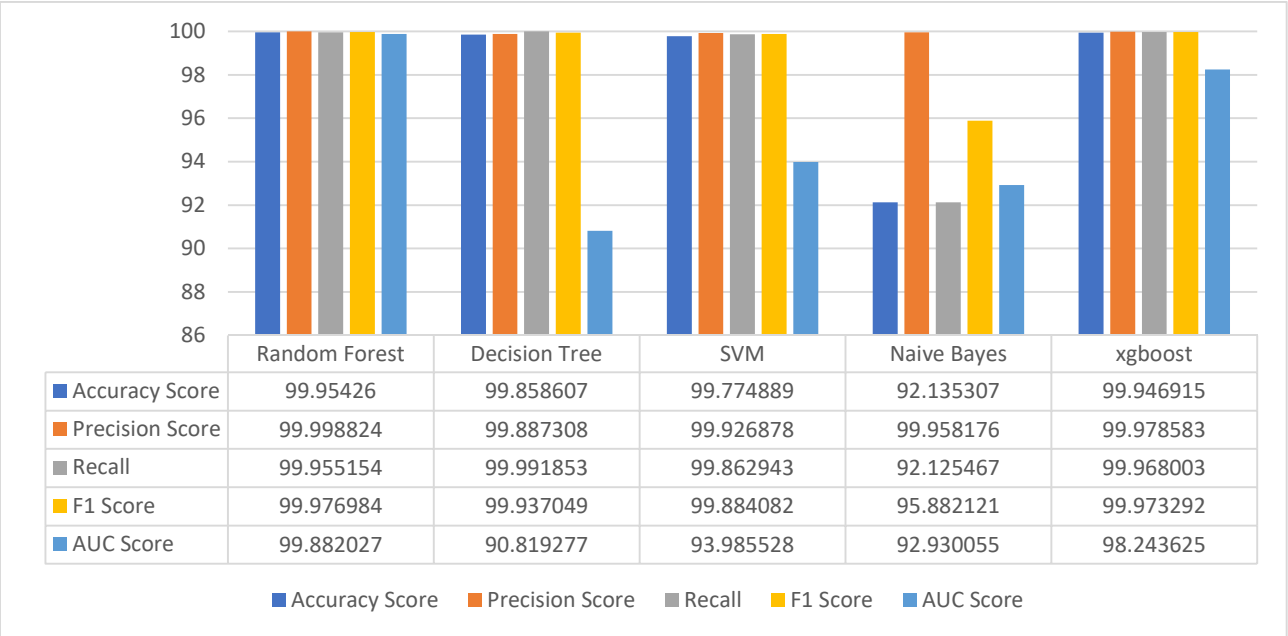

Fig. 3. The performance metrics of selected algorithms.

VI. CONCLUSION AND FUTURE WORK

This paper evaluated the effectiveness of using intelligent classification to detect DDoS attacks. The CiCDDOS2019 dataset was chosen for this scenario because there are many attack classes and families of the most common and recent DDOS, which are similar to the real data from which a DDOS classification can be proposed. From the datasets, there is training and testing of the data using five classification algorithms (Random Forest, Decision Tree, SVM, Naive Bayes, and xgboost), it can be concluded that from the five classification algorithms used, Random Forest algorithms have achieved the highest level of accuracy (99.95426%) This means that this algorithm can detect DDOS attacks and this can be used. The results are to develop and improve protection technologies from this type of attack, which poses a great danger to large and small companies and Internet users.

Future research can offer useful insights into the strengths and weaknesses of various machine learning algorithms by taking into account variables like computational complexity, training time, and capability to handle real-time data, assisting users in making decisions about which algorithm to use in their particular context.

Also, the potential limitations and future directions, such as exploring ensemble methods or deep learning techniques are recommended for future study, to further improve detection accuracy and adaptability to evolving attack strategies.

REFERENCES

[1] Bakri H., et. al., "Machine Learning for Industrial IoT Systems." In Handbook of Research on Innovations and Applications of AI, IoT, and Cognitive Technologies. edited by Zhao, Jingyuan, and V. Vinoth Kumar, 336-358. Hershey, PA: IGI Global, 2021.

[2] Mahboub, Sara A. and et. al.,"Smart IDS and IPS for Cyber-Physical Systems." In Artificial Intelligence Paradigms for Smart Cyber-

Physical Systems. edited by Luhach, Ashish Kumar, and Atilla Elçi, 109-136. Hershey, PA: IGI Global, 2021.

[3] Faroug M. Osman, et. al.,. "Cyber-Physical System for Smart Grid." In Artificial Intelligence Paradigms for Smart Cyber-Physical Systems. edited by Luhach, Ashish Kumar, and Atilla Elçi, 301-323. Hershey, PA: IGI Global, 2021.

[4] Hassan, M; et. al., 'Artificial intelligence in IoT and its applications' (Telecommunications, 2021), 'Intelligent Wireless Communications', Chap. 2, pp. 33-58, IET Digital Library,

[5] R. Amrish, K. Bavapriyan, V. Gopinaath, A. Jawahar, C. Kumar, Mobile, Analytics,, and Cloud, "DDoS detection using machine learning techniques," vol. 4, no. 1, pp. 24-32, 2022.

[6] M. M. Saeed, E. S. Ali, and R. A. Saeed, "Data-Driven Techniques and Security Issues in Wireless Networks," in Data-Driven Intelligence in Wireless Networks: CRC Press, 2023, pp. 107-154.

[7] M. Saeed et al., "Preserving privacy of user identity based on pseudonym variable in 5G," vol. 70, no. 3, pp. 5551-5568, 2022.

[8] R. A. Saeed, M. M. Saeed, R. A. Mokhtar, H. Alhumyani, and S. Abdel-Khalek, "Pseudonym Mutable Based Privacy for 5G User Identity," vol. 39, no. 1, pp. 1-14, 2021.

[9] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT," vol. 7, no. 7, pp. 6242-6251, 2019.

[10] Y. Chen, J.Sheu, et. al.,, "Design and implementation of IoT DDoS attacks detection system based on machine learning," in 2020 European Conference on Networks and Communications (EuCNC), 2020, pp. 122-127: IEEE.

[11] M. M. Saeed, et. al., "Green Machine Learning Approach for QoS Improvement in Cellular Communications," in 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), 2022, pp. 523-528: IEEE.

[12] P. S. Saini, S. Behal and S. Bhatia, "Detection of DDoS Attacks using Machine Learning Algorithms," 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2020, pp. 16-21,

[13] S. ur Rehman et al., "DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)," vol. 118, pp. 453-466, 2021.

[14] A., Fahad et. al.,. 'Machine Learning Techniques in Internet of UAVs for Smart Cities Applications'. Journal of Intelligent & Fuzzy Systems, vol. 42, no. 4, pp. 1-24, 2021

[15] R. Aswathy, et al. Optimized Tuned Deep Learning Model for Chronic Kidney Disease Classification. CMC-Computers, Materials & Continua, 70(2), 2097–2111,2022.

[16] R. F. Mansour, et. al.,. "Optimal deep learning-based fusion model for biomedical image classification" Expert Systems, vol. 39, no. 1, pp. 34-54, June 2021.

[17] Eز Sayed et. al.,."Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications", Wiley-Hindawi, Journal of Security and Communication Networks (SCN), Volume 2021, 2021

[18] L. E. Alatabani; et. al.,."Robotics architectures-based machine learning and deep learning approaches", 8th International Conference on Mechatronics Engineering (ICOM 2022), 2022 p. 107 – 113, Kuala Lumpur, Malaysia.

[19] R. J. Alzahrani and A.Alzahrani, "Survey of Traffic Classification Solution in IoT Networks," vol. 183, pp. 37-45, 2021.

[20] M. M. Saeed, et. al.,., "Green Machine Learning Approach for QoS Improvement in Cellular Communications," 2022 IEEE MI-STA, 2022, pp. 523-528.

[21] L. Anatabine, et. al., "Deep and Reinforcement Learning Technologies on Internet of Vehicle (IoV) Applications: Current Issues and Future Trends", Journal of Advanced Transportation, vol. 2022, Article ID 1947886, 16 pages, 2022.

[22] G. S. Kushwah, V. Ranga, and C. Sciences, "Distributed denial of service attack detection in cloud computing using hybridextreme learning machine," vol. 29, no. 4, pp. 1852-1870, 2021.

[23] E. S. Alghoson, O. Abbass, and Applications, "Detecting Distributed Denial of Service Attacks using Machine Learning Models," vol. 12, no. 12, 2021.

[24] B. M. Kanber, et. al., "DDoS Attacks Detection in the Application Layer Using Three Level Machine Learning Classification Architecture," vol. 14, no. 3, 2022.

[25] J. M. Biju, N. Gopal, A. Prakash, and Technology, "Cyber attacks and its different types," vol. 6, no. 3, pp. 4849-4852, 2019.

[26] I. Sharafaldin, et. al.,. "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in 2019 International Carnahan Conference on Security Technology (ICCST), 2019, pp. 1-8: IEEE.

[27] A. Lohachab, B et. al.,."Critical analysis of DDoS—An emerging security threat over IoT networks," vol. 3, pp. 57-78, 2018.

[28] Q. Liu and Y. Zhang, "TFTP vulnerability finding technique based on fuzzing," vol. 31, no. 14, pp. 3420-3426, 2008.

[29] X. Wang, et. al.,. "Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps," in USENIX Security Symposium, 2019, pp. 1151-1167.

[30] A. Hudaib, E. Hudaib, and Security, "DNS advanced attacks and analysis," vol. 8, no. 2, p. 63, 2014.

[31] J. M. Alonso, et. al.,."LDAP injection techniques," in 2008 11th IEEE Singapore International Conference on Communication Systems, 2008, pp. 980-986: IEEE.

[32] B. G. Sarıkoz, "An Information security framework for web services in enterprise networks," Middle East Technical University, 2015.

[33] L. Rudman and B. Irwin, "Characterization and analysis of NTP amplification based DDoS attacks," in 2015 Information Security for South Africa (ISSA), 2015, pp. 1-5: IEEE.

[34] J. Gondim, R. de Oliveira Albuquerque, and A. Orozco, "Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols," vol. 108, pp. 68-81, 2020.

[35] J.-P. A. et. al., "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," pp. 1-44, 2022.

[36] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0, 2000, vol. 3, pp. 2275-2280: IEEE.

[37] J. Chica, J. Imbachi, J. Vega, and C. Applications, "Security in SDN: A comprehensive survey," vol. 159, p. 102595, 2020.

[38] A. Ahmed, et. al.,. "Machine Learning in Cyber-Physical Systems in Industry 4.0." In Artificial Intelligence Paradigms for Smart Cyber-Physical Systems. edited by Luhach, Ashish Kumar, and Atilla Elçi, 20-41. Hershey, PA: IGI Global, 2021

[39] R. Salih Abdalla; et. al.,.IoE Design Principles and Architecture; Book: Internet of Energy for Smart Cities: Machine Learning Models and Techniques; CRC Press Publisher,

[40] Saeed, M.M.; et. al.,.. Anomaly Detection in 6G Networks Using Machine Learning Methods. Electronics 2023, 12, 3300.

[41] Khalifa, O.O.; et. al.,. An IoT-Platform-Based Deep Learning System for Human Behavior Recognition in Smart City Monitoring Using the Berkeley MHAD Datasets. Systems 2022, 10, 177.

[42] Gadal, S.; et. al.,.. Machine Learning-Based Anomaly Detection Using K-mean Array and Sequential Minimal Optimization. Electronics 2022, 11, 2158.

[43] A. Khan, et. al.,."PackerRobo: Model-based robot vision self-supervised learning in CART," Alexandria Engineering Journal, Volume 61, Issue 12, 2022, Pages 12549-12566,

[44] M. B. Hassan, et. al.,. "Green Machine Learning for Green Cloud Energy Efficiency," 2022 IEEE MI-STA, 2022, pp. 288-294.