Review of Detection Denial of Service Attacks using Machine Learning through Ensemble Learning

Nazanin Najm Abdulla [1]

[1]*Informatics Institute for Postgraduate Studies Iraqi Commission for Computers & Informatics(IIPS/ICCI)*

Nazanin.shafi95@gmail.com

Rajaa K. Hasoun [2]

[2] *Department of Information System Management, University of Information Technology and Communications Baghdad, Iraq*

dr.rajaa@uoitc.edu.iq

Abstract - Today's network hacking is more resource-intensive because the goal is to prohibit the user from using the network's resources when the target is either offensive or for financial gain, especially in businesses and organizations. That relies on the Internet like Amazon Due to this, several techniques, such as artificial intelligence algorithms like machine learning (ML) and deep learning (DL), have been developed to identify intrusion and network infiltration and discriminate between legitimate and unauthorized users. Application of machine learning and ensemble learning algorithms to various datasets, consideration of homogeneous ensembles using a single algorithm type or heterogeneous ensembles using several algorithm types, and evaluation of the discovery outcomes in terms of accuracy or discovery error for detecting attacks. The survey literature provides an overview of the many approaches and approaches of one or more machine-learning algorithms used in various datasets to identify denial of service attacks. It has also been shown that employing the hybrid approach is the most common and produces better attack detection outcomes than using the sole approaches. Numerous machine learning techniques, including support vector machines (SVM), K-Nearest Neighbors (KNN), and ensemble learning like random forest (RF), bagging, and boosting, are illustrated in this work (DT). That is employed in several articles to identify different denial of service (DoS) assaults, including the trojan horse, teardrop, land, smurf, flooding, and worm. That attacks network traffic and resources to deny users access to the resources or to steal confidential information from the company without damaging the system and employs several algorithms to obtain high attack detection accuracy and low false alarm rates.

Keywords: Machine-Learning, Ensemble-Learning, Denial of Services Attack, Distribution Denial of Services.

I. INTRODUCTION

A computer's security refers to defending the system from any strange activity that could cause damage or result in the loss of data and resources. Since the goal of network hacking is to prohibit users from accessing the network's resources, whether for offensive or financial reasons, it has grown more harmful for resources, especially in businesses and organizations that rely on the internet [1]. Any attackers organize the transmission of a large amount of meaningless data to try to overload the target's computing resources or the close network links in a volumetric DoS attack. DoS is the most dangerous attack that causes network traffic problems [2]. Since the Computer Incident Warning Service announced the first attack event in 1999, DDoS attacks have been one of the most persistent network security risks. DDoS attacks continue to pose a serious threat that only worsens yearly, even though several protection measures have been proposed in business and academia. Any network architecture must address the crucial security issue of DDOS assaults. The entire network may be damaged when excessive bandwidth is used, such as during DDoS attacks [3]. With the help of the supervised ml task of learning a function that maps an input to an output based on example input-output pairs such as Dt, FR, and ensemble learning techniques. The unsupervised algorithms recognize previously unidentified patterns in data to develop rules like k-means. This study intends to gather knowledge about how machine learning through ensemble learning might be used to identify assaults, particularly those that block access to network traffic like denial of service attacks. Ensemble learning improves machine learning performance by combining several models. It may be difficult to learn a single model that applies to all forms of invasions due to the diverse nature of intrusions. The basic idea is to train many intrusion detection models and combine them into a single system. This study also examines several attack detection methods utilizing hybrid algorithms like SVM-K-NN, bagging, or boosting. It shows numerous attacks and how used ensemble learning that. By merging many models, ensemble learning enhances the performance of machine learning. This tactic performs better than a single model in terms of prediction accuracy. The advantages of ensemble learning, combining multiple classifiers to create a more effective classifier, have received extensive research in the machine learning (ML) community. There are two methods for ensemble classifiers: homogeneous and heterogeneous. When similar classifiers are combined to generate a training model, the result is a homogenous ensemble (e.g., bagging, boosting). In contrast, various classifier types create a heterogeneous ensemble for detecting various DoS attacks. The rest of the study is structured as follows: Section II presents the types of DoS attacks and Ensemble learning algorithms; section III offers a method that is related to our work; section IV addresses the related work; section V explores the rationale and challenges of the papers that collected, and section VI wraps up our research.

2. Denial of Service Attack

A DOS attack is launched against a single system by a group of infected computers known as bots or zombies. A DOS attack is computer security in which a hacker attempts to prevent end-users from using a computer or another device by disrupting its usual operation. A DOS attacks work by overwhelming or overloading a targeted system with requests until it can no longer handle regular traffic, causing other users to experience a denial of service.

2. 1 The Most Popular Kinds of DOS Attacks are:

- UPD flood attack: The target system is attacked by transmitting UDP (User Datagram Protocol) packets to a particular or arbitrary port on a casual port.

- An ICMP flood attack: the victim receives a large volume of ICMP (Internet Control Message Protocol) rebound demands (i.e., ping flood) packets for spoofed source IP address.

- A Smurf attack: The ICMP packets are redirected to these boosters with a fake source IP address, leading to a reflection or amplification attack on the routers and servers. The faked address will be the IP address of the victim's system. The sources of UDP and ICMP flood attacks are easy to detect, but the sources of Smurf attacks are more challenging.

- Hypertext Transfer Protocol(HTTP) flood: HTTP queries overwhelm the web server. It is a volumetric attack that has nothing to do with reflection or spoofing.

- Land Attack: is a high number of packets with the same host, IP, and port for the destination provided, causing the system to stop.

- A TCP SYN attack: This attack uses a flaw in the Transmission Control Protocol (TCP)[3].

3. Ensemble Learning Technique

Ensemble learning enhances machine learning outcomes by including many models. This strategy outperforms the single models in terms of prediction accuracy. Two types of ensemble learning are recognized: A multi-classifier system has been classified as both a homogeneous and heterogeneous ensemble when it contains different types of learners. The most widely used ensemble methods include:

- The bagging, or bootstrap aggregation method, was one of the earliest ensemble algorithms, and it is one of the simplest ways to increase efficiency. Bagging is a way to attain a range of outcomes using bootstrapped backups of the learning algorithm. A distinct classification model of the same category was modeled using a fraction of the training data. The popular vote on their selections enables the fusion of specific classifiers[4].

- Through boosting, Schapire proved that a weak learner, which develops classifiers capable of correctly categorizing all but a tiny proportion of examples, can transform into a strong learner who constructs classifiers capable of marginally outperforming random guessing. Boosting, like bagging, creates an ensemble of classifiers by resampling the data and combining the results using a majority vote [4].

- Stacking: some occurrences are close to the decision border and, as a result, are frequently positioned on the wrong side of the classifier-determined boundary; they are particularly likely to be misclassified. On the other hand, some cases are more likely to be correctly classified since they are on the right side and are a distance from the critical judgment limits [4].

4. Method of Selected Related Work

This study gathered related papers for the actual subject from four databases: Science Direct (SD), IEEE Explore, Scopus, and Web of Science (WOS), while conducting meta-analyses and systematic reviews by employing sufficient details[5]. The first database (SD) includes credible scientific, engineering, and technology references. The second database (IEEE) contains every scientific and technical literature in computer science, electrical engineering, and electronics engineering. The third is Scopus, founded in 2004 by Elsevier as an abstract and citation database. Fourth, Web of Science is a subscription-based service that allows users to access many databases, including precise citation data for various academic fields.

5. LITERATURE REVIEW

Despite the availability of a wide range of traditional detection systems, DDoS attacks continue to grow in frequency, volume, and intensity.

Meitei et al. (2016), the author explains that the Domain Name System (DNS) is a major factor. Since it transforms domain names into IP addresses, UDP (User Datagram Protocol) can be used for DNS, searches, and replies. DNS amplification attacks are a constant danger to DNS name servers. A method is described in this study to discover such attacks originating from infected devices. They evaluated DNS traffic streams utilizing machine-learning classification techniques such as DS, MLP, NB, and SVM to identify regular and irregular DNS traffic. This method uses attribute selection techniques, including Information Gain, Gain Ratio, and Chi-Square, to get the best feature subset [6].

Reneilson Santos et al. (2018). This paper examines the subject and recommends categorizing DDoS attacks using learning algorithms (DT, SVM, and RF) in a software-defined network simulated environment. With this in mind, DDoS attacks were simulated using the Scapy tool and a list of valid IPs, with the Random Forest method producing the best accuracy and the Decision Tree method yielding the fastest processing time [7].

Al-Naymat et al. (2018). This study uses the Management Information Base (MIB), a database linked to the Simple Network Management Protocol (SNMP), to suggest an effective methodology for network attack detection and classification. This study also looks into the impact of SNMP-MIB information on outlier detection. Three classifiers are used to create the detection model Random Forest, AdaboostM1, and MLP. A method has provided a way of detecting network attacks based on SNMP-MIB data using the machine-learning algorithms in this research. The objective was to prove the ability and efficacy of SNMP-MIB data in detecting network irregularities by showing the identities of the most common and current attacks that can occur on the interface layer [8].

Rui-Hong Dong et al. (2018) stated that the challenge is that the size of the traffic data that needs to be processed in the Wireless sensor network (WSN) intrusion detection technique is too huge. Resulting in high computational complexity of the intrusion detection model and poor intrusion detection performance [9].

Naveen Bindraa et al. (2019) published using the most recent comprehensive dataset to train their machine-learning-based classifiers. This research aims to see how effective machine learning categorizes network traffic. The results are encouraging, and they've set us on a path to improve performance and accuracy by utilizing efficient dataset preparation techniques. Their research emphasizes the need for an effective DDoS detection mechanism to protect networks. Their study is more relevant because it examines the use of supervised learning algorithms on a dataset that incorporates a stream of simulated DDoS attacks [10].

Alsirhani et al. (2019) presented a dynamic DDoS attack detection system in this article, which comprises three essential parts: a distributed system, classification methods, and a fuzzy logic system. Their solution uses fuzzy logic to dynamically select a method for detecting various DDoS attack Patterns from a list of pre-prepared classification methods. NB, (entropy), DT (Gini), and RF have been chosen as candidate classification methods of the several available approaches. They assessed the performance of the classification techniques and their delays in verifying the fuzzy logic system. They also looked at how well the system affected the classification algorithm latency. This study presents a technique for detecting dynamic DDoS attacks that incorporates three ideas: distributed classification algorithms, a fuzzy logic system in charge, distributed classification algorithms run in a distributed system, and distributed classification algorithms controlled by a fuzzy logic system [11].

Saikat et al. (2019) used ml to construct their IDS, which has undoubtedly been the key impetus behind numerous recent Artificial Intelligence (AI) victories. However, most of these approaches have been centered on learning a single interference model. However, because so many different types of interference exist, it may be difficult to identify a single model that applies to all of them. Finally, their primary concept is to train many intrusion detection models before combining them into a single system [12].

SkhumbuzoZwane et al. (2019) were offered a flow-based intrusion detection technique for intrusion detection that utilizes an ensemble machine-learning model. The suggested ensemble learning IDS performance has been assessed using the state-of-the-art CIDDS-001 flow-based NIDS testing datasets and SDN-based distribution architecture. In a wireless SDN context, the planned FIDS was installed and assessed [13].

Wani et al. (2019) conducted their cloud environment research using Tor Hammer as an attack tool. IDS is used to create new information. Various machine learning methods are used in this project, such as (SVM), (NB), and (RF), which are three classification algorithms that may be used to identify DDOS on the cloud. SVM and NB had an overall accuracy of 99.7% and 97.6%, respectively [14].

Gopal Singh Kushwah et al. (2020) published their findings. In this study, they have proposed a method for detecting DDOS traffic using net flow feature selection and machine learning. To begin with, they used real-time net flow sampling to extract adaptive flow-and pattern-based features. They then created a detector using Random Forest. They tested it on a network trace in a research facility that included benign traffic and simulated DDOS traffic of various types generated by typical DDOS tools. According to test results, their system has an average false-positive rate of less than 1% and a 99 % accuracy rate. Furthermore, their solution is universal for previous DDOS methods because it validates DDOS types such as sneaky attacks. Finally, they test their detector on real-world net flow logs that a large ISP has provided to determine DDOS features [15].

Alamri et al.(2020) described the LR-DDOS attacks on software-defined networks that can be identified and prevented using a scalable modular system environment in this work. They used machine learning strategies like RF, J48, REP Tree, and MLP. In the Canadian Institute of Cybersecurity (CIC), the DoS dataset was used for their design training and testing (IDS). Despite the challenges of detecting LR-DOS

attacks, the evaluation results revealed that our technique has a 95 percent detection rate. ONOS (the open network operating system manager) was used on a Minivet virtual server to imitate production networks as closely as feasible [16].

Gargi Kadam et al. 2020. The researchers demonstrated a network intrusion detection system customized to identify these attempts. The major goal is to identify the sorts above of attacks with the least amount of ambiguity possible and to limit the number of false positives to improve detection reliability. Initially training it on the KDDCup99 and ISTS datasets, then refining it by testing it on real-time data gathered by TCP Dump. A feature selection and classification model has been built utilizing data mining combined with deep learning and machine learning techniques. Real-time information was acquired using an ISTS dataset, first labeled using unsupervised machine-learning algorithms, then compared to the records in the KDDCup99 dataset [17]

Kumar et al. (2020) examined the many DDoS attacks that may be launched against an SDN controller and the key characteristics that indicate unexpected traffic. Machine-learning techniques are also utilized to distinguish between legal and malicious communications. The model that has been created by combining these techniques aided in the identification of DDoS attacks in real-time [18].

S. Shanmuga Priya et al.(2020) incorporated machine learning to build an automated DDoS detector that can be executed on any com DDoS attacks, including ICMP floods, TCP floods, UDP floods, etc. Their proposals identified various machine-learning algorithms, such as SVM, NB, RF, and KNN. The reason for adopting these three algorithms is that they require fewer characteristics and a smaller amount of training data to execute the detection process than other machine-learning algorithms. Compared to other machine-learning algorithms, they require fewer characteristics and a smaller amount of training data to complete the detection process [19].

Eduardo A. Sousa et al. (2021) looked at how the Ethereum network responds to a DOS attack. They have examined the Under-priced DOS Attack [4], in which attackers take advantage of the Ethereum fee structure by paying a tiny cost for many low-value transactions. Then, using publicly accessible transaction information, they provide a collection of machine learning techniques. They have been used to detect this attack according to genuine traces; they analyzed the solution by simulating the *Ethereum* network. According to their findings, an underprized DOS attack can increase the average pending time of a transaction by more than 42 percent. Furthermore, the proposed usage of the machine-learning approaches yielded respectable results [20].

Tayfour et al. (2021) have explained the identification and prevention of DDoS in the SDNs. Three parts comprise the proposed technique: a classifier, a mitigation module, and a collaboration module. V-NKDE, an ensemble classifier, is capable of reliably identifying DDoS attacks. The mitigation module keeps malicious traffic out of the switching flow entry and removes harmful traffic. Using Redis Simple Message Queue technology, the collaborating element distributes DDoS detection and mitigation rules across many SDN controllers. The developed classifier was tested on the datasets InSDN2020, CICIDS2017, UNSW-NB15, and NSL-KDD [21].

Pushpa Iyer et al. (2021) This paper addresses the use of ML algorithms for anomaly detection on a computer network to determine whether the traffic is normal, contains any anomalies, or is an attack. This essay critically analyzes IDS technology and the difficulties encountered during implementation. Several ML approaches, including DT, RF, NB, K-NN Classifier, and other DL models, including CNN and ANN models, are used to automate the task of identifying the intrusion [22].

Some articles used only the ml algorithms such as SVM, DT, or K-NN. Others used ensemble-learning methods homogenous like (bagging and boosting) or heterogenous like (stacking) for detecting different dos, either bandwidth like (flooding and amplification) or resources such as (malformed packet and protocol) attacks and compared the results, as shown in figure 2

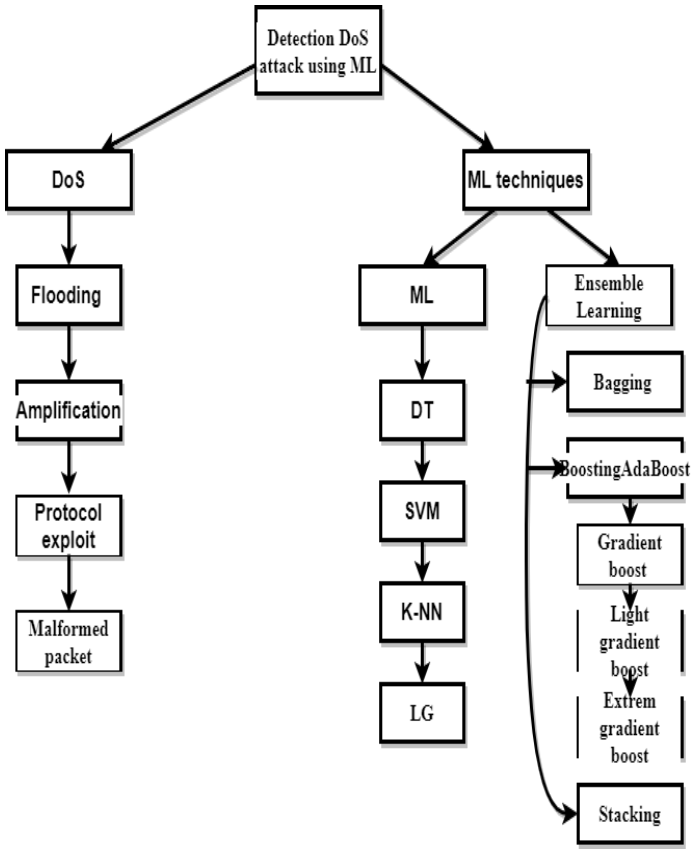

Fig.2 Research taxonomy of using ensemble learning to detect DOS attacks

Table 1 shows the important information in several articles about the types of attacks in different dataset targets to use several categorization techniques to detect different forms of DOS attacks. Like SVM, DT, K-NN, and bootstrap, stacking and boosting are examples of ensemble learning. The results showed that ensemble learning improves detection accuracy more than the single method and evaluates the performance of these methods using confusion matrix measurement, especially the accuracy. Most results showed that the accuracy of detection attacks for single algorithms is less than that of the hybrid methods. The vacuole can be in research because most authors did not use many features to detect the attacks with high accuracy or only used two machines learning without comparisons with more methods to get the best ones.

Table1. Characteristics of Research in the Literature

NO.	DOS type	Algorithms	Dataset	Accuracy& time detection in second
[6]	DDoS	DT. SVM, MLP,NB	Simple Web, CAIDA	99% DT
[8]	DoS flooding attack	RF, Ada Boost, MLP	Management Information Base (MIB)	99% RF
[9]	Probe, U2R, R2L, DoS	NB ,ANN, boosting	NSL-KDD	80% ,Boosting- C5.0 7.1 s
[10]	Botnet-based DDoS	SVM ,Gaussian NB(GNB), K-NN, RF	CICIDS 2017	96 % RF
[11]	DDoS	RF, NB, DT	CAIDA	95% DT
[12]	DDoS	MLP,SMO SVM, IBK KNN, J48	NSL-KDD	97% J48
[13]	DDoS	Ada Boost, DT	CIDDS-001	99% Ada Boost
[14]	ICMP, TCP downfall, UDP downfall	SVM, NB, RF	N/A	98%, NB
[15]	DDOS	RF, SVM, C4.5, Ad boost	ISCX & NSL-KDD	Ada boost & RF 98% AdaBoost 3.1 s RF 7.7s
[16]	DDoS	RT, J48, SVM, REP Tree RF	A Canadian Institute of DOS for Cybersecurity (CIC)	RF 94%
[17]	U2R, R2L	KNN,ANN, RF	KDDCup99	99% RF
[18]	DDoS	KNN,MLP, SVM	SDN environment	99% MLP,KNN, 12s
[19]	DDoS	KNN, linear kernel (LK-SVM) ,RF	SIOTLAB and UNSW datasets	LK-SVM98% 0.00118 s
[20]	DoS	DT, RF	N/A	95%RF
[21]	DoS	DT,RF,ANN, CNN	CICIDS2017, NSL-KDD ,UNSW-NB15	99%DT, 8.3 s

5. challenge and Motivation

The challenges and motivations to discover with high accuracy and low error rate denial of service attack that seeks to deny services and prevent users from accessing network traffic as shown in table 2:

Table.2 Challenge and Motivation

Challenge	Motivation
Packet-based IDS (PIDS) is a form of DS that utilizes deep packet inspection to discover threats in network traffic. Deep packet inspection checks the entire packet payload, which might be challenging if the packets are encrypted.	They can see that ensemble-based classifiers have a higher AUC than single learner classifiers, and an adaptive boost has an accuracy of 0.99 percent.
inguishing regular users from cyber criminals becomes extremely difficult. Moreover, as technology progresses, so do the methods for launching DoS attacks. Because there are numerous forms of DoS attack techniques, identifying the DoS attack gets more difficult. DoS attacks include ICMP floods, SYN floods, and IP packet floods.	ne systems may demand many features compared to earlier systems, while others may require a high number of criteria to identify DDoS. Contrarily, our suggested method addresses these problems by identifying DDoS in any form without requiring a distinct protocol with fewer features.
ckers modify their attack tools and techniques that have evolved with time. Defenders are constructing new IDS to deal with attackers' novel approaches and enhance detection accuracy; strong defense methods, approaches, and procedures have been developed. (Improve accuracy and reduce the number of false positives.).	must constantly react to counteract these attackers' novel DDoS attack strategies and patterns. They proposed a NIDS in this article that can identify both existing and novel forms of DDoS attacks. Their NIDS's main feature is that it uses ensemble models to combine numerous classifiers with the idea that each classifier will focus on a different part of the intrusion problem, resulting in a more powerful coping strategy against future intrusions.
Because of its technological limitations, the central server cannot handle a significant volume of data in a short period, such as massive Internet traffic. They must monitor a vast amount of Internet traffic during a DDoS attack, which is impossible for a single server to handle. Some monitoring methods use packet selection to limit the amount of data input. However, this produces inaccurate results.	the volume of Internet traffic grows, solutions for monitoring a network in the classic sense based on a single workstation are no longer adequate. Current methods use large data frameworks to speed up processing, but they are mostly geared for offline data analysis. Spark Streaming has been used in this work to develop a machine-learning-based online DDoS attack detection system.
DDoS attacks are identified and prevented.	machine learning techniques, an effort has been made to evaluate such attacks and extract attributes that might uniquely differentiate them from attack communications. Finally, a real-time controller module for the Open Network Operating System (ONOS) was created to recognize an ongoing DDoS attack.
Despite the impact on crypto-currency systems, scholarly research examining attacks on such platforms is still lacking.	ereum is a well-known cryptocurrency with a market value of more than $20 billion as of April 2020. Its service allows smart contracts to be executed. Because of its extensive features, Ethereum is more vulnerable to many threats and attacks. One of the most serious threats to crypto-currency systems is a DoS attack.
Despite the difficulty of dealing with all types of denial of service attacks, DDoS attack mitigation and denial of service (DoS) attack Low-Rate DDoS (LR-DDoS) attacks are notoriously hard to expose, especially in software-defined networks (SDN).	practice, it's difficult to install effective LR-DDoS attack mitigation methods. Existing methods, for example, could include updating the router's firmware, which, in some cases, isn't possible. Given the growing prevalence of software-defined networks (SDNs) [9], LR-DDoS attacks have been documented against them.
With the increased use of wired and wireless networks, As the Internet has grown in popularity, so has the number of security breaches and hostile attacks. Therefore, the problem is detecting these attacks with high precision using machine-learning methods.	DOS flooding attack is one of the most common attacks that affect networks. DoS attacks have recently become the most tempting type for attackers, putting network services at risk. As a result, dependable network intrusion detection solutions are necessary.
A DNS amplification attack is one of the most serious risks to the DNS server. As a result, it is vital to take appropriate precautions to identify such an attack.	S amplification attacks are a continuous danger to DNS. One of the most common (DDoS) attacks is DNS amplification.
Multiple scientific	oS methods are difficult to evaluate and apply because of various

questions have prompted this survey. 1) Which supervised echnique will produce etter results in DDOS ttack detection? 2) How effective would these algorithms be if they were trained on a data set?	variables, including the complexity, rigidity, expense, and vendor-specific design of contemporary networking equipment and protocols. Machine Learning (ML) models are being used to identify DDoS attacks. However, the question of which machine learning model is the best among the alternatives remains unsolved. Different data pre-processing strategies can be used to evaluate all machine-learning models.
The task There is much data for Network Intrusion Detection Systems (NIDS) to look over to detect new intrusions that are not typical. A huge amount of data reduces the training rate, interferes with testing, and has a negative impact.	With the rise in internet traffic, designing effective network intrusion detection systems (NIDS) that can notice existing attack patterns and detect new threats is more crucial than ever. NIDS keeps an eye on the internet traffic for harmful activities such as denial-of-service attacks, unwanted network access, attempts to obtain further privileges, and port scans.
In more extreme cases, hackers have access to sensitive government data, resulting in invasions of privacy. A resistant system is necessary to deal with such issues by implementing ways that limit the amount of harm that the problem causes.	ead of a local delete rule, the attack should have a network-wide delete rule. Using machine-learning algorithms has many advantages within an SDN
DDoS attacks have evolved to the point where they may bypass detection systems, making static solutions impossible to detect.	current study has several difficulties, including detection systems, efficiency, ability to identify DDoS attacks, detection costs, and the ability to handle large amounts of data. These are all factors to consider. A novel technique is required to dynamically recognize DDoS attacks, manage dynamic DDoS attack patterns, and efficiently process enormous amounts of data.

6. Conclusion

Because of the internet's explosive growth and the evolving complexity of communication protocols, computer system security is complicated. Network hacking has become more resource-damaging in recent years because network hackers now aim to restrict users from accessing network resources. As a result of its significance in cyber security, DoS detection has recently become a popular research area. DoS attack packets were viewed by them as a stream of data as well. Computer safety system ID, or IDS, protects computers against cyber-attacks. In this study, the research activities were broken down and represented by a general process model. Since the primary areas of research for increasing the detection rate in IDS are in these stages, new researchers should concentrate on the pre-processing and model core components depicted in our generic process flow. Pre-processing is crucial because it directly influences how accurate classifiers are. Pre-processing combined with detection rates are among the highest. The strength of the ensemble is often much greater than that of the base learners. Because it can make marginally better predictions than random guesses from weak forecasters into strong predictors, ensemble learning is intriguing. Single learners are therefore also referred to as weak learners. The most current results show that the outcome of the hybrid strategy is superior to the most accurate detection attack for single algorithms. The majority of authors, the research claims, did not use a substantial number of features to accurately identify assaults or only used two machine-learning approaches to find the best answers without weighing them against alternative solutions. That employing the ensemble stacking method to address issues with credit card theft and cyberattacks has enormous promise and could be improved by experimenting with various base model combinations and the number of folds in the model. Therefore conclude that ensemble methods were more accurate than single techniques at detecting DoS attacks. Although it takes longer to employ algorithms on huge data sets, doing so is preferable when just using a small amount of data is available.

Reference

[1] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, 2018, doi: 10.1016/j.jocs.2017.03.006.

[2] N. Bindra and M. Sood, "Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset," *Autom. Control Comput. Sci.*, vol. 53, no. 5, pp. 419–428, 2019, doi: 10.3103/S0146411619050043.

[3] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Comput. Secur.*, vol. 88, p. 101645, 2020, doi: 10.1016/j.cose.2019.101645.

[4] A. A. Aburomman and M. B. I. Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers," *Comput. Secur.*, vol. 65, pp. 135–152, 2017, doi: https://doi.org/10.1016/j.cose.2016.11.004.

[5] D. Moher, "Corrigendum to: Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. International Journal of Surgery

2010;8:336-341," *Int. J. Surg.*, vol. 8, no. 8, p. 658, 2010, doi: 10.1016/j.ijsu.2010.07.299.

[6] I. L. Meitei, K. J. Singh, and T. De, "Detection of DDoS DNS amplification attack using classification algorithm," in *ACM International Conference Proceeding Series*, 2016, vol. 25-26-Augu, doi: 10.1145/2980258.2980431.

[7] R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, "Machine learning algorithms to detect DDoS attacks in SDN," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 16, pp. 1–14, 2020, doi: 10.1002/cpe.5402.

[8] G. Al-Naymat, M. Al-Kasassbeh, and E. Al-Hawari, "Exploiting snmp-mib data to detect network anomalies using machine learning techniques," *Adv. Intell. Syst. Comput.*, vol. 869, pp. 991–1004, 2018, doi: 10.1007/978-3-030-01057-7_73.

[9] S. Liu, L. Wang, J. Qin, Y. Guo, and H. Zuo, "An intrusion detection model based on IPSO-SVM algorithm in wireless sensor network," *J. Internet Technol.*, vol. 19, no. 7, pp. 2125–2134, 2018, doi: 10.3966/160792642018121907015.

[10] N. Bindra and M. Sood, "Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset," *Autom. Control Comput. Sci.*, vol. 53, no. 5, pp. 419–428, 2019, doi: 10.3103/S0146411619050043.

[11] A. Alsirhani, S. Sampalli, and P. Bodorik, "DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 3, pp. 936–949, 2019, doi: 10.1109/TNSM.2019.2929425.

[12] S. Das, A. M. Mahfouz, D. Venugopal, and S. Shiva, "DDoS Intrusion Detection Through Machine Learning Ensemble," *Proc. - Companion 19th IEEE Int. Conf. Softw. Qual. Reliab. Secur. QRS-C 2019*, pp. 471–477, 2019, doi: 10.1109/QRS-C.2019.00090.

[13] S. Zwane, P. Tarwireyi, and M. Adigun, "Ensemble Learning for Flow-Based Intrusion Detection in SDN," *South. Africa Telecommun. Networks Appl. Conf.*, no. November, 2019.

[14] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Feb. 2019, pp. 870–875, doi: 10.1109/AICAI.2019.8701238.

[15] G. S. Kushwah and V. Ranga, "Voting extreme learning machine based distributed denial of service attack detection in cloud computing," *J. Inf. Secur. Appl.*, vol. 53, p. 102532, 2020, doi: https://doi.org/10.1016/j.jisa.2020.102532.

[16] H. A. Alamri and V. Thayananthan, "Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Protecting Software-Defined Networks Against DDoS Attacks," *IEEE Access*, vol. 8, pp. 194269–194288, 2020, doi: 10.1109/ACCESS.2020.3033942.

[17] G. Kadam, S. Parekh, P. Agnihotri, D. Ambawade, and P. Bhavathankar, "An Approach to Reduce Uncertainty Problem in Network Intrusion Detection Systems," in *2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS)*, Nov. 2020, pp. 586–590, doi: 10.1109/ICIIS51140.2020.9342634.

[18] C. Kumar *et al.*, "Intelligent DDoS Detection System in Software-Defined Networking (SDN)," in *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, Jul. 2020, pp. 1–6, doi: 10.1109/CONECCT50063.2020.9198312.

[19] H. Gordon, C. Batula, B. Tushir, B. Dezfouli, and Y. Liu, "Securing Smart Homes via Software-Defined Networking and Low-Cost Traffic Classification," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, Jul. 2021, pp. 1049–1057, doi: 10.1109/COMPSAC51774.2021.00143.

[20] J. Eduardo A. Sousa *et al.*, "Fighting Under-price DoS Attack in Ethereum with Machine Learning Techniques," *Perform. Eval. Rev.*, vol. 48, no. 4, pp. 24–27, 2021, doi: 10.1145/3466826.3466835.

[21] O. E. Tayfour and M. N. Marsono, "Collaborative detection and mitigation of DDoS in software-defined networks," *J. Supercomput.*, vol. 77, no. 11, pp. 13166–13190, 2021, doi: 10.1007/s11227-021-03782-9.

[22] P. Iyer, T. Jadhav, A. Pillai, and Samundiswary, "Analysis of Modern Intrusion Detection Algorithms and Developing a Smart IDS," in *2021 International Conference on Intelligent Technologies (CONIT)*, Jun. 2021, pp. 1–7, doi: 10.1109/CONIT51480.2021.9498519.