Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8481452, 16 pages
https://doi.org/10.1155/2022/8481452

Research Article

ML-DDoSnet: IoT Intrusion Detection Based on Denial-of-Service Attacks Using Machine Learning Methods and NSL-KDD

Mona Esmaeili,[1] Seyedamiryousef Hosseini Goki,[2] Behnam Hajipour Khire Masjidi,[3] Mahdi Sameh,[4] Hamid Gharagozlou ,[5] and Amin Salih Mohammed[6,7]

[1]*Department of Electrical & Computer Engineering, University of New Mexico, Albuquerque, NM 8731, USA*
[2]*Department of Computer Science, University of Victoria, Victoria, BC, Canada*
[3]*Department of Computer, Faculty of Electricity and Computer, Islamic Azad University, North Tehran Branch, Tehran, Iran*
[4]*Department of Computer Engineering, Sabzevar Branch, Islamic Azad University, Sabzevar, Iran*
[5]*Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran*
[6]*Department of Computer Engineering, College of Engineering and Computer Science, Lebanese French University, Kurdistan Region, Iraq*
[7]*Department of Software and Informatics Engineering, Salahaddin University, Kurdistan Region, Iraq*

Correspondence should be addressed to Hamid Gharagozlou; hamid.gh@aut.ac.ir

Received 3 February 2022; Revised 1 March 2022; Accepted 7 July 2022; Published 21 August 2022

Academic Editor: Ashish Bagwari

The Internet of Things (IoT) is a complicated security feature in which datagrams are protected by integrity, confidentiality, and authentication services. The network is protected from external interruptions and intrusions. Because IoT devices run with a range of heterogeneous technologies and process data over time, standard solutions may not be practical. It is necessary to develop intelligent procedures that can be used for multiple levels of data flow in the system. This study examines metainnovations using deep learning-based IDS. Per the findings of the earlier tests, BiLSTMs are better for binary (regular/attacker) classification; however, sequential models (LSTM or BiLSTM) are better for detecting some brutal attacks in multiclass classifiers. According to experts, deep learning-based intrusion detection systems can now recognize and select the best structure for each category. However, specific difficulties will need to be solved in the future. Two topics should be studied further in future attempts. One of the researchers' concerns is the impact of various data processing techniques, such as artificial intelligence or metamethods, on IDS. The BiLSTM approach has chosen the safest instances with the highest accuracy among the models. According to the findings, the most reliable and suitable solution for evaluating DDoS attacks in IoT is the BiLSTM design.

1. Introduction

As the secure network architecture transitions to open connectivity, the network becomes more adaptable, omnipresent, and cognitive. These advancements have accelerated the development of next-generation Internet technologies, including big data, cloud computing, the Internet of Things, and programmable networks. However, with software-defined network architecture, the potential of a DDoS attack brought on by centralized control becomes more apparent [1]. IDS are divided into two categories. Vulnerability assessment, which finds attacks based on recognized signatures, and anomaly detection, which detects aberrant attacks based on usual usage patterns, are the two types. At the same time, it is difficult to find unknown threats using abuse detection and anomaly detection benefits in finding them. Nevertheless, because defining a range of typical use patterns is complex, anomaly detection has a high rate of false alerts [2]. DDoS attacks are presently one of the most challenging network attacks to recognize [3]. The goal is to deplete the target platforms or network capabilities, making the victim unable to perform routine tasks. There are two types of

DDoS attacks: resource bandwidth-consuming attacks and system resource-consuming attempts. Many zombie hosts are used in resource bandwidth attacks to swiftly produce a significant volume of traffic that converges on the victim's server and entirely consumes its network bandwidth resources. Sending a high number of UDP, TCP, and ICMP packets repeatedly, for example, might trigger a flooding attack, resulting in UDP flooding, TCP flooding, and ICMP flooding. Amplification attacks, such as DNS reflection amplification attacks, can also be performed via reflection. Protocol vulnerabilities are commonly used in system resource attacks to use the victim's host resources (TCP-SYN half-connection attack employing TCP three-way handshake, for example [4]).

Conventional network approach checking and data analytics confront various obstacles and issues in such networks, such as reliability and practical real-time analysis of massive data. Furthermore, due to varied factors such as device mobility and network heterogeneity, the pattern of network traffic, particularly in cellular networks, shows exceptionally complicated behavior. Deep learning has been successfully used in large data systems to aid analytics and knowledge discovery by recognizing hidden and complex patterns. Researchers in the field of networking are using deep learning techniques for network traffic monitoring and analysis applications, such as traffic categorization and prediction, as a result of these results [5]. Conceptual designs based on traditional machine learning, based on manually and expert-generated features, are outmoded and unable to keep up with the rapidly increasing collection of applications and the moving target nature of mobile traffic [6].

As cyberattacks grow more intelligent, it is becoming increasingly challenging to find advanced cyberattacks in many industries, including industry, national defense, and healthcare. Traditional intrusion detection systems can no longer detect sophisticated attacks with unusual patterns. Attackers get around recognized signatures by impersonating regular users. Deep learning is a potential solution to these problems [2]. Deep learning (DL) intrusion detection does not require much malicious activity or a list of typical activities to create detection rules. Through empirical data learning, DL defines incursion characteristics on its own. Since machine learning is widely used in IDS research, KDD has been used as a dataset in many of them. Most of these research studies use binary categorization to divide the KDD into the attack and benign categories. They also use multiclass classification to divide the KDD into four distinct groups. Even though the large-scale CNN algorithm has produced impressive results in detecting attacks, few people consider keeping good detection performance with limited resources. Deploy the learned CNN model in the SD-IoT controller, for example. As more IoT devices are installed in the system, the likelihood of the network being attacked by unsecured IoT devices grows, needing the development of a defense mechanism. Deep learning can dynamically extract high-level characteristics from low-level ones, allowing for sophisticated representation and reasoning.

Standard solutions may not be practical since IoT devices employ various heterogeneous technologies and analyze data over time. Intelligent processes that can be used for various levels of data flow in the system must be developed. The IDS, based on deep learning, is used to investigate metainnovations in this work. BiLSTMs are better for binary (regular/attacker) classification. At the same time, sequential models (LSTM or BiLSTM) are better for finding some harsh attacks in multiclass classifiers, according to the results of prior testing. Deep learning-based intrusion detection systems, according to experts, can now recognize and pick the best structure for each category. On the other hand, specific problems will need to be resolved in the future. In future attempts, two things should be investigated further. The influence of various data processing techniques, such as artificial intelligence or metamethods, on IDS is one of the researchers' concerns. The BiLSTM technique has found the safest examples with the maximum accuracy among the models. According to the findings, the BiLSTM design is the most reliable and proper choice for analyzing DDoS attacks in IoT. MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF are among the eight machine learning algorithms used in this study to find DDoS attacks in IoT. NSL-KDD is the process dataset, with 1 and 0 labels denoting normal and abnormal behaviors, respectively. A confusion matrix is used to display the classification findings.

This paper includes the following sections. (1) Introduction supplies the main problem statement and importance, contribution, and novelty of the presented method. (2) Literature Review represents the background of both the method and the problem of recent years' research. (3) Methods and Material illustrates the approach characteristics and introduction to supplied machine learning techniques. (4) Results and Discussion also presents the classification and diagnosis outcomes. And finally, (5) Conclusion presents the overall results and future works.

2. Literature Review

DDoS attacks are presently the most common and effective dangers to businesses, becoming increasingly tempting [7]. GitHub, for instance, was the target of one of the most significant DDoS attacks ever in 2018 [8]. This devastating attack is one of the most well-publicized attacks of the modern era, shattering the foundations of one of the CIA security triad's pillars (presence). Thousands of dump terminals, computers, and botnets are used by attackers to perform DDoS attacks simultaneously, exhausting the target system's significant resources and rendering all services inaccessible. There are many legitimate and effective technologies available that may be used to conduct DDoS attacks on both big sizes and small sizes. Another DDoS attack occurred recently [8]; the lawful Memcached utility, whose primary task is to lessen the load on the supporting Internet services, was abused by the attackers. The attacker used Memcached items and fake IP addresses, allowing Memcached answers to be routed to the target addresses at a rate of 126.9 million packets per second, using a significant amount of target capacity. Furthermore, the use of fake IPs makes tracing DDoS attacks nearly hard [9].

Numerous publications have been written on IDS. IDS based on software-defined networks is proposed by Manso et al. [10]. DDoS attacks are detected by the proposed IDS, which alerts the sensor nodes. Karim et al. [11] investigated the performance of Snort-based IDS on a network. Xu et al. [12] proposed a deep forest-based distributed denial-of-service detection and defense model. They concentrate on attacks on smart nodes and the significant data context. Anomaly detection approaches for commercial sensor networks based on machine learning have also been studied [13]. According to Lv et al. [14], solving the security problems of CITS Digital Twins (DTs) using deep learning (DL) is possible. Chen et al. [15] have concluded that motorcycle bans reduce traffic accident deaths by a significant amount, and their effectiveness doesn't diminish over time due to the diversity of their policies. A proposed study by Lv et al. [16] examines the application of Digital Twins in manufacturing intelligent equipment and further optimizes its fault diagnosis effect. In Liu et al. [17], a framework has been proposed for analyzing lung and colon histopathological images. Sun et al. [18] describe a lightweight remote control communication scheme. The authors believe that analyzing the scheme's performance shows that it is practical and appropriate for non-time-sensitive scenarios that require high anonymity. Naive Bayes, random forests, and logistic regression were proposed as machine learning approaches to detect fake identity attacks by Mehbodniya et al. [19]. According to Cao et al. [20], an optimization model based on SAGIN-IoV service requirements is constructed and an improved algorithm is proposed. A lifelong learning framework called the Generalized Lifelong Spectral Clustering (GL22SC) has been explored by Sun et al. [21]. According to Ahmadi et al. [22], deep-Q-reinforcement learning ensembles can choose a subset of devices in each communication round by using a combined deep-Q-reinforcement learning ensemble based on spectral clustering (DQRE-SCnet). According to Sun et al. [23], Flexible Clustered Lifelong Learning (FCL3) comprises two knowledge libraries: a feature learning library and a model knowledge library. According to Liu et al. [24], the SFERNN was optimized by minimizing the cross-entropy loss on the source branches and the distributional discrepancy between the source branches and the target branches. Using the modified Lamport Merkle Digital Signature method, Mehbodniya et al. [25] developed a framework for generating and verifying digital signatures. An improved gray wolf optimization (IGWO) algorithm was used by Zhang et al. [26] to develop a charging safety early-warning model for electric vehicles (EV). It is a pioneering attempt to distinguish transferable or untransferable knowledge across domains with the Knowledge Aggregation-induced Transferability Perception (KATP) developed by Dong et al. [27]. According to Yang et al. [28], aggregated vehicle fuel consumption data can be protected against time series-based differential attacks using a negative survey approach. An algorithm combining interactive machine learning and active learning for HBR prediction was proposed by Wu et al. [29]. Using local differential privacy (LDP) and elliptic curve cryptography (ECC), Khaliq et al. [30] describe parking recommender systems with research gaps. Recent SBR prediction models have performed poorly due to mislabeled instances in five publicly available datasets, according to Wu et al. [31]. Kim et al. employed several KDD computer vision experiments to divide the dataset into four groups or two or more independent variables, attack and benign. Instead of concentrating on primary groups, they focus on specific attacks within the same area. They also looked at the DoS category in both databases and created a DL model for detecting DoS [2]. In a software-defined Internet of Things setting, Wang et al. suggested a DDoS attack detection system to safeguard in real time. They used an updated firefly method to find DDoS attacks to enhance the convolutional neural network (CNN). The findings showed that the proposed technique could detect innocuous traffic and DDoS activities with more than 99 percent [4]. Depending on the information entropy and deep learning, Liu et al. suggested a two-level DDoS attack detection approach. First, the information entropy detection technique found suspicious elements and ports with coarse granularity. The convolutional neural network (CNN) model used a fine-grained packet-based detection technique to find regular traffic from suspect traffic. The controller implemented the defense strategy to thwart the onslaught. The testing findings reveal that the suggested method's detection accuracy is 98.98 percent, indicating that it can successfully identify DDoS attack traffic in an SDN context [1]. Based on their analysis of the impact of class imbalance on SBR prediction, Zheng et al. [32] found that it had a negative impact on prediction accuracy. A random forest classifier was used by Zhang et al. [33] to train a Just-in-Time defect prediction model based on six open source projects. A DeepBAN communication framework was proposed by Liu et al. [34]. The results showed that it can improve the energy efficiency of dynamic WBANs by 15% over stochastic scheduling schemes. The dominant feature set was extracted using a novel dominant feature selection algorithm developed by Gera et al. [35]. Smart contract vulnerability detection using graph neural networks and expert knowledge was explored by Liu et al. [36]. The proposed solution by Zhang et al. [37] is aimed at achieving rapid video prefetching and traffic reduction. With their new detection method, Zong et al. [38]applied a multiscale grouping (MSG) structure to a 3D point cloud tunnel dataset and applied a 3D-BoNet instance segmentation model. An optimization of energy consumption in dynamic wireless sensor networks using fog computing and fuzzy multiattribute decision-making was proposed by Varmaghani et al. [39]. According to Zong and Wan [40], a 3D scanner can be used to acquire 3D data. The method's validity and reliability have been further verified. As a result of sophisticated fuzzy logic, Singh et al. [41] develop algorithms for mobility and traffic management that are as flexible as possible while retaining high performance. Xie et al. [42] have proposed many heuristic or metaheuristic algorithms/methods to solve this NP-hard problem. Using the traditional undesired multiuser interference and the interference caused by imperfect hardware components, Li et al. [43] summarize constructive interference (CI) and explain how it can benefit the 1-bit signal design. As a future multichannel communication application for terahertz (THz), Feng et al. [44] presented a 220 GHz four-channel, noncontiguous, and manifold-coupled waveguide multiplexer.

Ghanbari upgraded the VFD and devised feature extraction methods with a mother wavelet to boost detection. For DDoS attacks, the adoptive mother wavelet was designed to reach the best similarity and flexibility to the input data for a specific purpose. Because Internet traffic data with DDoS-ITD is a long-range-dependent signal, a variational technique is used to extract the hidden properties of each DDoS-ITD scale. This study employs and advances an online variance fractal dimension approach. Then, a CNN-based IDS was created to improve the sensitivity of DDoS attack detection. As a result, a weighted cost function was designed for assessing the artificial neural network and CNN structure. The suggested structure of the polyscale CNN about policy gradient-based deep reinforcement learning was used to develop and execute the IDS for unlabeled data to get a more real IDS. The IDS discovered the irregularities with 93 percent accuracy [45]. A 220 GHz multicircuit integrated front end based on solid-state circuits was presented by NIU et al. [46]. The knowledge-based VQA (Visual Question Answering) module developed by Zheng et al. [47] is designed to extend the versatility of knowledge-based VQA. Ramtin et al. [48] analyzed the maximum damage that a DDoS attacker can make without being detected by a detection system at the network edge. They considered two classical classifiers based on hypothesis testing, whether the detector knows the distribution of attack traffic or not. The authors theoretically proved that the maximum damage follows a square root law. They also illustrated their results using empirical data. The study by Zheng et al. [49] proposes a detailed visual reasoning model as a theoretical and experimental basis for introducing different levels of knowledge representation into deep learning. Zheng et al. [50] developed a multilayer semantic representation network for sentence representation. In a side-channel attack using an off-the-shelf smartphone, Yu et al. [51] demonstrated the feasibility of inferring keystrokes on touch screens. The concept of user authentication was advanced by Kong et al. [52] in order to protect user privacy and to provide personalized services to users. According to Hajipour et al. [53], the Breast Cancer Ultrasound Dataset is used as the input image for a two-dimensional contourlet. A fog-based smart grid scheme with sensible pricing and packing was presented by Zhao et al. [54]. In a study by Meng et al. [55], they propose a method for adaptive neural tracking control of an uncertain two-link rigid-flexible manipulator under vibration amplitude constraints. In earlier papers, Ghanbari and Kinsner have described an abnormality detector for enhancing the detection rate of a DDoS attack in a smart grid. Increased categorization of the training and testing stages was used to carry out this improvement. A full version of the variance fractal dimension trajectory (VFDTv2) was applied to extract intrinsic characteristics from the stochastic fractal input data. A discrete wavelet transform was applied to the input data during data preprocessing. The VFDTv2 removed critical differentiating features (see Table 1).

Mishra and Pandya analyzed and contrasted intrusion detection and prevention methods for minimizing DDoS attacks, emphasizing detection approaches. In addition, the categorization of intrusion detection systems, numerous anomaly detection approaches, different intrusion detection systems patterned on datasets and various machine learning methods, and pattern recognition algorithms for data preprocessing and malware detection were covered. Finally, a more significant viewpoint was imagined while reviewing research obstacles, possible answers, and future aspirations [67]. According to Ahmadi and Abadi [68], the expert can access and develop the system without knowing the underlying code by using the object orientation properties of C++. For selecting the optimal BFTIs, Zhou et al. [69] proposed a multiobjective function consisting of a BFTI's smallest occlusion and its largest facade texture area. Ahmadi et al. [70] used deep neural networks with fuzzy wavelets to predict Iranian energy demand. Among the innovative studies presented by Zhou et al. [71], one focuses on the design of airborne-oriented supercontinuum laser hyperspectral (SCLaHS) LiDARs with 50 bands but with a 20 nm spectral resolution and a 0.5-meter ground sampling distance (GSD). A case study method was used by Tondro et al. [72] to gather in-depth data timeline attributes of all ICT-based enterprises and academic institutions within Alborz province in Iran. This paper presents a generalized buffering algorithm (GBA), which considers all instances within a buffer zone in terms of geometric distance and attribute characteristics [73]. For a comprehensive review of relevant research, Liang et al. [74] used bibliometric mapping, text mining, and qualitative analysis. In a study by Zhao and Wang [75], they have improved lightweight mobile networks based on YOLOv3 for pedestrian detection. For visual tracking, Zhu et al. [76] developed the Siamese-ORPN (Siamese Oriented Region Proposal Network). Li et al. [77] proposed a novel neural network architecture for encoding and synthesizing 3D shapes. The authors discussed transfer learning-based neural network models for the identification of butterfly species in Rajeena et al. [78]. Ghayvat et al. suggested a strategy that combines a blockchain-based nondisclosure method with a two-step authentication architecture and an elliptic curve cryptography-based cryptographic signature framework. Furthermore, a process was designed to protect the ecosystem from DoS- and DDoS-based attack methods [79]. Mirsky et al. proved a plug-and-play network intrusion detection system that can autonomously and efficiently train to find attacks on the local network. Kitsune's main algorithm collaboratively used autoencoders to distinguish between the normal and anomalous traffic patterns. Kitsune was shown to be capable of detecting a variety of attacks at a rate equivalent to that of offline anomaly trackers, even on a Raspberry Pi [80]. Additionally, Bovenzi et al. suggested a two-stage hierarchical technique for detecting attacks. It detected

Table 1: The summary of the research in the field of IoT intrusion detection.

Author	Year	Feature extraction	Attack	Classification
Wang et al. [4]	2022	(i) Per networking flow, the number of packets (ii) The amount of data transferred each networking flow in bytes (iii) Each networking flow's duration (iv) Networking flow rate (v) The communication flow's source IP addresses (vi) The IP addresses of the networking flow's source	DDoS	Firefly and CNN
Liu et al. [1]	2022	Source IP address, destination IP address, source port, destination port, packet length, and packet protocol	DDoS	Information entropy, CNN
Najafimehr et al. [56]	2022	CICFlowMeter features	DDoS SDN flood, reflection, Portmap reflection, MSSQL reflection, NetBIOS reflection amplification	CLSTMNet, CNN-LSTM
Prasad and Chandra [57]	2022	COLS_WONA features	Volumetric DDoS	Defensive fast detection mode
Xu et al. [58]	2022	Automatic spatial feature extraction	DoS attack	CNN, LSTM
Tsogbaatar et al. [59]	2021	Time Series Benchmark Suite	Very short intermittent DDoS	CNN
Tang et al. [60]	2021	Multifeature fusion	Low-rate denial-of-service attack	CNN
Alkahtani and Aldhyani [61]	2021	Properties of switch device port replication in IoT scenarios	Botnet attack	CNN, LSTM
Mendonca et al. [62]	2021	User features of HTTP, HTTPS, FTP, SSH, and email protocols	DDoS	Fast hierarchical deep CNN, tree CNN
Ghanbari and Kinsner [63]	2021	Adaptive mother wavelet	DDoS	CNN, genetic neural network
Liu et al. [64]	2019	NetFlow images	DDoS, DoS	SVM, CNN, ANN
Cheng et al. [65]	2020	Grayscale matrix feature	DDoS	Multiscale CNN
Cil et al. [66]	2021	(i) In the reverse direction, the average number of the bulk rate (ii) In the rearward order, the average number of bytes of the bulk rate (iii) In the reverse direction, total bytes used for headers (iv)The total number of bytes delivered in the backward order in the first window (v) In the backward direction, the maximum size of a packet (vi) In the reverse order, the smallest packet size (vii) In the backward direction, the standard deviation of the packet size	DDoS	Feedforward-based deep neural network

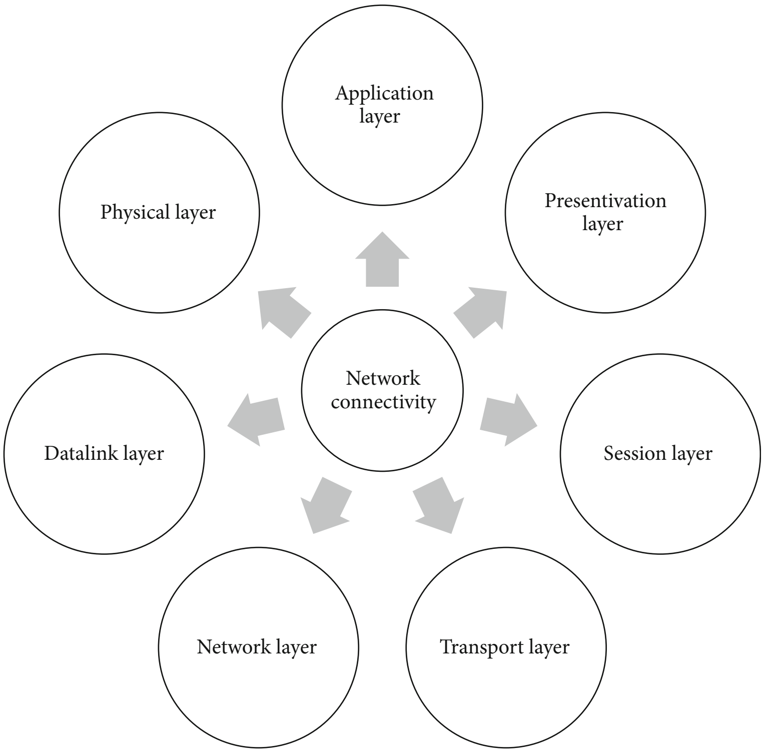


Figure 1: The 7-layer conceptual framework for describing network connectivity.

and classified attacks using a unique lightweight method based on a multimodal deep autoencoder and soft-output classifications. Apart from the performance benefits, their approach is well suited for dispersed and privacy-preserving deployments while minimizing the need for retraining, which is necessary for the high speed and durability needed in IoT applications [81].

For data postprocessing, a support vector machine (SVM) was used. The solution correctly identified the DDoS attack with an accuracy of 87.35 percent [82]. Zhang et al. [83] proposed updating a particle swarm template (PST) to accelerate the randomized search. This is a set of uniformly sized particles in the 6D space of the camera pose that are presampled within the unit sphere. According to Zhang et al. [84], orthogonal processing on compression (orthogonal POC) can efficiently support text analytics irrespective of how the data is processed. Fouladi et al. suggested a continuous wavelet transform and CNN-based detection and countermeasure technique. To distinguish attack data from baseline characteristics, the approach employed CWT characteristics as the input for the CNN algorithm. The suggested system has a high detection rate against DNS amplification, NTP, and TCP-SYN flood attacks, with a low false alarm rate, according to the empirical observations [85].

3. Methods and Material

3.1. Distributed Denial-of-Service (DDoS) Attack. DDoS attacks stand for distributed denial-of-service attacks. This form of attack takes advantage of network resource ability restrictions, such as the infrastructure that supports a company's website. The DDoS attack will make many requests to the targeted online resource to overwhelm the website's ability to handle multiple demands and prevent it from operating correctly. In a DDoS attack, the incoming traffic that floods the target comes from various places. It makes stopping the attack by blocking a single source difficult [86]. A DoS or DDoS attack is like a mob of people surrounding a shop's entrance door, making it difficult for genuine companies to visit and disrupting business. Numerous attack machines can create more attack traffic than a single attack machine. Multiple attack machines are more difficult to switch off than a single attack machine. Each attack machine's activity can be stealthier, making it more difficult to detect and shut down. Because the received signal overwhelming the target comes from various sources, using ingress filtering alone may not be enough to halt the attack. It is also difficult to distinguish between regular user traffic and DoS attacks when dispersed over numerous places of origin [87].

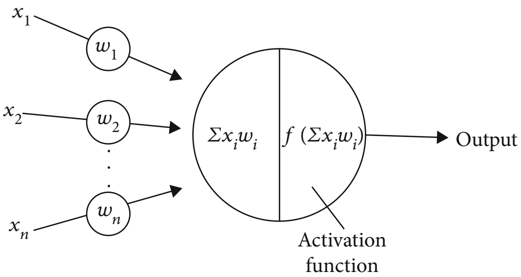
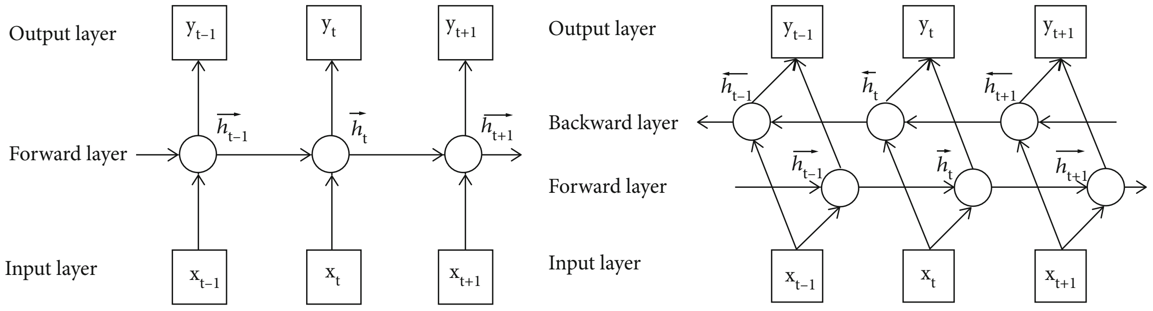


Figure 2: The leading architecture of the MLP method.



(a) LSTM

(b) BiLSTM

Figure 3: The architecture of the LSTM and BiLSTM methods.

Table 2: The correlation coefficient for IoT intrusion detection.

Correlation value	Categorical value
(-0.1, 0.1)	Very weak
(-0.3, -0.1) or (0.1, 0.3)	Weak
(-0.5, -0.3) or (0.3, 0.5)	Moderate
(-1, -0.5) or (0.5, 1)	Strong

Computer networks connected to the Internet are used to conduct DDoS attacks. Malware-infected PCs and other devices (such as the Internet of Things equipment) form these networks, run remotely by an intruder. Bots (or zombies) are standalone devices, while a botnet refers to a collection of bots. To conduct an offensive using a botnet, the attacker can send remote commands to each bot. Each bot in a botnet queries the IP address of the victim's server or network. Overburdening the server or network could result in a denial-of-service attack against ordinary traffic. As each bot is an actual Internet node, it can be difficult to distinguish attack traffic from regular traffic [88]. DDoS attacks target various parts of a network connection. Before you can understand how other DDoS attacks work, you must first understand how a network connection is made. A networking line on the Internet forms numerous components or "layers." Each layer in the model has a distinct function, like how each layer in a home carries out a specific goal. The OSI model is a seven-layer theoretical framework for explaining network connections (see Figure 1).

While virtually all DDoS attacks include flooding a target device or network with traffic, there are three types of attacks. In response to the target's defenses, an intruder may utilize one or more alternative attack vectors or cycle possible attacks [86–88].

3.2. Feature Extraction. The three significant processes are data preprocessing, training, and validation. The data preparation stage's primary purpose is to turn raw data into a well-formatted dataset with suitable properties and labels. Data is acquired from various sources for network traffic categorization, including recorded network traffic, checked network information, and sampled packet data. The preprocessing is then completed [89]. Based on the parameters of the chosen machine learning technique and the problem's knowledge domain, the primary method may vary. After data processing, feature extraction, an essential part of a classification model, is performed. The feature extraction is aimed at enhancing the classification model's performance by removing unnecessary features and speeding up the training process by lowering the number of attributes in the dataset. The final dataset, which has the proper collection of features, is divided into separate sets for training and test data. The chosen learning approach employs the movement set to automatically learn the model parameters and produce a classifier during the training phase.

It must be emphasized that the human setting of a collection of hyperparameters is needed for most learning algorithms. Decide the proper hyperparameter values for a model for a particular circumstance. The rule of thumb, earlier experiences, values used in other successful applications, and validation techniques have all been used to select suitable hyperparameters. The training set can train separate classifiers targeting diverse groups of hyperparameters using the specified learning method. The performance of the classifiers developed is then estimated using a validation set that does not overlap with the training set. The finished classifier is constructed using the same hyperparameters that supply the best performance. The performance of the finished classifier is assessed in the testing step based on the predictions it makes using the activity that can be defined [90].

3.3. Multilayer Perceptron. An ANN is inspired by the form and functionality of biological neural networks. Artificial neurons, a collection of nodes stacked into layers and linked by weighted edges, make up the system. Figure 2 depicts a primary artificial neuron. The received signals are weighted and aggregated. Then, using an activation function for each neuron, they were converted into an output signal. The output signals are passed on to the next layer [91]. This procedure is repeated until the final and output layers are reached. Between the input and output levels are hidden layers that do processing and calculations. The weights of coupled neurons are initially randomly given during the training phase. Then, the underlying learning algorithm is perfected. Backpropagation with gradient descent is the most widely used learning approach for perfecting edge weights. ANN comes in a variety of shapes and sizes. A simple ANN consists of a feedforward network link devoid of cycles [91].

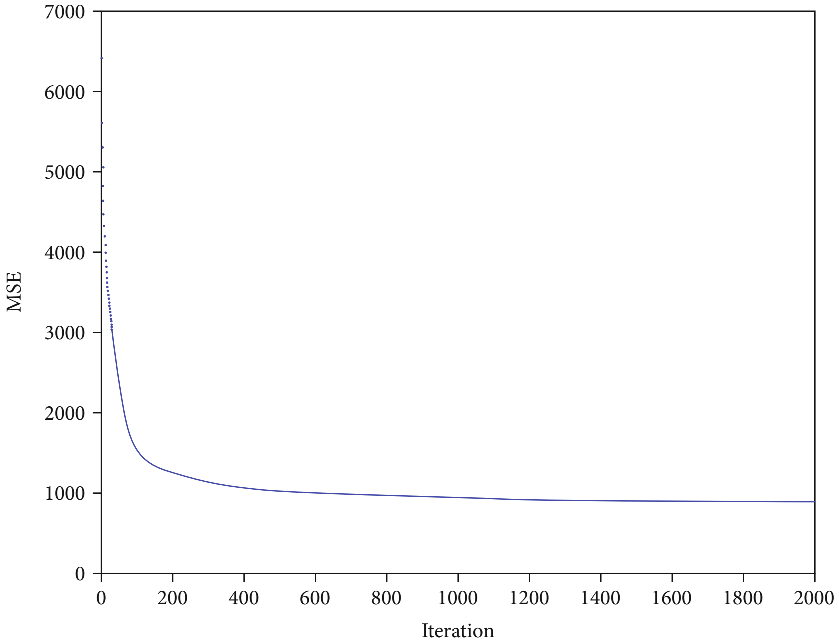


Figure 4: The training process of the MLP method.

3.4. Long Short-Term Memory (LSTM). Long short-term memory (LSTM) is a paradigm first suggested in 1997. Bidirectional LSTM expands the LSTM model, a gated recurrent neural network. The crucial aspect is that these networks may keep data for future cell processing. We may conceive of LSTM as an RNN with two key vectors and a memory pool [92]:

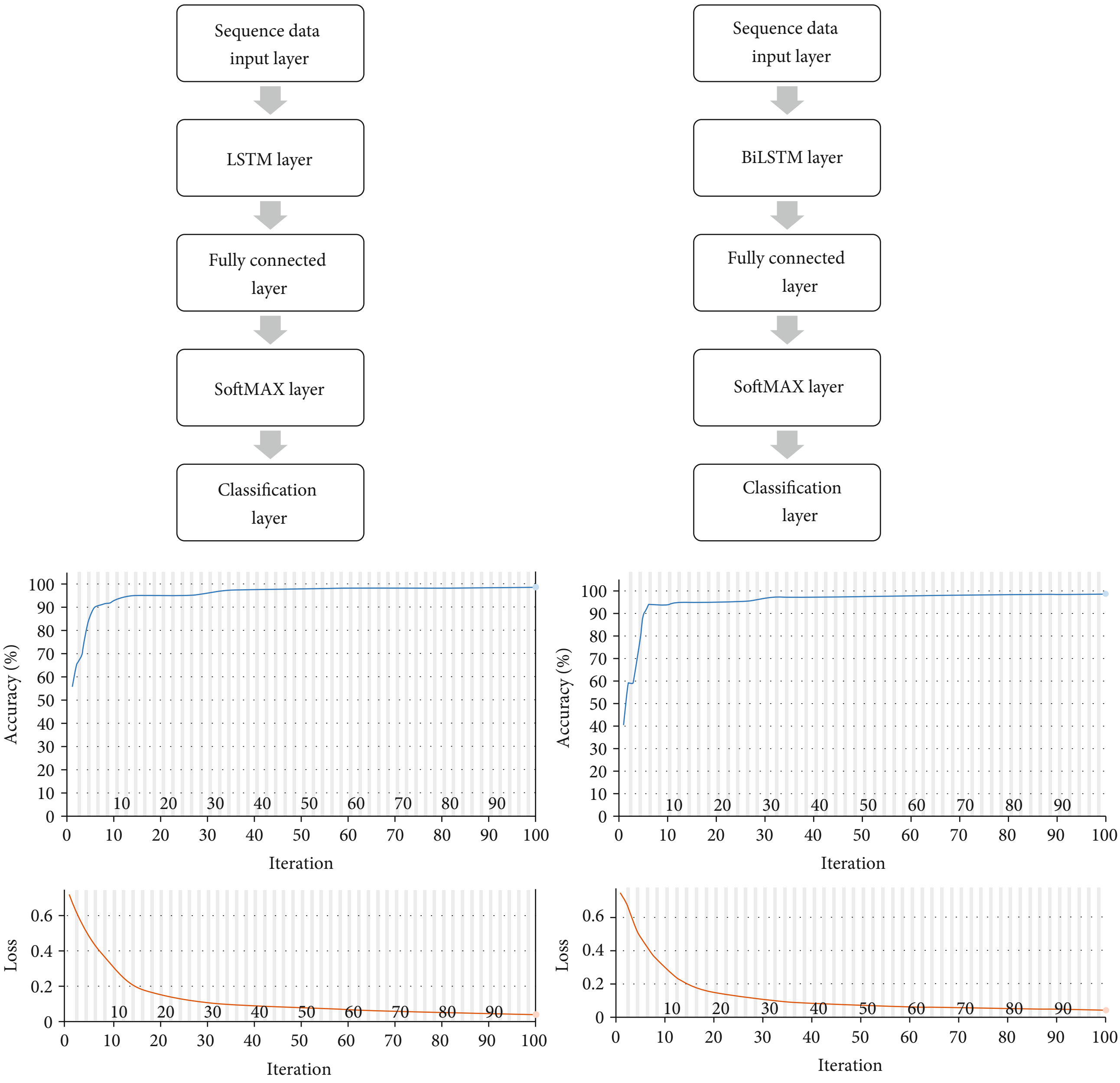
(1) The output stays at the present step in a short-term condition

(2) The long-term state, while moving across the network, saves, retrieves, and refuses things intended for the long-term

As shown in Figure 3, the choice to read, store, or write is dependent on some perceptron. The result of the activation functions is a number between 0 and 1 $(0, 1)$. The forget and output gates decide whether fresh material should be kept or discarded. The model choice is made using the LSTM block's storage and the output gate's situation. The output is then sent again into the network as an input, resulting in a recurrent sequence. When categorizing texts, the LSTM model may be used to resolve the challenges that typical machine learning methods struggle to extract high-level meaning [93]. This model takes as input a content matrix made up of pretrained distributed word vectors and then uses its unique memory structure to extract feature expressions forming context information (see Figure 3). Figure 3(a) depicts the LSTM modeling approach. A conventional LSTM network may use only the historical context. The lack of future context, on the other hand, may result in an insufficient grasp of the compound word. A forward LSTM layer and a backward LSTM layer are combined in BiLSTM. The correlation method may be used entirely by summing the knowledge of two ideates before and after the word. Figure 3(b) depicts the model's architecture [93].

4. Results and Discussion

4.1. Data Collection. NSL-KDD is a database suggested to address some of the KDD dataset's profound contradictions [94]. The definitive collection of data to be examined is contained in this database, which forms a wide range of simulated intrusions in a military network environment. However, McHugh's issues stay in this latest version of the KDD dataset. The natural network structure may not be completed. It can still be used as a collection due to the absence of public datasets for network-based systems. Researchers can employ user data to compare different intrusion detection technologies. Furthermore, the NSL-KDD training and test suites have a reasonable quantity of records. This edge can save money by allowing you to do tests on the complete set without having to pick a tiny section at random. As a result, the assessment outcomes of various research projects will be similar and consistent [94]. The NSL-KDD dataset offers benefits over the original KDD dataset: the learning suite lacks more information. Therefore, classifiers will not be biased toward more records. Because the testing sets have no history of duplicating, training performance is not influenced by approaches with higher detection capability in repeating data [95]. The proportion of records in the primary KDD dataset is inversely linked to the number picked from each category. As a result, the recognition accuracy of various machine learning methods varies across a more excellent range, making a correct assessment of different learning strategies more efficient. The training and test suites have a considerable number of records, making them cost-effective to run the tests in their



LSTM

BiLSTM

Figure 5: The architecture and the training process of the LSTM and BiLSTM networks.

entirety rather than selecting a tiny part at random. As a result, the outcomes of various research paper assessments will be uniform and similar. One of the critical drawbacks of KDD datasets is the enormous quantity of extra records, which causes pattern recognition to learn duplicate entries, which is typically destructive to networks such as U2R and R2L attacks. Furthermore, these repeated data in the test suite skew the assessment findings since approaches with superior detection rates in repeating records influence the outcome [94].

4.2. Results of Feature Extraction. Network traffic is often collected by DDoS detection techniques using passive network monitoring. The bought data is then analyzed to check whether there is any attack traffic. There are two basic methods for scanning an inactive network. For instance, packet capture intercepts and records network data packets. Wireshark and TCP dump are two tools that can gather data packets. Network flow monitoring supplies aggregated traffic data for a flow between two endpoints. Consequently, DDoS detection systems' effectiveness is assessed using two feature sets: packet-level and flow-level characteristics. Table 2 summarizes the packet- and flow-level characteristics. This study describes a flow as a one-way series of packages with identical 5-tuple values, including the source IP address, source port number,

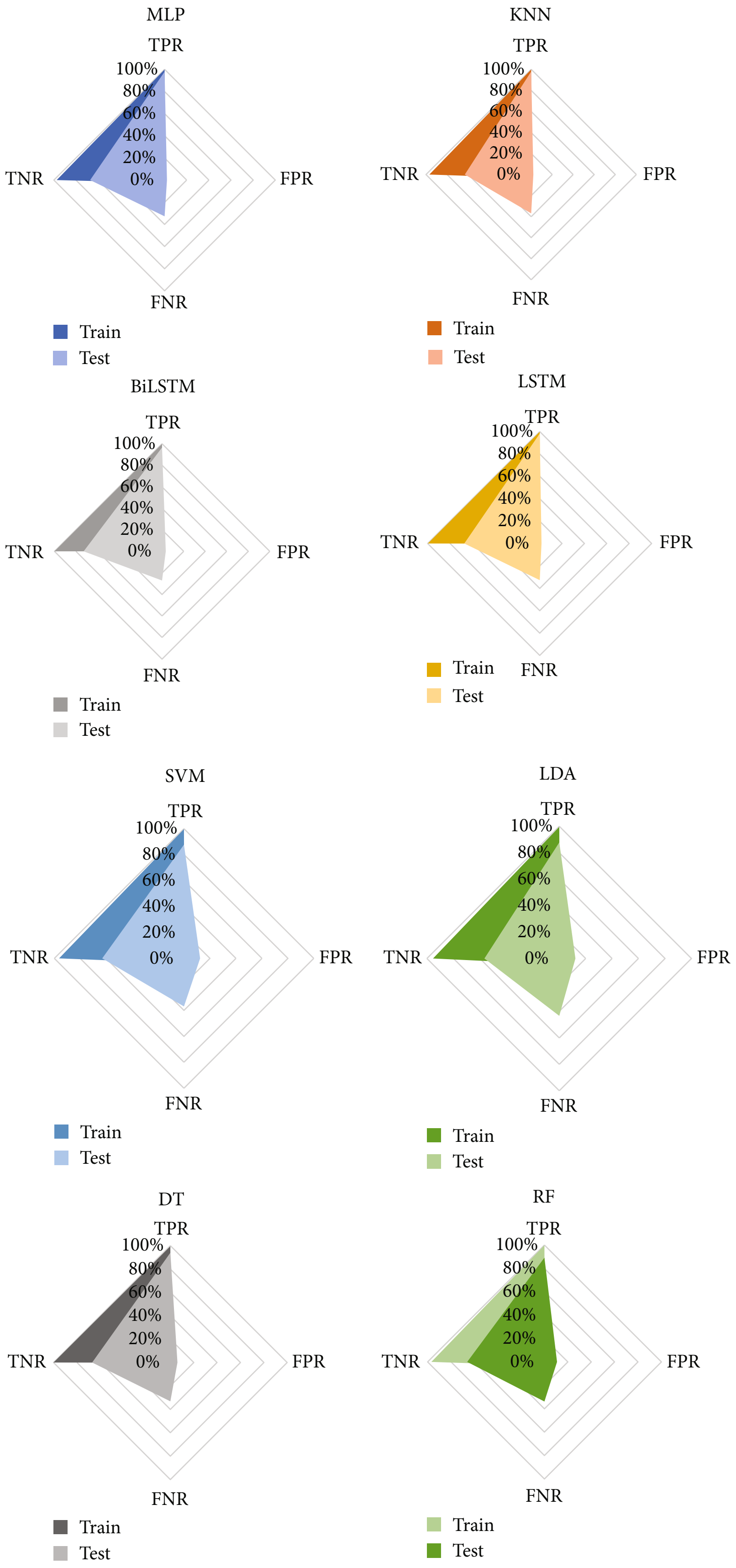


Figure 6: The confusion plots of the used ML methods.

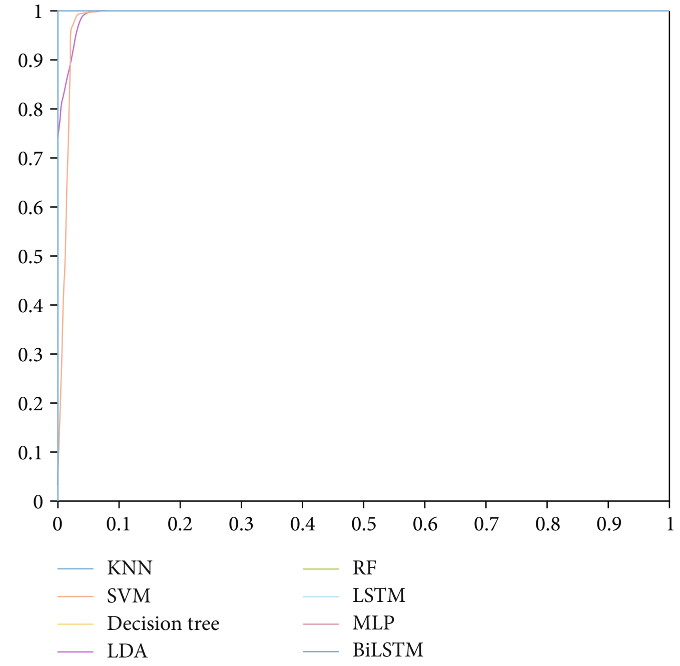


Figure 7: The ROC curve of the proposed methods.

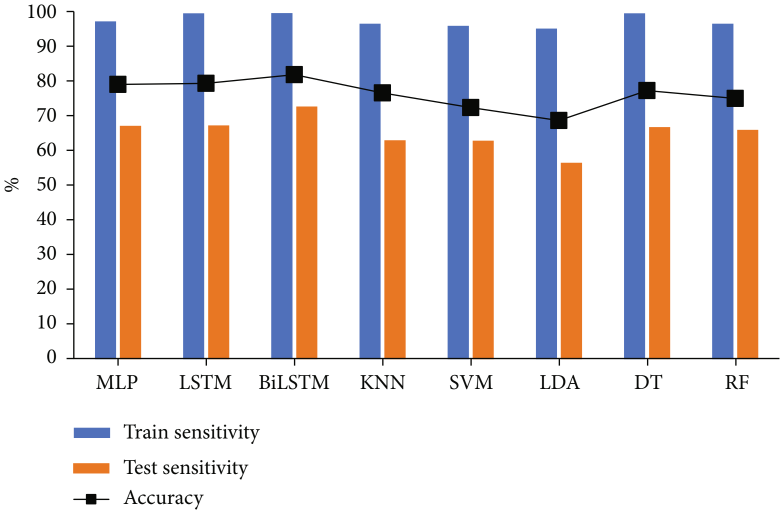


Figure 8: The accuracy, train sensitivity, and test sensitivity of the proposed approach.

destination IP address, port number, and protocol ID. This research investigates the detection performance of ML-based algorithms on both specified characteristics.

4.3. Classification Results. Various DDoS detection techniques have been presented. Many of them rely on a simple ANN using the backpropagation algorithm. The significant distinction between such designs is the structure of the recommended ANN in proportion to the number of neurons in each layer and the number of hidden layers. The majority of ANNs that have been evaluated have only one hidden layer. Neurons in the input layer reflect the gathered features from network traffic. In contrast, neurons in the output layer show the needed labels. Neurons in the buried layer typically range from 3 to 50 in number. ANNs are used to perform a wide range of detection tasks.

An ANN is used to decide the number of zombies engaged in a DDoS attack in this research. The system generates a regular profile in advance and continuously analyzes network traffic to detect an attack. A DDoS attack is recorded when the entropy of flow size deviates from a usual preset threshold. The deviation value is given into the ANN model to calculate the number of zombies. An ensemble detection strategy was developed to find DDoS attacks, which combines multiple ANN classifiers. The training dataset was first partitioned into two groups, attack and routine traffic, in the proposed way. The dataset for each class was further separated into n subgroups. The data was divided into k distinct groups in each subset. k training sets were reconstructed using these disjoint sets by omitting one of the disjoint sets. As a result, $k$and$n$ ANN classifiers were created for each class. After then, a fresh instance is put through its paces with all the classifiers. Weighted majority voting is used to make decisions over n subsets in each class. In contrast, a weighted product rule is used to make decisions across distinct classes.

Eight machine learning algorithms are employed in this article to diagnose DDoS attacks in IoT. The process dataset is NSL-KDD, with 1 and 0 labels showing normal and anomalous behaviors, respectively. The MLP network is the first way of diagnosis. The ANN network is designed with two hidden layers, each having 19 and 10 neurons. 70% of the dataset is trained, with the remaining 30% used for validation and testing. Iteration continues until the MSE of numerical labels is fixed. Figure 4 shows the outcomes of the MLP network.

The categorization results are shown in the form of a confusion matrix (see Figure 5). Figure 6 shows the results of the training confusion matrix, which show that 99.9% of the attacks are effectively found. To put it another way, out of 12109 anomaly nodes, 12098 (99.9%) are discovered and trained; however, 11 are misdiagnosed. As a result, the training procedure has a sensitivity of 99.9%. Furthermore, specificity is the opposite side of the diagnostic. This measure depicts the frequency of bad outcomes. Based on these findings, 8115 (97.6%) normal nodes are appropriately categorized, while 199 (2.4%) are misdiagnosed. Finally, the accuracy metrics showed the true-positive rate as a percentage of all diagnostic positives. In this case, 98.4 percent of the 12297 nodes used in DDoS attacks are indeed positive nodes or attacks. Finally, the training procedure is 99 percent correct. The findings of the testing dataset, on the other hand, confirm the networks that were used. According to the results, the testing samples' accuracy for 30% of the data is 79.5 percent. Furthermore, the sensitivity, specificity, and accuracy scores are 97.9 percent, 67.3 percent, and 66.5 percent, respectively. If we use the overfitting metrics (OF) to measure the difference between the two accuracies, the OF is 19.5 percent. The lower value of this OF confirms the categorization findings. The LSTM and BiLSTM architectures are depicted in Figure 5. The accuracy value of the LSTM and BiLSTM for the training procedure is 99.9% and 100%, respectively, based on their results. Furthermore, the OF values are 20.1 percent and 17.7 percent, respectively. MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF are among the eight machine learning algorithms used to verify the classification findings in this study. The LSTM and BiLSTM approaches surpass other methods in terms of test accuracy.

The ROC is illustrated in Figure 7 to compare the provided machine learning approach for diagnosing DDoS attacks. The horizontal axis of the ROC curve is the rate of the false-positive index depending on the anomaly class. The vertical axis shows the actual positive rate. The best classifier has the highest rate of true positives and the lowest number of false positives. The BiLSTM approach appears to be the best classifier for the supplied characteristics based on the findings. Figure 8 shows the accuracy of the machine learning classifiers. MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF accuracy values are 79.5 percent, 80 percent, 82.3 percent, 77 percent, 82.8 percent, 69 percent, 77.7 percent, and 75.4 percent, respectively, according to the data. Using the provided strategy, the BiLSTM architecture with the maximum accuracy is more correct and suitable for diagnosing DDoS attacks in IoT.

5. Conclusion

This study uses eight machine learning algorithms to diagnose DDoS attacks in IoT, including MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF. The process dataset is NSL-KDD, with 1 and 0 labels showing normal and anomalous behaviors, respectively. The categorization results are shown in the form of a confusion matrix. According to the findings of MLP's training confusion matrix, 99.9% of attacks are effectively recognized. Furthermore, specificity is the opposite side of the diagnostic. This measure depicts the frequency of bad outcomes. Based on these findings, 8115 (97.6%) normal nodes are appropriately categorized, while 199 (2.4%) are misdiagnosed. Finally, the accuracy metrics showed the true-positive rate as a percentage of all diagnostic positives. The accuracy value of the LSTM and BiLSTM for the training procedure is 99.9% and 100%, respectively, based on their results. Furthermore, the OF values are 20.1 percent and 17.7 percent, respectively. The LSTM and BiLSTM approaches surpass other methods in terms of test accuracy. The ROC is shown to compare the provided machine learning algorithm for diagnosing DDoS attacks. Based on the findings, the BiLSTM process appears to be the best classifier for the supplied characteristics. MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF test accuracy values are 79.5 percent, 80 percent, 82.3 percent, 77 percent, 82.8 percent, 69 percent, 77.7 percent, and 75.4 percent, respectively. Using the provided strategy, the BiLSTM architecture with the maximum accuracy is more correct and suitable for diagnosing DDoS attacks in IoT. For future works, we suggest that other methods like GRU also can result in high accuracy like LSTM methods.

Acronyms

ANN:	Artificial neural network
BiLSTM:	Bidirectional long short-term memory
CNN:	Convolutional neural network
CWT:	Continuous wavelet transform
DL:	Deep learning
DNS:	Domain name system
DT:	Decision tree
ICMP:	Internet control message protocol
DDoS:	Distributed denial of service
DoS:	Denial of service
IDS:	Intrusion detection system
IoT:	Internet of Things
KNN:	k-nearest neighbor algorithm

LDA:	Linear discriminant analysis
LSTM:	Long short-term memory
MLP:	Multilayer perceptron
NSL-KDD:	Network-based intrusion detection system dataset
NTP:	Network time protocol
OSI:	Open system interconnection
R2L:	Remote to user
RF:	Random forest
RNN:	Recurrent neural network
ROC:	Receiver operating characteristic
SDN:	Software-defined networking
SVM:	Support vector machine
SYN:	Synchronize
TCP:	Transmission control protocol
U2R:	User to root
UDP:	User datagram protocol
VFDT:	Variance fractal dimension trajectory.

Data Availability

Data is available and can be provided over the emails querying directly to the corresponding author (hamid.gh@aut.ac.ir).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Y. Liu, T. Zhi, M. Shen, L. Wang, Y. Li, and M. Wan, "Software-defined DDoS detection with information entropy analysis and optimized deep learning," *Future Generation Computer Systems*, vol. 129, pp. 99–114, 2022.

[2] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics*, vol. 9, no. 6, pp. 916–921, 2020.

[3] F. O. Catak and A. F. Mustacoglu, "Distributed denial of service attack detection using autoencoder and deep neural networks," *Journal of Intelligent Fuzzy Systems*, vol. 37, no. 3, pp. 3969–3979, 2019.

[4] J. Wang, Y. Liu, H. Feng, and National Engineering Laboratory on Interconnection Technology for Next Generation Internet, Beijing Jiaotong University, Beijing, China, "IFACNN: efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks," *Mathematical Biosciences and Engineering*, vol. 19, no. 2, pp. 1280–1303, 2021.

[5] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep learning for network traffic monitoring and analysis (NTMA): a survey," *Computer Communications*, vol. 170, pp. 19–41, 2021.

[6] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Mobile encrypted traffic classification using deep learning: experimental evaluation, lessons learned, and challenges," *IEEE Transactions on Network and Service Management*, vol. 16, no. 2, pp. 445–458, 2019.

[7] K. S. Sahoo, S. K. Panda, S. Sahoo, B. Sahoo, and R. Dash, "Toward secure software-defined networks against distributed denial of service attack," *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4829–4874, 2019.

[8] S. Kottler, "February 28th DDoS incident report," *GitHub*, pp. 1–3, 2018, http://githubengineering.com/ddos-incident-report/.

[9] S. Haider, A. Akhunzada, I. Mustafa et al., "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020.

[10] P. Manso, J. Moura, and C. Serrão, "SDN-based intrusion detection system for early detection and mitigation of DDoS attacks," *Information*, vol. 10, no. 3, p. 106, 2019.

[11] I. Karim, Q. T. Vien, T. A. Le, and G. Mapp, "A comparative experimental design and performance analysis of Snort-based intrusion detection system in practical computer networks," *Computers*, vol. 6, no. 1, p. 6, 2017.

[12] R. Xu, J. Cheng, F. Wang, X. Tang, and J. Xu, "A DRDoS detection and defense method based on deep forest in the big data environment," *Symmetry (Basel)*, vol. 11, no. 1, p. 78, 2019.

[13] D. Ramotsoela, A. Abu-Mahfouz, and G. Hancke, "A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study," *Sensors (Switzerland)*, vol. 18, no. 8, p. 2491, 2018.

[14] Z. Lv, Y. Li, H. Feng, and H. Lv, "Deep learning for security in digital twins of cooperative intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[15] J. Chen, Q. Wang, J. Huang, and X. Chen, "Motorcycle ban and traffic safety: evidence from a quasi-experiment at Zhejiang, China," *Journal of advanced transportation*, vol. 2021, Article ID 7552180, 13 pages, 2021.

[16] Z. Lv, J. Guo, and H. Lv, "Safety Poka yoke in zero-defect manufacturing based on digital twins," *IEEE transactions on industrial informatics*, p. 1, 2022.

[17] X. Liu, J. Zhao, J. Li, B. Cao, and Z. Lv, "Federated neural architecture search for medical data security," *IEEE transactions on industrial informatics*, vol. 18, no. 8, pp. 5628–5636, 2022.

[18] Q. Sun, K. Lin, C. Si, Y. Xu, S. Li, and P. Gope, "A secure and anonymous communicate scheme over the Internet of Things," *ACM Transactions on Sensor Networks*, vol. 18, no. 3, pp. 1–21, 2022.

[19] A. Mehbodniya, J. L. Webber, M. Shabaz, H. Mohafez, and K. Yadav, "Machine learning technique to detect Sybil attack on IoT based sensor network," *IETE Journal of Research*, pp. 1–9, 2021.

[20] B. Cao, J. Zhang, X. Liu et al., "Edge-cloud resource scheduling in space-air-ground integrated networks for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5765–5772, 2021.

[21] G. Sun, Y. Cong, J. Dong, Y. Liu, Z. Ding, and H. Yu, "What and how: generalized lifelong spectral clustering via dual memory," *IEEE transactions on pattern analysis and machine intelligence*, vol. 44, no. 7, pp. 3895–3908, 2021.

[22] M. Ahmadi, A. Taghavirashidizadeh, D. Javaheri, A. Masoumian, S. J. Ghoushchi, and Y. Pourasad, "DQRE-SCnet: a novel hybrid approach for selecting users in federated learning with deep-Q-reinforcement learning based on spectral clustering," Journal of King Saud University-Computer and Information Sciences, 2021.

[23] G. Sun, Y. Cong, Q. Wang, B. Zhong, and Y. Fu, "Representative task self-selection for flexible clustered lifelong learning," *IEEE transaction on neural networks and learning systems*, vol. 33, no. 4, pp. 1467–1481, 2020.

[24] F. Liu, G. Zhang, and J. Lu, "Multi-source heterogeneous unsupervised domain adaptation via fuzzy-relation neural networks," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 11, pp. 3308–3322, 2020.

[25] A. Mehbodniya, J. L. Webber, R. Neware, F. Arslan, R. V. Pamba, and M. Shabaz, "Modified Lamport Merkle Digital Signature blockchain framework for authentication of Internet of Things healthcare data," *Expert Systems*, p. e12978, 2022.

[26] L. Zhang, T. Gao, G. Cai, and K. L. Hai, "Research on electric vehicle charging safety warning model based on back propagation neural network optimized by improved gray wolf algorithm," *Journal of Energy Storage*, vol. 49, p. 104092, 2022.

[27] J. Dong, Y. Cong, G. Sun, Z. Fang, and Z. Ding, "Where and how to transfer: knowledge aggregation-induced transferability perception for unsupervised domain adaptation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, p. 1, 2021.

[28] W. Yang, X. Chen, Z. Xiong, Z. Xu, G. Liu, and X. Zhang, "A privacy-preserving aggregation scheme based on negative survey for vehicle fuel consumption data," *Information Sciences*, vol. 570, pp. 526–544, 2021.

[29] X. Wu, W. Zheng, X. Chen, Y. Zhao, T. Yu, and D. Mu, "Improving high-impact bug report prediction with combination of interactive machine learning and active learning," *Information and Software Technology*, vol. 133, p. 106530, 2021.

[30] A. Khaliq, A. Anjum, A. Ajmal, J. Webber, A. Mehbodniya, and S. Khan, "A secure and privacy preserved parking recommender system using elliptic curve cryptography and local differential privacy," *IEEE Access*, vol. 10, 2022.

[31] X. Wu, W. Zheng, X. Xia, and D. Lo, "Data quality matters: a case study on data label correctness for security bug report prediction," *IEEE Transactions on Software Engineering*, vol. 48, no. 7, pp. 2541–2556, 2021.

[32] W. Zheng, Y. Xun, X. Wu, Z. Deng, X. Chen, and Y. Sui, "A comparative study of class rebalancing methods for security bug report classification," *IEEE Transactions on Reliability*, vol. 70, no. 4, pp. 1658–1670, 2021.

[33] W. Zheng, T. Shen, X. Chen, and P. Deng, "Interpretability application of the Just-in-Time software defect prediction model," *Journal of Systems and Software*, vol. 188, article 111245, 2022.

[34] K. Liu, F. Ke, X. Huang et al., "DeepBAN: a temporal convolution-based communication framework for dynamic WBANs," *IEEE Transactions on Communications*, vol. 69, no. 10, pp. 6675–6690, 2021.

[35] T. Gera, J. Singh, A. Mehbodniya, J. L. Webber, M. Shabaz, and D. Thakur, "Dominant feature selection and machine learning-based hybrid approach to analyze android ransomware," *Security and Communication Networks*, vol. 2021, Article ID 7035233, 22 pages, 2021.

[36] Z. Liu, P. Qian, X. Wang, Y. Zhuang, L. Qiu, and X. Wang, "Combining graph neural networks with expert knowledge for smart contract vulnerability detection," *IEEE Transactions on Knowledge and Data Engineering*, p. 1, 2021.

[37] X. Zhang, Y. Wang, M. Yang, and G. Geng, "Toward concurrent video multicast orchestration for caching-assisted mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 13205–13220, 2021.

[38] C. Zong, H. Wang, and Z. Wan, "An improved 3D point cloud instance segmentation method for overhead catenary height detection," *Computers & electrical engineering*, vol. 98, article 107685, 2022.

[39] A. Varmaghani, A. Matin Nazar, M. Ahmadi, A. Sharifi, S. Jafarzadeh Ghoushchi, and Y. Pourasad, "DMTC: optimize energy consumption in dynamic wireless sensor network based on fog computing and fuzzy multiple attribute decision-making," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9953416, 14 pages, 2021.

[40] C. Zong and Z. Wan, "Container ship cell guide accuracy check technology based on improved 3D point cloud instance segmentation," *Brodogradnja*, vol. 73, no. 1, pp. 23–35, 2022.

[41] R. Singh, A. Mehbodniya, J. L. Webber et al., "Analysis of network slicing for management of 5G networks using machine learning techniques," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9169568, 10 pages, 2022.

[42] Y. Xie, Y. Sheng, M. Qiu, and F. Gui, "An adaptive decoding biased random key genetic algorithm for cloud workflow scheduling," *Engineering applications of artificial intelligence*, vol. 112, article 104879, 2022.

[43] A. Li, C. Masouros, A. L. Swindlehurst, and W. Yu, "1-bit massive MIMO transmission: embracing interference with symbol-level precoding," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 121–127, 2021.

[44] Y. Feng, B. Zhang, Y. Liu et al., "A 200-225-GHz manifold-coupled multiplexer utilizing metal wave guides," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 12, pp. 5327–5333, 2021.

[45] M. Ghanbari, "Adaptive machine learning and signal processing detection schemes for DDoS attacks," 2022.

[46] Z. Niu, B. Zhang, B. Dai et al., "220 GHz multi circuit integrated front end based on solid-state circuits for high speed communication system," *Chinese Journal of Electronics*, vol. 31, no. 3, pp. 569–580, 2022.

[47] W. Zheng, L. Yin, X. Chen, Z. Ma, S. Liu, and B. Yang, "Knowledge base graph embedding module design for visual question answering model," *Pattern Recognition*, vol. 120, p. 108153, 2021.

[48] A. R. Ramtin, P. Nain, D. S. Menasche, D. Towsley, and E. D. S. E Silva, "Fundamental scaling laws of covert DDoS attacks," *Performance Evaluation*, vol. 151, p. 102236, 2021.

[49] W. Zheng, X. Liu, X. Ni, L. Yin, and B. Yang, "Improving visual reasoning through semantic representation," *IEEE Access*, vol. 9, pp. 91476–91486, 2021.

[50] W. Zheng, X. Liu, and L. Yin, "Sentence representation method based on multi-layer semantic network," *Applied Sciences*, vol. 11, no. 3, p. 1316, 2021.

[51] J. Yu, L. Lu, Y. Chen, Y. Zhu, and L. Kong, "An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing," *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 337–351, 2021.

[52] H. Kong, L. Lu, J. Yu, Y. Chen, and F. Tang, "Continuous authentication through finger gesture interaction for smart homes using WiFi," *IEEE Transactions on Mobile Computing*, vol. 20, no. 11, pp. 3148–3162, 2021.

[53] B. Hajipour Khire Masjidi, S. Bahmani, F. Sharifi, M. Peivandi, M. Khosravani, and A. Hussein Mohammed, "CT-ML: diagnosis of breast cancer based on ultrasound images and time-dependent feature extraction methods using contourlet transformation and machine learning," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 1493847, 15 pages, 2022.

[54] S. Zhao, F. Li, H. Li et al., “Smart and practical privacy-preserving data aggregation for fog-based smart grids,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 521–536, 2021.

[55] Q. Meng, X. Lai, Z. Yan, C. Su, and M. Wu, “Motion planning and adaptive neural tracking control of an uncertain two-link rigid-flexible manipulator with vibration amplitude constraint,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 8, pp. 3814–3828, 2021.

[56] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, “A hybrid machine learning approach for detecting unprecedented DDoS attacks,” *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8106–8136, 2022.

[57] A. Prasad and S. Chandra, “VMFCVD: an optimized framework to combat volumetric DDoS attacks using machine learning,” *Arabian Journal for Science and Engineering*, vol. 47, pp. 1–19, 2022.

[58] X. Xu, J. Sun, C. Wang, and B. Zou, “A novel hybrid CNN-LSTM compensation model against DoS attacks in power system state estimation,” *Neural Processing Letters*, vol. 54, no. 3, pp. 1597–1621, 2022.

[59] E. Tsogbaatar, M. H. Bhuyan, D. Fall et al., “A 1D-CNN based deep learning for detecting VSI-DDoS attacks in IoT applications,” in *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, vol. 12798 of Advances and Trends in Artificial Intelligence. Artificial Intelligence Practices, pp. 530–543, Springer, Cham, 2021.

[60] D. Tang, L. Tang, W. Shi, S. Zhan, and Q. Yang, “MF-CNN: a new approach for LDoS attack detection based on multi-feature fusion and CNN,” *Mobile Networks and Applications*, vol. 26, no. 4, pp. 1705–1722, 2021.

[61] H. Alkahtani and T. H. H. Aldhyani, “Botnet attack detection by using CNN-LSTM model for Internet of Things applications,” *Security and Communication Networks*, vol. 2021, 23 pages, 2021.

[62] R. V. Mendonca, A. A. M. Teodoro, R. L. Rosa et al., “Intrusion detection system based on fast hierarchical deep convolutional neural network,” *IEEE Access*, vol. 9, pp. 61024–61034, 2021.

[63] M. Ghanbari and W. Kinsner, “Detecting DDoS attacks using an adaptive-wavelet convolutional neural network,” *Canadian Conference on Electrical and Computer Engineering*, 2021, pp. 1–7, ON, Canada, September 2021.

[64] X. Liu, Z. Tang, and B. Yang, “Predicting network attacks with CNN by constructing images from NetFlow data,” in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 61–66, Washington, DC, USA, May 2019.

[65] J. Cheng, Y. Liu, X. Tang, V. S. Sheng, M. Li, and J. Li, “DDoS attack detection via multi-scale convolutional neural network,” *Computers, Materials & Continua*, vol. 62, no. 3, pp. 1317–1333, 2020.

[66] A. E. Cil, K. Yildiz, and A. Buldu, “Detection of DDoS attacks with feed forward based deep neural network model,” *Expert Systems with Applications*, vol. 169, p. 114520, 2021.

[67] N. Mishra and S. Pandya, “Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review,” *IEEE Access*, vol. 9, pp. 59353–59377, 2021.

[68] M. Ahmadi and M. Q. H. Abadi, “A review of using object-orientation properties of C++ for designing expert system in strategic planning,” *Computer Science Review*, vol. 37, p. 100282, 2020.

[69] G. Zhou, X. Bao, S. Ye, H. Wang, and H. Yan, “Selection of optimal building facade texture images from UAV-based multiple oblique image flows,” *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 2, pp. 1534–1552, 2021.

[70] M. Ahmadi, M. Soofiabadi, M. Nikpour, H. Naderi, L. Abdullah, and B. Arandian, “Developing a deep neural network with fuzzy wavelets and integrating an inline PSO to predict energy consumption patterns in urban buildings,” *Mathematics*, vol. 10, no. 8, p. 1270, 2022.

[71] G. Zhou, X. Zhou, Y. Song et al., “Design of supercontinuum laser hyperspectral light detection and ranging (LiDAR) (SCLaHS LiDAR),” *International journal of remote sensing*, vol. 42, no. 10, pp. 3731–3755, 2021.

[72] M. Tondro, M. Jahanbakht, S. B. Rabbani, and M. Zaber, “Does immergence of ICT focused institutions increase the pace of urban development? A provincial case study in Iran using data from the ground and above,” in *I2022 IEEE Conference on Technologies for Sustainability (SusTech)*, pp. 219–223, Corona, CA, USA, April 2022.

[73] G. Zhou, R. Zhang, and S. Huang, “Generalized buffering algorithm,” *IEEE Access*, vol. 9, pp. 27140–27157, 2021.

[74] X. Liang, L. Luo, S. Hu, and Y. Li, “Mapping the knowledge frontiers and evolution of decision making based on agent-based modeling,” *Knowledge-Based Systems*, vol. 250, p. 108982, 2022.

[75] L. Zhao and L. Wang, “A new lightweight network based on MobileNetV3,” *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 16, no. 1, pp. 1–15, 2022.

[76] H. Zhu, M. Xue, Y. Wang, G. Yuan, and X. Li, “Fast visual tracking with Siamese oriented region proposal network,” *IEEE Signal Processing Letters*, vol. 29, p. 1437, 2022.

[77] J. Li, K. Xu, S. Chaudhuri, E. Yumer, H. Zhang, and L. Guibas, “GRASS: generative recursive autoencoders for shape structures,” *ACM Transactions on Graphics (TOG)*, vol. 36, no. 4, pp. 1–14, 2017.

[78] P. P. F. Rajeena, R. Orban, K. S. Vadivel et al., “A novel method for the classification of butterfly species using pre-trained CNN models,” *Electronics*, vol. 11, no. 13, p. 2016, 2022.

[79] H. Ghayvat, S. Pandya, P. Bhattacharya et al., “CP-BDHCA: blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications,” *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1937–1948, 2021.

[80] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune: an ensemble of autoencoders for online network intrusion detection,” 2018, http://arxiv.org/abs/1802.09089.

[81] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescape, “A hierarchical hybrid intrusion detection approach in IoT scenarios,” in *2020 IEEE Global Communications Conference, GLOBECOM 2020- Proceedings*, pp. 1–7, Taipei, Taiwan, December 2020.

[82] M. Ghanbari and W. Kinsner, “Detecting DDoS attacks using polyscale analysis and deep learning,” *International Journal of Cognitive Informatics and Natural Intelligence*, vol. 14, no. 1, pp. 17–34, 2020.

[83] J. Zhang, C. Zhu, L. Zheng, and K. Xu, “ROSEFusion: random optimization for online dense reconstruction under fast

camera motion," *ACM transactions on graphics*, vol. 40, no. 4, pp. 1–17, 2021.

[84] F. Zhang, J. Zhai, X. Shen, O. Mutlu, and X. Du, "POCLib: a high-performance framework for enabling near orthogonal processing on compression," *IEEE transactions on Parallel and Distributed Systems*, vol. 33, no. 2, pp. 459–475, 2022.

[85] R. F. Fouladi, O. Ermiş, and E. Anarim, "A novel approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software-defined network," *Computers & Security*, vol. 112, p. 102524, 2022.

[86] Y. Cui, Q. Qian, C. Guo et al., "Towards DDoS detection mechanisms in software-defined networking," *Journal of Network and Computer Applications*, vol. 190, p. 103156, 2021.

[87] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proceedings -2018 IEEE Symposium on Security and Privacy Workshops, SPW*, pp. 29–35, San Francisco, CA, USA, May 2018.

[88] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Future Generation Computer Systems*, vol. 111, pp. 763–779, 2020.

[89] Z. Liu, X. Yin, and Y. Hu, "CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-learning," *IEEE Access*, vol. 8, pp. 42120–42130, 2020.

[90] J. Hou, P. Fu, Z. Cao, and A. Xu, "Machine learning based DDoS detection through NetFlow analysis," in *Proceedings-IEEE Military Communications Conference MILCOM*, pp. 565–570, Los Angeles, CA, USA, October 2018.

[91] Y. N. Soe, P. I. Santosa, and R. Hartanto, "DDoS attack detection based on simple ANN with SMOTE for IoT environment," in *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC*, pp. 1–5, Semarang, Indonesia, October 2019.

[92] Y. Li and Y. Lu, "LSTM-BA: DDoS detection approach combining LSTM and Bayes," in *Proceedings -2019 7th International Conference on Advanced Cloud and Big Data, CBD*, pp. 180–185, Suzhou, China, September 2019.

[93] W. Huang, X. Peng, Z. Shi, and Y. Ma, "Adversarial attack against LSTM-based DDoS intrusion detection system," in *Proceedings-International Conference on Tools with Artificial Intelligence, ICTAI*, pp. 686–693, Baltimore, MD, USA, November 2020.

[94] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA*, pp. 1–6, Ottawa, ON, Canada, July 2009.

[95] R. Rama Devi and M. Abualkibash, "Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets - a review paper," *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 11, no. 3, pp. 65–80, 2019.