Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549741

IMPROVED HEURISTIC FRAMEWORK FOR CYBER SECURITY SYSTEM ON DDOS ATTACK

Rinky Ahuja

(SET, Sushant University)

Meenakshi Gupta

(SET, Sushant University)

Abstract:
Nowadays, networks have adopted the always-connected concept and as time goes on, technology makes gadgets smaller and cheaper. This revolution lays the foundations for the next Internet iteration by enabling straightforward two-way communication between devices. The term "Internet of Things" (IoT) describes the emerging paradigm of the next generation of the web. Infrared sensors, laser scanners, gas indicators, RFIDs, and GPS systems are just a few examples of the many information-sensing objects and services that make up the IoT, which allows them to exchange data and coordinate their operations. Furthermore, with the recent developments in IP addressing methods and the decreasing cost of micro-controllers and CPU power, several devices and gadgets now have robust Internet connectivity.As a result, over 20 billion Internet-enabled gadgets are anticipated to increase over the next several years.

I. Introduction:

Meanwhile, the IoT isn't only for mundane uses around the home. Instead, its uses are broad and varied, including fields disparate as agriculture and industry. Manufacturers and IoT providers are rushing to get their products to market as demand for this kind of technology soars, putting users' privacy and safety at risk. Many IoT devices have security issues due to this behaviour at various implementation levels. For example, one of the largest distributed denial of service (DDoS) assaults in Internet history was initiated by the Miraibot because of weak security measures in these gadgets. The target network device's ability to function may be severely hampered by a distributed denial of service (DDoS) assault, resulting in lost revenue, data, and even increased danger to human life. While this may seem like an excessive solution in search of a problem,it is conceivable to halt the healthcare IoT system if an attack were to be started against hospitals and healthcare organizations. Message tampering, eavesdropping, and even more complex assaults like Sybil and node cloning are all possible against IoT devices and networks. And it doesn't even account for the many security holes that have persisted in the original Internet architecture. The IoT is a network with constrained resources that makes it difficult to provide the same level of security used in more traditional networks. Because of the complex and varied nature of IoT networks and the inherent restrictions and constraints of the devices themselves, a new security model is required to adequately handle security issues at all levels of the IoT paradigm. While there are undoubtedly many security difficulties and challenges, addressing concerns about trust, privacy, confidentiality, and integrity is a necessary first step in constructing a safe and resilient IoT

ecosystem. This study**Improved heuristic framework (IHF)**to clarify some of these issues, characterize known attacks that compromise network availability, and investigate existing defenses against these threats.

2. Literature Study

Yusof, A. R. A. et al. [1] expressed detrimental impacts of DDoS attacks on organizations' assets have made them a hot topic in the computer security realm. They are provided with a description of DDoS, classifications of DDoS assaults, an overview of existing DDoS detection technologies, and strategies for forecasting DDoS attacks, as well as a detailed comprehensive review of the literature and quantitative analysis of the impact of DDoS.

Shen, Y. et al [2]deliberated the impact of DoS assaults on the ability to regulate the frequency of power use in a single geographic region. As a result, the closed-loop power system model for a single region was developed first with lag in the routes of communication taken into consideration. Second, the power system's load frequency management scheme benefits from incorporating an event-triggering control mechanism, which optimizes channels used for control error transmission in a geographically dispersed setting.

Hypertext Transfer Protocol (HTTP) web servers are vulnerable to denial-of-service assaults described by Jaafar, G. A. et al. [3]. DDOS assaults, a more advanced form of this technique, are among the most hazardous types of cyberattacks because of their potential to slow down or even bring down a website's server.A table-based overview of each detection approach and detailed critical analysis are provided to aid in designing future studies devoted to HTTP DDoS assault detection.

This research gives a comprehensive taxonomy of cloud-based DDoS attack methods and an in-depth explanation of how these attacks might be defined, identified, and countered by Agrawal, N., &Tapaswi, S. [4]. In addition, this article examines the key performance indicators that should be used when comparing security systems and their behaviour in the cloud. This survey report was written to inspire cloud security experts to develop novel and efficient methods of protecting networks against DDoS assaults.

In this study, they are conducting a literature review on CPS security. We begin by discussing some current cyber threat detection technologies illustrated by Mahmoud, M. S. et al. [5]. DoS, deception, and replay assaults are the primary areas of attention here. They have reviewed existing models of these assaults and methods for filtering and controlling CPS that are vulnerable to them.

An Optimal Approach to Protecting Software-Defined Networks from DoS Attacks explained by Imran, M. et al. [6].Using Software Defined Networking (SDN), switches are rendered ineffective and only responsible for passing data. In addition,it will identify potential flaws in these mitigation strategies and provide the characteristics of a best-case scenario for protecting against DDoS assaults. This paper was the first effort they are aware of to categorize DoS mitigation techniques and identify their limitations in an SDN setting.

This paper [7] offered a comprehensive review of the literature on DDoS attacks against SDN. The security aspects of SDN are discussed once they have been analyzed from a security standpoint. In the first perspective, SDN improved traditional networks' safety. However, another point of view is that the centralized nature of SDN's control mechanism makes it vulnerable to attack.

Cybersecurity Threats, Attacks, and Countermeasures in IoT-Based Smart Homes examined the Abdullah, T. A. et al. [8]. This study examined previous research on smart house design, potential dangers, and security measures. This study offered some current architectural suggestions for the smart home setting. Moreover, the most typical dangers and weaknesses in smart homes were examined. This article concluded bydiscussing the best user practices and solutions for smart home setups.

An analysis of the literature on cyberattacks from the point of view of command and controlwas demonstrated by Sánchez, H. S. et al. [9]. This research gives a bibliographical overview of cyber assaults in networked control systems (NCSs) and cyber-physical systems (CPSs), including definitions, classifications, and applications. This analysis approaches the subject from a control-centric vantage point, complementing informational and communicative approaches. This paper first explains why novel methods of attack detection and secure control are necessary before going into detail about those methods, including the goals of attacks, how attacks are modelled, the definitions of specific attacks and threats, and the methods employed to identify them.

Risk management framework (RMF) for the Protection of Personal Information in Cyber-Physical Systems expressed by Chong, M. S. et al. [10]. The authors suggest beginning the process of designing safe and resilient CPS with a thorough risk analysis that identifies the most relevant attack scenarios. It happens because many common methods of reducing security risk are susceptible to modifications in the attacker or defender models. For example, although certain techniques can ensure security against assaults affecting up to half of the sensors, this may not be the case when the attacker controls more than half of the sensors.

Vishwakarma, R., & Jain, A. K. [11] discussed the DDoS assault on an IoT network attempts to compromise the availability of servers by overwhelming it with bogus requests from compromised endpoints.This article explores 'Distributed' DoS in the IoT and malware and botnets' role in its creation and execution. Furthermore, they explain and evaluate the different DDoS defence strategies to highlight each security hole.

Nooribakhsh, M., &Mollamotalebi, M. [12] demonstrated techniques for identifying DDoS assaults based on statistical abnormalities in received packets were the primary emphasis of this article. To identify suspicious activity, anomaly detection systems must establish a baseline profile of acceptable network traffic behaviour.This study's findings suggest that statistical techniques have emerged as one of the most effective strategies for analyzing network traffic to identify outliers in data packets.

Internet services continue to expand and improve. One of the most dependable and sturdy options is software-defined networking.This study thoroughly analyzes the benefits of SDN's layered architecture in the fight against DDoS assaults and its flaws that might open the door to novel DDoS attacksexpressed by Singh, J., &Behal, S [13].To design a decentralized DDoS detection and mitigation framework using a metric based on generalized information theory to cut down on the need for a central controller inside an SDN.

Load frequency control system (LFCS) for Cybersecurity in Power System Load RegulationMohan, A. M. et al. [14]. Moreover, the instability of the whole network is threatened by the frequency variation caused by load shift or cyber assault in one region,which impacts all other related areas. As a result, researchers continue their work in frequency

regulation and cyber security. In this study, they provide a thorough analysis of the LFC mechanism's cyber-security in the context of the power grid. A few of the paper's more notable features include its examination of attack techniques, its formulation of several attack models, and its short analysis of current detection and protection systems against cyber-attacks on the LFC system, all vulnerable to assault.

New network node authentication module (NNNAM) and naïve Bayes classifier module (NBCM) for identifying and isolating the traffic patterns of a DDoS assault expressed by Reddy, K. G., &Thilagam, P. S. [15].To evaluate the efficacy of the network, they simulated a DDoS assault, a non-attack, and a DDoS attack using the suggested technique in NS2. Our simulations show that our suggested method reduces the impact of DDoS assaults and that network nodes handle 80% of legal traffic. In contrast, network nodes handle zero percentageof valid traffic when our method is risky.

This paper proposes taxonomy to define and discuss methods of defending against DDoS assaults using SDN in IoT settings.The proposed taxonomy takes into account four (4) crucial aspects of the prevention process, including (i) whether or not the solutions carry out the method conveniently or collaboratively, (ii) whether additional technologies were utilized in conjunction with SDN to execute the process, (iii) the strategy to prevention employed, and (iv) the targeted connected device circumstance. Malicious flow filtering systems supported by machine learning algorithms have shown promise in mitigating DDoS assaults over a wide range of traffic densities.

Machine Learning (ML)based Intrusion Detection Systems (IDS) for single and multi-classifier systems for detecting DoS and DDoS assaults using ICMPv6 illustrated by Tayyab, M et al. [17].Additionally, the use of blockchain technology in CIDS architecture built around One of the major challenges for identifying DoS and DDoS attacks centred around ICMPv6 has been given as a solution using the integrated architecture. The study also categorizes ICMPv6's susceptibility to DoS and DDoS attacks, providing researchers with a useful tool.

Layer-wise assaults and attack taxonomy are two vantage points from which the study analyzes security attacks in depth, examined by Alferidah, D. K., &Jhanjhi, N. Z. [18]. In addition, it provides an in-depth examination of the assaults in terms of the IoT layers and the attack taxonomy. Finally, it details possible approaches and fixes for protecting IoT infrastructure from intrusion. This research aggregates data to provide a detailed picture of the problems and dangers facing the IoT'ssecurity. Furthermore, it may provide light on the precautions that must be taken to secure IoT devices and prevent attacks on these kinds of networks.

This article introduces the software-defined-network (SDN) paradigm by demonstrating the significance of SDN characteristics in SDN controller-based network management, monitoring, and programming examined by Aladaileh, M. A. et al. [19].In addition, this article is the first to categorize current DDoS attack detection methods according to methodology and characteristics employed threshold type, and deployment location in the SDN setting.

The physical protection of people driving and the effectiveness of transport providers are directly dependent on cybersecurity in intelligent transportation systems (ITS) explored by Mecheva, T., &Kakanakov, N. [20]. Most security metHowever, most concentrate on one of four l. This article discusses the need to modify several tried-and-true approaches such as network segmentation and encryption, for ITS cybersecurity.

This article by Kuzlu M. et al. [21] examined the common methods used to disrupt or breach the IoTand explained how these assaults work.As IoT systems become more pervasive, and especially as large-scale networks like smart cities begin experimenting with them, these kinds of attacks will become more commonplace for two reasons: (1) large-scale networks are more difficult to secure due to the sheer number of attacks surfaces they present, and (2) people's lives and safety depend on AI, which must be remarkably robust to be of any use at all.

To assess DOS-DDOS models for forecasting depending on the improved DOS-DDOS characteristics, the authors reviewed and analyzed the effect of various wrapping strategies, the total amount of DOS-DDOS capabilities, and numerous popular measures. [22]. This study provides three crucial dashboards for analyzing the effectiveness of three wrapper techniques often used in DOS-DDOS ML defences.Many preexisting ML solutions were greatly improved using Wrapper approaches, which enabled a better selection of important DOS-DDOS properties.

Comprehensive survey (CS) for detecting, mitigating, avoiding, or degrading gracefullyDDOS attacks in software-defined networks (SDN) explained by Eliyan, L. F., & Di Pietro, R. [23]. While packet forwarding and processing on a standard SDN network may take many orders of magnitude longer than the suggested technique, it only takes approximately 310 milliseconds.Finally, we cover potential safeguards and associated components against DoS/DDoS assaults in SDNs. The packet loss percentage is calculated assuming a 500 bps attack rate. Results showed that almost no packets were lost during the assault, proving the validity of the proposed strategy.

Distributed denial of service attack defence mechanisms (DDoSADM) has been proposed to identify, mitigate, and prevent DDoS assaults using SDN in programmable networks deliberated by Dalmazo, B. L. et al. [24].They consider the RFC7426 definition of SDN's layers—data, control, and application—in our literature study. They use a systematic approach to collect relevant literature and classify it into a taxonomy of DDoS defensive methods based on three criteria: degree of activity, location of deployment, and degree of collaboration.In particular, they see multilayered protection methods that can more fully manage DDoS assaults as a viable avenue of future development.

Quantum machine learning methods (QMLM) for detecting DDoS attacks through intrusion analyzed by Payares, E. D., & Martinez-Santos, J. C [25].In this study, we provide three quantum methods for detecting DDoS assaults. Quantum support vector machines, mixed quantum-classical neural networks, and a two-circuit ensemble strategy using two dynamic computational units are all tested for efficacy. As a result of our efforts, we have achieved performance levels very close to 100%, with a worst-case scenario of 96%. This illustrates that quantum models successfully support existing and future cybersecurity systems.

An anomaly-based intrusion detection system (A-IDS) for DDosBased on ICMPv6 expressed by Alghuraibawi, A. H. B. et al. [26].The proposed A-IDS uses a method for selecting features based on bio-inspired algorithms to generate an ideal solution that picks a subset to benefit the detection efficiency of an ICMPv6 DDoS assault. Anomaly detection strategies need to be modified to address the unknown ICPMv6-DDoS attack in conjunction with the limits linked to the use of other techniques. Furthermore, monitoring and observing the impact of ICPMv6-DDoS assaults on real-time systems may be accomplished via anomaly detection strategies.

Information theory-based detection approaches (IT-DA) for detecting DDoS assaults on SDN controllerswere examined by Aladaileh, M. A. et al. [27]. In addition, the purpose of this study is to demonstrate the originality of this work by providing a qualitative comparison between it with the current evaluations on DDoS attack detection methodologies utilizing a variety of metrics. Detailed discussion and comprehension of the gaps in the existing identification strategies; evaluation of the various IT-DA used to detect low-rate and high-rate DDoS assaults on the SDN controller; qualitative comparison of this paper with previous reviews about similar participants in terms of the information theory used and organizes the recognizing approach.

Systematic review method (SRM) for conducting an in-depth analysis of the current process by Alatawi, F [28].After reviewing the available literature, we classified the defence mechanisms into four categories: source-based, core-router, victim-based, and distributed. Comprehensively assessing the efficacy of these buffering mechanisms, a qualitative study was used. The efficiency of the defensive mechanisms was assessed based on six important factors, which were as follows: coverage, execution, deployment, precision of detection, reaction mechanism, and robustness. During the comparison examination, both the drawbacks and the advantages of each mechanism were discussed.

Systemic survey (SS) described the safety of autonomous cars against cyberattacksKim, K. et al. [29].Separated into three groups for identified autonomous assaults as those targeting the control system, the motoring system, and the vehicle-to-everything interactions. To counteract these threats, researchers separated them into three categories: security architecture, intrusion detection, and anomaly detection. With the proliferation of large data and advances in communication technology, artificial intelligence and machine learning-based methods for spotting anomalies are being created. In conclusion, they conclude our SS, arguing that AI and smart city components will be integral to future research on autonomous assaults and countermeasures.

Using Shield Techniques (ST), [30] provides a Methodological Review of the Application-Layer DDoS Attacks in a Mobile Ad Hoc Network.Since a DDOS attack may diminish an individual's online experience attack management is especially important in today's mobile computing environment. It was vital to distinguish DDoS attacks from comparable Events since they are initiated simultaneously with genuine requests.More specifically, this research investigatesDDoS attacks at the application layer and the many phases of their management, including prevention, detection, mitigation, and differentiation. Furthermore, it provides a comparative assessment of the most effective strategies revealed at each level.

An intrusion detection system (IDS) and deep learning model to identifyDDoS assaults obtained by Akgun, D. et al. [31].To this end, several models built on DNN, CNN, and LSTM have been tested and compared for their detection efficacy and speed of execution. The widely-known CIC-DDoS2019 dataset was utilized to evaluate the proposed model. They have preprocessed the CIC-DDoS2019 dataset by removing unnecessary features, picking features at random, eliminating duplicates, and standardizing the data. Consequently, both the training and test assessments of recognition performance improved.

Intruder and threat actions in the IoT were studied using an evolutionary sparse convolution network (ESCNN) [32]. Here, the stated intrusion detection system is processed using data from the DDoS Evaluation Dataset. The gathered information is segmented into an instruction

set, a set to be tested, and a set for validation. The data is trained using the various long-short term network layers, which results in more accurate attack detection. Test data classification is achieved using learned knowledge via feature extraction and sparse matrix creation. This approach improves attack detection reliability by decreasing the occurrence of false positives.
This study provides an alternative strategy for simulating and testing cyberattack scenarios using the DEVS modelling methodology and evaluating the outcomes [33]. Application created to generate acceptable intrusion detection system signals to mimic an attack situation in a virtual network and analyze detector alarms. As a simulation setting for development, DEVS-Suite was employed.
DDoS prediction system using a two-stage hybrid methodology with Deep Sparse Autoencoder and Light Gradient Boost Machine for DDoS e Attacks [34].Different learning models are fine-tuned to categorize assaults according to the retrieved feature sets. Finally, the gathered characteristics assess the models' efficiency under balanced and unbalanced conditions. The experimental findings show that the suggested model outperforms the conventional approaches.
Flow-Based Anomaly Detection Approach (F-BADA) With Feature Selection Method Used Against DDoS Attacks in SDNs [35]. The goals of this experiment, a modified Deep Learning model that was based on LSTM-Autoencoder, were employed; on the other hand, the DDoS assaults were regarded to be a case study. Our strategy results in a high detection rate and reduces the time required to construct the model, making it more efficient overall. We conducted further tests on the trained model's influence on the performance of the SDN controller to determine the extent to which the dataset used may affect that performance. The findings demonstrated that the strategy that was presented did not bring about a reduction in the performance of the network.
Novel Spark Streaming and Kafka-based distributed classification system (SSK-DDoS) to categorize the various kinds of DDoS assaults and legal network traffic [36]. To classify streams in real-time, Catalyst's streaming service employs a method that employs a distributed set of Catalyst MLlib machine learning algorithms on a collection of Hadoop nodes. The created SSK-DDoS categorisation approach proved accurate when tested using the most recent CICDoS2019 dataset.
Resilient eventtriggered (RET) logic-based security controller layout for nonlinear networked control systems (NCSs) for detecting DoS Attacks [37]. To simplify the management structure of the internet against DoS assaults and guarantee that the right packets get delivered to the control system even against non-periodic attacks, a brand-new security controller that involves the RET system and is not compatible with a membership capacity has been proposed. This helps to keep performance losses to a minimum. The benefits of the suggested method are then shown via simulated results.
In a distributed denial of service (DDoS) assault, many infected computers in various locations send a flood of traffic to one another to bring down the targeted computer [38]. Consequently, effectively and quickly identifying DDoS assaults remains a constant priority for the cybersecurity research community. This work will aid future researchers and academics in better understandingDDoS attacks.

This research provides a DDoS attack detection framework (DDoS- ADF) to effectively recognize DDoS attacks based on reflections and exploits [39].Using the J48 classifier, the framework is evaluated on the most recent DDoS evaluation dataset (CICDDoS2019). Maximum feature reduction using the feature reduction technique is 82.92%, with a minimum reduction of 56. The experimental findings favour the suggested framework above those obtained by employing a smaller collection of characteristics. Accuracy for binaries and multi-level classification utilizing decreasing features by 60.97 percentage is improved when the suggested framework is tested on the knowledge discovery and data mining KDD Cup 1999 dataset.

To investigate and construct machine learning models to identify DDoS assaults, the CICDDOS2019 dataset was utilized in this research [40].All ML algorithms were trained using these characteristics, and their accuracy was measured. This study compared the performance of several machine learning (ML) algorithms. It showed that, during the whole k-fold cross-verification stage, the decision trees and random forests fared the best.

Optimized Ensemble Framework (OEF) is described to detect the DDoS attack using big data in IoT [41].This research suggests a paradigm for spotting fraudulent data transfers across a network. The framework uses a Support Vector Machine (SVM) and a deep neural network model Convolutional Neural Network (CNN) embedded with a Gated Recurrent Unit (GRU), both tuned with a Slime Mould Algorithm (SMA) for improved accuracy of 98.45 and 94.84%, respectively, to detect malicious network traffic. Specificity, predicting time, instruction, and correctness are evaluated after applying the suggested method to the KDD dataset.

DDoS attack authentication using an asynchronous federated learning arbitration model (AF-bLAM) explained by Liu, Z. et al. [42]. The AsyncFL-bLAM suggests using a leader node election process to build. The suggested bLAM model comprising a feature extractor and an arbitrator has been assigned LDDoS detection on a regional level. In addition, the unique AsyncFL architecture allows the parameters of the bLAM models to be uploaded and aggregated asynchronously between the node in leadership and the customer nodes.

Ryu controller-based software-defined networks (RyuC-bSDN) to detect DDoSattacks using extracting features and classifying themChouhan, R. K. et al. [43]. Using the extraction and classification of features from real-time SDN data, this study detects distributed denial-of-service attacks. The performance of ML algorithms may be enhanced by using an efficient feature extraction process, which will aid in selecting the most relevant data for the tasks at hand. The collected characteristics are used to train and evaluate popular classifiers like Support Vector Machines (SVM) to determine which performs best.

Feature and model selection (FAMS) proposed to which is used to detect DDoS assaults and whose models and characteristics are sought after because of their generalizability, preciseness, and speed of prediction [44].Four distinct stages make up the FAMS framework. The first stage is data pre-processing, which includes various operations such as characteristic coding, outlier processing, duplicate record removal, data balancing, and standardisation. Our enhanced RF model for detecting DDoS attacks has excellent generalization performance, a quick prediction time, and accuracy, making it very deployable. Additionally, it may be used in tandem with big data technologies in a manufacturing setting, allowing for distributed real-time detection networks.

Bagging ensemble-based DDoS attack detection system to detect DDoS Attacks in the Multimedia Cloud [45]. An extreme learning machine(ELM) trained on a single class of data serves as the

foundation of the classification system. These intrusions have been discovered using an outlier detection-based strategy. The suggested system's efficacy was tested experimentally using the NSL-KDD and CICIDS2017 benchmark datasets.

The authors present a stacked-ensemble privacy-preserving attack detection framework (P2ADF) for the cloud-based Internet of Things [46]. The system has a maximum detection rate of roughly 99.98% and can identify common threats like man-in-the-middle (MiTM) and DoS/DDoS in a fog-IoT environment. The CICDDoS19 and benchmark datasets are used to train the proposed model. P2ADF outperforms the proposed model and other state-of-the-art approaches by a wide margin.

Blockchain and IoT-based Intrusion Detection Systems IDS (BIoTIDS)tosee DDoS assaults in IoT networks and can spot unauthorized users on the network.A DDoS attack is one of several threats to IoT networks described in this study [47]. Blockchain, a novel technology for cryptocurrency transactions, may be included in developing a framework to secure IoT devices.

Anomaly-based network intrusion detection to use deep learning for IoT-based assaults examined by Sharma, B. et al. [48].To address the class imbalance problem in the dataset they offer and evaluate a DNN-based framework for boosting the amount of minority attack class packets in an IoT network. This system makes use of choosing features and GANs.Using GANs to generate minority assault synthetic data, the team achieved 91% accuracy despite the data set's severe class imbalance issues.

Novel feature-based framework (NF-bF) for detecting several forms of DDoS assaults described by Zhou, L. et a l [49].In this paper, they performed a deep dive into the characteristics of distributed denial of service (DDoS) assaults. They proposed five new metrics derived from various data packets: IP source circulating the entropy, flowing entropy, packet-based size entropy, package-based size entropy, and the number of ICMP destination unreachable packets. According to the experiments, the recommended fives characteristics outperformed the most popular traits by a wide margin.

Novel unsupervised GAN-based IDS (NUGAN-IDS) for self-focus and time-variant convolutional neural networks illustrated by de Araujo-Filho, P. F. et al. [50].The suggested IDS is designed for edge servers, which move computational resources closer to end nodes and benefit from edge computing. Our suggested IDS, as shown by the experiments, may be adjusted to meet a variety of detection rates and detection time needs. Table 1 shows the advantages and limitations of the research

Table 1: Advantages and limitations of the existing methods.

Ref	Author	Advantages	Limitation
1	Yusof, A. R. A. et al	Improved productivity may result from a mix of machine learning and other approaches with cooperation, distribution, and even mobility.	This method may manage or regulate network traffic congestion by dropping or rerouting packets beyond the allotted rate.
2	Shen, Y. et al.	The average dwell time design approach is used to meet the exponential stability requirement and provide an outstanding stability effect in a single-area electrical system employing an event-triggered demand frequency monitoring	The limitation of our research is a delay when occurred in the entire system processing

		strategy in the context of denial-of-service attacks.	
3	Jaafar, G. A. et al.	Several methods for the detection of HTTP DDoSattacks have emerged as a result of recent advances.	The database that contains information must be updated daily for improved outcomes, and here is where the suggested effort falls short.
4	Agrawal, N., &Tapaswi, S.	This work is stimulating classifies and describes numerous sorts of low-rate DDoS assaults, as well as protection techniques against them.	High-rate DDoS assaults are the primary focus of current defensive strategies in the area of DDoS attacks. However, for low-rate DDoS assaults, there is a shortage of published material.
5	Mahmoud, M.S. et al	This article will concentrate on these assaults, including how to model and identify them and maintain control of a CPS under attack.	Byzantine assaults on the fusion centre may lead to inaccurate sensor readings examining the upper limit of cooperative spectrum sensing under these conditions.
6	Imran, M. et al.	The SDN administrators may tailor a system to protect against DDoS assaults to their requirements and preferences.	This is the first study to try to categorize DoS mitigation techniques and determine their limits in an SDN setting.
7	Swami, R. et al.	It's decided that the study of ensuring safety using SDN capabilities has advanced considerably.	The assaults cannot be detected throughout the whole network, a major shortcoming.
8	Abdullah, T. A.	The finest user habits as well as remedies for smart home environments, were emphasized in this article.	With the help of a VPN, the secure communication channel may boost network traffic so that only authorized users can access it.
9	Sánchez, H. S. et al	Literature excerpts are used to illustrate the features of each attack and to illuminate possible defences.	Previously published research assumed an attacker with complete system knowledge might compromise a small subset of sensors.
10	Chong, M. S. et al	The risk management framework presents a summary of the area. Itconnects its contributions to the framework's three core pillars: outlining potential attack circumstances, quantifying their impact and likelihood,	The most vulnerable parts of a system may be identified using qualitative methods such as expert understanding and historical and empirical data. At the same time, quantitative techniques can determine which parts of a system must be

		and creating mitigating measures.	penetrated to carry out an attack.
11	Vishwakarma, R., & Jain, A. K.	A categorical description is offered based on the system models employed, major aspects, and flaws as their vulnerabilities, allowing for a comprehensive comparison study among the primary defence systems in recent past years.	Functions at this node are rethought with its restricted memory, storage, and power supply as primary considerations.
12	Nooribakhsh, M. et al	. According to the findings, the speed and precision with which an attack may be detected are the most crucial aspects of statistical attack detection systems, and this is particularly true when the detection system is taking the role of the victim.	Many statistical methods for detecting DDoS attacks rely on correlation, however these methods are prone to false positives because of the shift and scale connection between the properties of network traffic.
13	Singh, J., &Behal, S.	To lessen the burden of a central controller in SDN have been inspired to create a decentralized DDoS detection and mitigation framework based on the generalized theory of information metrics.	Another major difficulty is the increasing difficulty of controller scalability owing to computing limits as network sizes expand rapidly.
14	Mohan, A. M. et al.	Covert attack impacts on networked control systems like LFC are strongly urged research.	Noise in communication networks, whether caused by individual assaults or concerted attacks on LFC systems, is the subject of this analysis.
15	Reddy, K. G., &Thilagam, P. S.	The outcomes of our simulations indicate that naive Bayes DDoS attack traffic categorization excels in an adversarial setting and protects genuine traffic from DDoS attacks.	Therefore, the assault may be carried out by a single attacker with few network resources, and losing only one or two links would not significantly lessen the impact.Machine learning algorithms are required to manage unpredictable traffic flows, for which nodes must first gather training data.

16	Dantas Silva, F. S. et al	When SDN is combined with other technologies, it is advised that those technologies have a high innovation potential.	The research is limited in two ways: (i) because no strategies are presented for mitigating DDoS attacks based on low traffic rates, and (ii) because the procedure for mitigation is handled centralized at the outer boundaries of the network's infrastructure without proper consideration for the overlay managers.
17	Tayyab, M. et al.	Researchers have focused a lot of their attention on the capability of ML approaches to learning from examples, and the ML-based intrusion detection system is one of the methods that can identify DoS and DDoS assaults based on ICMPv6 packets.	On the one hand, an organization's privacy concerns limit the dissemination of its data, making it difficult to enhance the detection and efficiency of the machine learning-based intrusion detection system mode.
18	Alferidah, D. K., &Jhanjhi, N. Z.	The study delves into security breaches in great depth, analyzing them from two different points of view: layer-wise assaults and attack taxonomy.	Poor memory capabilities and constrained processing power might have caused the resource enervation assault.
19	Aladaileh, M. A. et al	To protect itself against DDoS assaults, the SDN controller suggests detection techniques that use an upper limit determined by a certain number of packets received in a specified time.	Attackers will take advantage of any constraints posed by the switches in the data plane, such as the capacity of their memories.
20	Mecheva, T., &Kakanakov, N.	They have proven useful in security for the Internet of Things and may be expected to play a role in ITS protection.	Additional challenges are introduced due to the restricted number of nodes and the stringent timing restrictions.
21	Kuzlu, M.et al	Because cybercriminals are continuously seeking new technologies to exploit to their advantage, it is essential to carefully consider all possible repercussions that a technical advancement might have before and after it is made public.	It should be emphasized that developers are at a disadvantage when it comes to the process of protecting a system or device, even though these detection technologies are available to developers as well;

22	BOUZOUBAA, K. et al	The feature selection step is an important aspect of the preprocessing phase for developing and optimizing these DOS-DDOS cybersecurity intelligence models. In particular, the feature selection approach based on the Wrapper method is essential.	It is not possible for predictive models to effectively address DOS-DDOS attacks and overcome the limitations and performance concerns that are associated with conventional security solutions.
23	Eliyan, L. F., & Di Pietro, R.	When it comes to giving a solution for DoS/DDoS assaults on SDN, we emphasized the implementation methods utilized to develop the solutions that were listed, along with the strategies that should be examined and the essential aspects that should be considered.	On the other hand, it places restrictions on the configurations and sizes of networks.
24	Dalmazo, B. L. et al	A systematic approach to collecting relevant articles and classifying them into a taxonomy of DDoS defensive methods based on three characteristics: degree of operation, location of implementation, and degree of collaboration	The SDN-Monitor prioritizes cutting down on control messages by minimizing the number of monitoring nodes via strategic switch placement and rerouting of network traffic.
25	Payares, E. D., & Martinez-Santos, J. C.	This research demonstrates that quantum ML may be used to predict DDoS attacks reliably.	We considered the constraints of the Frameworks while building our models, and we realized that the large dimensionality of our data might be a challenge.
26	Alghuraibawi, A. H. et al	While the experimental examination showed a high detection accuracy rate, this approach was only tested in an IPv4 network setting.	The researchers are tasked with developing a real-time system for detecting ICPMv6-DDoS assaults through anomaly detection techniques.
27	Aladaileh, M. A. et al	It has been observed that the detection accuracy of current IT-DA for DDoS assaults on the SDN controllers varies widely.	Although the proposed method attempts to detect distributed denial of service (DDoS) attacks early on, it is not very successful since it has a fixed threshold, which is unsuitable for detecting DDoS attacks with varying attack rates and

			hence increases the false-positive rate.
28	Alatawi, F.	The results showed that there is no one-hundred-percent-effective strategy for protecting from DDoS attacks. However, distributed defence is the best option since it assures that defensive components are deployed to all nodes.	Since the host system has much capacity for processing requests, these fake ones will quickly exhaust it.
29	Kim, K. et al	Research on assaults and countermeasures against autonomous vehicles is presented in a time-ordered fashion, with a clear breakdown of the many approaches used.	However, the protocol is incompatible with the CAN bus, which is standard in automobiles.
30	Salunke, K., &Ragavendran, U.	Efforts focusing on spotting anomalies tend to provide the most accurate detections. In contrast, capability-based methods are well-suited to mitigation, and divergence-based schemes yield superior results in differentiating between Flash Events.	Although this study offers some protection against clever DDoS attacks, its answers are not generalizable to public servers.
31	Akgun, D. et al	Together, the suggested IDS system and preprocessing techniques outperform the state-of-the-art.	The suggested model's inference time is reduced for simpler baseline models.
32	Ali, M. et al	Testing data is categorized using feature extraction and sparse matrix-building techniques learned from training data. Using this strategy makes it more likely that an assault will be detected.	The study's limitations are high dependability, quick computing, and decreased calculation complexity.
33	Kara, S. et al.	The reliable simulation tool reduced the cost and improved the performance	The limitation of this study is that it is critical to obtain data, outliers and item sets from cyber-attack.
34	Batchu, R. K., &Seetha, H.	During evaluations, the model scored an impressive 99.98% accuracy on the CICIDS-2017 database and 99.99% on the CICDDoS-2019 dataset.	The limitation of this study is that fewer datasets are used for this analysis.

35	El Sayed, M. S.	Our method has a high identification rate and a shorter, faster model-building time.	They test the model's performance with a single SDN controller to change the throughput and latency. Then, several controllers should be studied to ensure everyone is on equal ground and demonstrate how the embedded model may effectively collaborate with other kinds.
36	Patil, N. V. et al	The results show that the proposed SSK-DDoS successfully sorted the incoming data into seven distinct categories and recorded those classifications with each outbound connection's expected value in HDFS.	However, the scalability problem arises when we create a model using these methods and then deploy it on DPF/DSPF.
37	Pan, Y et al.	Attacks on bandwidth and resources are within its capabilities.	However, the suggested control technique may fail when both DoS and deception assaults are simultaneously launched against the communication networks of nonlinear NCSs experiencing time-varying latency.
38	Gaurav, A.	DDoS assaults are a reliable tool for hackers due to the lack of a reliable detection or filtering method.	In this method, each router sets its maximum amount of outgoing traffic; if the amount of incoming traffic exceeds that amount, the router filters the excess.
39	Kshirsagar, D., & Kumar, S	The framework effectively recognizes Portmap, LDAP, NetBIOS, and MSSQL vulnerabilities.	The study's limitations are the inadequate performance achieved by the suggested strategy and the limited scope of the datasets employed.
40	Bandi, A. et al.	DDoS assaults may be detected in real-time with great accuracy and precision using machine learning techniques.	Several limitations were discovered when training our models for this investigation. First, stochastic gradient boosting (SGB) training was tedious and fruitless since it required all available features.
41	Ahmad, I. et al.	Improving classification performance while reducing computing overhead and cost	This study needed to focus on Inadequate data in IDS

		necessitates using a feature selection strategy, which must be implemented.	
42	Liu, Z. et al.	The bi-LSTM networks' accuracy can improve to 98.5 percentage on a short dataset.	Researchers sought a solution by maximizing the usage of current public datasets using improved feature representations algorithms or machine learning techniques.
43	Chouhan, R. K.et al	It was chosen for use in the software-defined networking (SDN) controller that can detect threats in real-time due to its enhanced efficiency compared to other state-of-the-art works.	The performance of ML algorithms cannot be enhanced without a reliable feature extraction technique to filter out just the most relevant data for the given job.
44	Ma, R. et al.	More than a million synthetic datasets and over 330 thousand CIC-DDoS2019 datasets were used to demonstrate the framework's superior generalization capability.	Bagging sampling is preferred because it allows for rapid sub-model training without being limited by small sample size or from the dependence issue of copying and pasting.
45	Mustapha, A. et al.	It extracts features using the Kolmogorov-Smirnov test, which is based on the median absolute deviation around the median. Finally, it selects features using the chimp optimization approach based on the robust confidence interval.	This research has several limitations since identifying bots after an assault has been detected relies on network traffic analysis and the Turing test.
46	Kaur, J. et al.	Standard datasets, such as IoTID20, TON_IoT, N-BaIoT, UNSW-NB15, and CICDDoS19, hone the suggested model's capabilities.	In addition, hackers and curious onlookers are more likely to target a system when the processing layer is located near the user end.
47	Bediya, A. K., & Kumar, R.	IoT network intrusion and DDoS assaults may be identified with the help of BIoTIDS.	When one organization controls more than half of the nodes in a blockchain, that organization may have significant influence over the network.
48	Sharma, B. et al.	Create a filter-based strategy for decreasing the required number of characteristics. For example, removing one of every two highly correlated characteristics from the dataset	Networked devices are constrained in their ability to process data and store information.

		decreases the difficulty of training the model.	
49	Zhou, L. et al.	Compared to conventional approaches, the suggested framework may boost detection accuracy by as much as 53 percentage.	Compared to conventional approaches, the suggested framework may boost detection accuracy by as much as 53 percentage.
50	deAraujo-Filho, P. F. et al	The proposed IDS outperforms two state-of-the-art GAN-based IDSs, which are utilized as benchmarks in terms of accuracy and are at least 3.8 times quicker.	This research has an important weakness in that it uses a threshold to determine whether or not a data point is an abnormality in a time series.

1. Conclusion

When a service is under attack from a Distributed Denial of Service attack, it becomes temporarily unavailable to users. However, it has been shown that security on these devices is often ignored.This research aims to identify the most effective approach to detecting volumetric DDoS attacks by comparing several current machine learning approaches and constructing an IHF that uses just a few traffic parameters and basic DDoS detection criteria. Compare the normal and assault cases' graphs to choose the neural network's input properties heuristically. Most DDoS attack methods generate a significant volume of flows using a relatively small number of octets and packets, so these are the features selected for analysis. Based on experimental results our method achieved double the effectiveness of heuristic selection compared to the misclassification rate of automated selection. After that, the normalized target status for each attack type to provide more context about the attacks themselves. While heuristic feature selection and other standalone data mining methods may provide better results in a lab setting, our method has produced the greatest outcomes in the actual world.

Reference

1. Yusof, A. R. A., Udzir, N. I., &Selamat, A. (2019). Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), 292-315.
2. Shen, Y., Fei, M., & Du, D. (2019). Cyber security study for power systems under denial of service attacks. *Transactions of the Institute of Measurement and Control*, *41*(6), 1600-1614.
3. Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of recent detection methods for HTTP DDoS attack. *Journal of Computer Networks and Communications*, *2019*.
4. Agrawal, N., &Tapaswi, S. (2019). Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, *21*(4), 3769-3795.

5. Mahmoud, M. S., Hamdan, M. M., &Baroudi, U. A. (2019). Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing*, *338*, 101-115.
6. Imran, M., Durad, M. H., Khan, F. A., &Derhab, A. (2019). Toward an optimal solution against denial of service attacks in software defined networks. *Future Generation Computer Systems*, *92*, 444-453.
7. Swami, R., Dave, M., &Ranga, V. (2019). Software-defined networking-based DDoSdefense mechanisms. *ACM Computing Surveys (CSUR)*, *52*(2), 1-36.
8. Abdullah, T. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges attacks and solutions for Internet of Things based smart home. *Int. J. Comput. Sci. Netw. Secur*, *19*(9), 139.
9. Sánchez, H. S., Rotondo, D., Escobet, T., Puig, V., &Quevedo, J. (2019). Bibliographical review on cyber attacks from a control oriented perspective. *Annual Reviews in Control*, *48*, 103-128.
10. Chong, M. S., Sandberg, H., &Teixeira, A. M. (2019, June). A tutorial introduction to security and privacy for cyber-physical systems. In *2019 18th European Control Conference (ECC)* (pp. 968-978). IEEE.
11. Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems*, *73*(1), 3-25.
12. Nooribakhsh, M., &Mollamotalebi, M. (2020). A review on statistical approaches for anomaly detection in DDoS attacks. *Information Security Journal: A Global Perspective*, *29*(3), 118-133.
13. Singh, J., &Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. *Computer Science Review*, *37*, 100279.
14. Mohan, A. M., Meskin, N., &Mehrjerdi, H. (2020). A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems. *Energies*, *13*(15), 3860.
15. Reddy, K. G., &Thilagam, P. S. (2020). Naïve Bayes classifier to mitigate the DDoS attacks severity in ad-hoc networks. *International Journal of Communication Networks and Information Security*, *12*(2), 221-226.
16. Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., VenancioNeto, A. J., & Esposito, F. (2020). A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. *Sensors*, *20*(11), 3078.
17. Tayyab, M., Belaton, B., & Anbar, M. (2020). ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: a review. *IEEE Access*, *8*, 170529-170547.
18. Alferidah, D. K., &Jhanjhi, N. Z. (2020). A review on security and privacy issues and challenges in internet of things. *International Journal of Computer Science and Network Security IJCSNS*, *20*(4), 263-286.
19. Aladaileh, M. A., Anbar, M., Hasbullah, I. H., Chong, Y. W., &Sanjalawe, Y. K. (2020). Detection techniques of distributed denial of service attacks on software-defined networking controller–a review. *IEEE Access*, *8*, 143985-143995.

20. Mecheva, T., &Kakanakov, N. (2020). Cybersecurity in intelligent transportation systems. *Computers*, *9*(4), 83.
21. Kuzlu, M., Fair, C., &Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, *1*, 1-14.
22. BOUZOUBAA, K., TAHER, Y., & NSIRI, B. (2021). Predicting DOS-DDOS attacks: Review and evaluation study of feature selection methods based on wrapper process. *International Journal of Advanced Computer Science and Applications*, *12*(5).
23. Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, *122*, 149-171.
24. Dalmazo, B. L., Marques, J. A., Costa, L. R., Bonfim, M. S., Carvalho, R. N., da Silva, A. S., ... &Cordeiro, W. (2021). A systematic review on distributed denial of service attack defense mechanisms in programmable networks. *International Journal of Network Management*, *31*(6), e2163.
25. Payares, E. D., & Martinez-Santos, J. C. (2021). Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview. *Quantum Computing, Communication, and Simulation*, *11699*, 35-43.
26. Alghuraibawi, A. H. B., Abdullah, R., Manickam, S., &Alyasseri, Z. A. A. (2021). Detection of ICMPv6-based DDoS attacks using anomaly based intrusion detection system: A comprehensive review. *International Journal of Electrical and Computer Engineering*, *11*(6), 5216.
27. Aladaileh, M. A., Anbar, M., Hasbullah, I. H., &Sanjalawe, Y. K. (2021). Information theory-based approaches to detect DDoS attacks on software-defined networking controller a review. *International Journal of Education and Information Technologies*, *15*, 83-94.
28. Alatawi, F. (2021). Defense mechanisms against distributed denial of service attacks: comparative review. *Journal of Information Security and Cybercrimes Research*, *4*(1), 81-94.
29. Kim, K., Kim, J. S., Jeong, S., Park, J. H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, *103*, 102150.
30. Salunke, K., &Ragavendran, U. (2021). Shield techniques for application layer DDoS attack in MANET: a methodological review. *Wireless Personal Communications*, *120*(4), 2773-2799.
31. Akgun, D., Hizal, S., &Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security*, *118*, 102748.
32. Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., &Bahaj, S. A. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). *Electronics*, *11*(3), 494.
33. Kara, S., Hizal, S., &Zengin, A. (2022). Design and Implementation of ADevs-Based Cyber-Attack Simulator for Cyber Security. *International Journal of Simulation Modelling (IJSIMM)*, *21*(1), 53-64.

34. Batchu, R. K., &Seetha, H. (2022). A hybrid detection system for DDoS attacks based on deep sparse autoencoder and light gradient boost machine. *Journal of Information & Knowledge Management*, 2250071.
35. El Sayed, M. S., Le-Khac, N. A., Azer, M. A., &Jurcut, A. D. (2022). A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs. *IEEE Transactions on Cognitive Communications and Networking*, *8*(4), 1862-1880.
36. Patil, N. V., Krishna, C. R., & Kumar, K. (2022). SSK-DDoS: distributed stream processing framework based classification system for DDoS attacks. *Cluster Computing*, 1-18.
37. Pan, Y., Wu, Y., & Lam, H. K. (2022). Security-based fuzzy control for nonlinear networked control systems with DoS attacks via a resilient event-triggered scheme. *IEEE Transactions on Fuzzy Systems*, *30*(10), 4359-4368.
38. Gaurav, A., Gupta, B. B., Alhalabi, W., Visvizi, A., &Asiri, Y. (2022). A comprehensive survey on DDoS attacks on various intelligent systems and it'sdefense techniques. *International Journal of Intelligent Systems*, *37*(12), 11407-11431.
39. Kshirsagar, D., & Kumar, S. (2022). A feature reduction based reflected and exploited DDoS attacks detection system. *Journal of Ambient Intelligence and Humanized Computing*, 1-13.
40. Bandi, A., Sherpa, L., &Allu, S. M. (2022). Machine learning algorithms for DDoS attack detection in cybersecurity. In *Modern Approaches in Machine Learning & Cognitive Science: A Walkthrough* (pp. 269-281). Cham: Springer International Publishing.
41. Ahmad, I., Zhong, W., & Ahmad, A. (2023). A Big Data Analytics for DDOS Attack Detection using Optimized Ensemble Framework in Internet of Things. *Internet of Things*, 100825.
42. Liu, Z., Guo, C., Liu, D., & Yin, X. (2023). An Asynchronous Federated Learning Arbitration Model for Low-Rate DDoS Attack Detection. *IEEE Access*, *11*, 18448-18460.
43. Chouhan, R. K., Atulkar, M., &Nagwani, N. K. (2023). A framework to detect DDoS attack in Ryu controller based software defined networks using feature extraction and classification. *Applied Intelligence*, *53*(4), 4268-4288.
44. Ma, R., Chen, X., &Zhai, R. (2023). A DDoS Attack Detection Method Based on Natural Selection of Features and Models. *Electronics*, *12*(4), 1059.
45. Mustapha, A., Khatoun, R., Zeadally, S., Chbib, F., Fadlallah, A., Fahs, W., & El Attar, A. (2023). Detecting DDoS attacks using adversarial neural network. *Computers & Security*, *127*, 103117.
46. Kaur, J., Agrawal, A., & Khan, R. A. (2023). P2ADF: a privacy-preserving attack detection framework in fog-IoT environment. *International Journal of Information Security*, 1-14.
47. Bediya, A. K., & Kumar, R. (2023). A novel intrusion detection system for internet of things network security. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 330-348). IGI Global.

48. Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. *Computers and Electrical Engineering*, *107*, 108626.
49. Zhou, L., Zhu, Y., Xiang, Y., &Zong, T. (2023). A novel feature-based framework enabling multi-type DDoS attacks detection. *World Wide Web*, *26*(1), 163-185.
50. deAraujo-Filho, P. F., Naili, M., Kaddoum, G., Fapi, E. T., & Zhu, Z. (2023). Unsupervised GAN-based intrusion detection system using temporal convolutional networks and self-attention. *IEEE Transactions on Network and Service Management*.